Author's Note on the Free Digital Version:

You are reading the free digital version of Cash - The Only Way to Preserve Basic Human Freedom. Some of the formatting, layout and page count have been modified to make this document easier to read on a screen. There are two reasons I am making this book available for free in digital form, despite the enormous amount of time and resources it cost me to write and produce it:

1. Since this book contains an enormous amount of references to articles and videos available online and links listed to those in the footnotes, I want to spare the reader the work of having to type these links manually into a browser and instead enable you to copy and paste the urls if you would like to look them up.
2. The message is so important and urgent that it is more important to me that as many people read it as soon as possible than to recover compensation for the time and resources I have spent. For this reason, please feel free to share the link and the file with as many people as you can.

Nevertheless, if you appreciate what you read, would like to spread the word, and/or support my work, please consider purchasing a physical copy of the book at www.preservecash.org.

In any case: thank you for reading this book and please help spread the word before it is too late!

In Liberty,
Tobi Maier

CASH

THE ONLY WAY TO PRESERVE BASIC HUMAN FREEDOM

Why using and preserving physical cash is so crucial.

The potential disappearance of cash is perhaps the greatest threat to freedom in human history. We must do everything in our power to prevent it.

By Tobias E. Maier, Esq.

www.preservecash.org v.1.0

v.1.1

Digital and paperback version available at www.preservecash.org

© 2026 All rights reserved.

ISBN: 978-1-935877-95-0

Artwork by Rebekah Ross and Tobi Maier

Printed in the United States of America.

The information in this book is neither investment nor legal advice. While the author is an attorney, the reading or purchasing of this book, or a donation to the author, or attending an event with him as a speaker, do not establish an attorney-client relationship.

The author has made every effort to ensure the information in this book was correct and accurate at the time of publication. The author does not assume, and hereby disclaims, any liability to any party for any loss, damage, disruption or other injury caused by errors or omissions whether such are the result of negligence, accident or any other cause. Every person is responsible for their own actions, and the consequences of their actions. While this book is intended to be food for thought, the reader is encouraged and expected to use his or her own critical thinking in determining his or her actions. The author does not assume and hereby disclaims any liability for actions and decisions by the reader or a third party.

Note: Some of the cited internet links may stop working over time as their content gets removed by the respective site owners. If you run into a link that no longer works, please try out the Internet Archive Wayback Machine at archive.org and enter the link there. You will then see some archived versions of the page you are looking for.

Dedicated to Frank Samuel Niceley,

one of the wisest men who walked the earth during our lifetime.

www.presentcash.org v.1.1

Table of Contents

I. Executive Summary....1
II. Preface: A Note on AI....5
III. Introduction....7
IV. Electronic Payments....9
V. Programmable Money....11
VI. Social Credit Score....15
VII. Why Cash is the Only Option that Preserves Freedom....19
VIII. Stability of Value is Secondary to Transaction Freedom....25
IX. Convenience....33
X. Secondary Reasons to Use Cash Instead of Electronic Payments....35
1. Resilience against Disruptions....35
2. Resilience against Cyberattacks....38
3. Resilience against Debanking....41
4. Fraud....43
5. Saving Money....46
6. Fees....47
7. Negative Interest Rates....48
8. Surveillance Pricing....49
9. Surveillance Wages....55
10. Quishing....56
11. Terms and Conditions....59
12. Enshittification....61
13. Save Small, Independent Businesses....65
14. Save Small Farms and Retain Access to Trustworthy Food....66
15. Budgeting....68
16. Discrimination and Exclusion....68
17. Crucial Education....70
18. Courtesy....71
19. Drain on the Economy....72
XI. Arguments Against Cash - And Counterarguments....75
XII. Are there any Freedom-Preserving Alternatives to Cash? 81

1. Cryptocurrencies? 81
2. Checks? 87
3. Debit Cards? 88
4. Apps? 90
5. Gold and Silver? 91
6. Barter? 94
XIII. How Close Are We? 97
XIV. Is It Too Late? 105
XV. A Case for Hope....107
XVI. What Legislators Can Do....113
1. Laws Requiring Cash Acceptance....113
2. Create Incentives for Cash Usage....115
3. Put Guardrails on Programmable Money....116
4. Protect the Right to a Non-Digital Life....117
5. Prohibit Surveillance Pricing....118
6. Bring Back Larger Denomination Bills....119
XVII. What Individuals Can Do....121
1. Pay Cash Only. Always. 121
2. Refuse to do Business with Businesses that Don't Accept Cash. 122
3. Don't Fall for Red Herrings. 123
4. Don't Scan QR Codes. Ever! 123
5. Don't Get a Digital ID! Ever! 124
6. Make a Conscious Decision Where You Bank. …126
7. Be Conscious What You Fund. 128
8. Shop in Brick and Mortar Stores. 129
9. Educate Those Around You. 129
10. Talk to Your Legislators. 130
11. Sign a Petition to Protect Cash. 131
12. Support Businesses that Offer Cash Discounts. .131
13. Consider Getting a Dumbphone. 132
14. Share and Spread this Book as Much as You Can. 134
15. Turtle Forward and Never Give Up. 134
XVIII. Use it or lose it....137
XIX. Conclusion....139
Acknowledgments....142
About the Author....144
Organizations and People to Support....145
Glossary....146

I. EXECUTIVE SUMMARY

If you would like to continue to live your own self-determined lifestyle, this book is for you.

Cash is essential for the preservation of basic individual liberty. We take the ability to use cash for granted. For the first time in history, however, our ability to pay, exchange goods and services, and participate in public life, is becoming conditional upon the consent of invisible third parties.

With cash, transactions are between **two** parties. In contrast, electronic transactions always require the consent of a **third** party. This has the potential to directly curtail your personal freedom and fundamentally change what life looks like, although it won't become fully apparent until cash no longer exists as an option.

The existence of cash keeps digital payment providers, as well as banks and governments, comparably kind as they know you could simply use cash if they deny too many of your transactions, impose negative interest rates, make the use of their products and services too frustrating, or suspend your ability to pay altogether.

This is why protecting our ability to use cash may well be one of the most important things we can do in our day-to-day lives. If we do not want to find ourselves in a world that resembles the episode "Nosedive"[1] from the TV-series "Black Mirror" in

1 A great visualization of what life under a social credit score regime could look like. Quite similar to the reality in China, the characters are constantly forced to live a fake, compliant life, lest they want to risk losing access to society's amenities and experience a serious downgrade of their quality of life.

the near future, cash is the main feature of our daily lives we must preserve.

This book dives deeper into various reasons why it is crucial to use and protect cash, benefits which using cash has for you and for others, as well as what you can do to help. Your daily choices actually matter. Whether you pay with cash or electronically essentially counts as a vote. We'll go more into this later, as well as into what else you can do to protect cash.

Aside from protecting your freedom and the liberty of your children and grandchildren, cash also helps keep money in your community. Credit card fees siphon out a percentage of every transaction, which otherwise would go to local shops, restaurants or other businesses.

During disasters (power outages, internet disruptions), or disruptions to a payment provider's servers, data or infrastructure, cash is often the only way to pay. If you are stuck somewhere late at night, are hungry, or need to urgently pay for something else and your credit card transaction gets denied because the provider's algorithm erroneously suspects that the transaction might be fraudulent, or because your phone's battery is dead or the network is down, cash can save you from many problems.

Keeping cash alive is also important for younger generations. Pocket money or an allowance as a teenager is a great and risk-free way to learn basic skills like budgeting. If children and teens do not get to make payment decisions and learn the function and value of money until they are adults, how are they supposed to understand the gravity of signing promissory notes for a student loan or a mortgage?

The debate about cash is therefore not about some quaint gimmick or nostalgia, it is fundamental to your independence as a person and the freedom of our society.

The following pages will evaluate in detail what matters and what doesn't when it comes to currency and equip you with powerful arguments for using, accepting, cherishing, and protecting cash, as well as concrete steps you can take to help protect us all from a cashless dystopia.

www.preservecash.org v.1.1

www.preservecash.org v.1.1

II. PREFACE: A NOTE ON AI

Every word in this book was manually written by a human being without the help of generative artificial intelligence or large language models. The same is true even for the graphics and my research for this book (I did use search engines, but no AI prompts). The reason I deem this noteworthy is because I feel a deep and sincere appreciation for you, the reader, taking your valuable time to read what I have to say about this important issue. In return, I promise you that I wrote every single word in this book with my own brain, fingers and keyboard and that nothing in this book is autogenerated.

It took way over a year (and much sacrifice) to put this book together. A few wonderful human beings supported and helped me along the way, reviewed this book, and offered suggestions for improvements based on their own thoughts and perspectives. The following individuals specifically deserve mentioning for their contributions, input, feedback and suggestions: Catherine Austin Fitts, Claire Viadro, Sullivan Wyndham, Proctor Teague, Taylor Gallagher, Susan Luschas, Andreas Maier, Paul Howson, Isaac Botkin, and Ralf Werner. I took their input and feedback, conducted more research, and continued editing and writing. While it would have been a lot faster to autogenerate a book with AI, it would not be mine, I would not be able to vouch for it or its content, and I would not feel comfortable presenting it to you in my name.

I am, on the other hand, very grateful that you are taking your valuable time to read this book and that you are taking the issues of cash and human freedom seriously. I do not take this for granted. Thank you for that!

www.preservecash.org v.1.1

III. INTRODUCTION

Without cash, human freedom will disappear. It will happen faster than you could imagine in your worst nightmare. You will be forced to do things you would never voluntarily agree to do. But you won't have a choice. You will have nowhere to escape to. Say or write something wrong, purchase the wrong item (or at the wrong time or place) and you will immediately be punished. Fail to visit your parents often enough (no matter your relationship with them), or visit them in an emergency despite a lockdown, and your money loses functionality; criticize the government or even make the wrong moves in a video game: ditto. Don't even think about making your own health choices! You will be subject to a level of control which never existed in human history. And it will be more absolute than any system of slavery ever was. The next generation will comprehend freedom as much as a person born blind comprehends color. They will have no concept of it. They will never get to experience it. It won't mean anything to them and it won't make sense to them.

In thousands of years of human history, we may never have been this close to losing freedom altogether. Privacy is obviously being lost along with it. Here in the United States, generations of Americans had to make unimaginable sacrifices, risk being tried for treason, and fight bloody wars in order to secure our freedom. Specifically the Revolutionary War, the Civil War and World War II. All their sacrifices will be wasted if cash disappears.

Unfortunately, we are closer to this historically unprecedented dystopia becoming reality than most of us are aware of. In

fact, some countries are already there.[2] The good news is: there is something you can do: pay with cash, refuse to spend money at businesses that don't accept it, and educate others.

We'll talk more about what you can do at the end of this book in chapters XVI and XVII.

Before we get into the details: note that the discussion about fiat currency, gold-standards, etc. is completely separate from the question of financial transaction freedom. For freedom, you need physical cash![3] Period. Whether that cash is fiat or gold-backed is completely irrelevant for the question of human freedom. The best gold-standard or "blockchain-guaranteed scarcity" will not prevent the enslavement just mentioned. It might enhance stability of value, but if you cannot access or use that value for anything, it will be useless.

Any reality in which payments are only possible electronically spells the end of your sovereignty as a human being. Keep that in mind and let it guide every decision you make going forward from this point!

www.preservecash.com

2 https://hrf.org/latest/tracking-cbdcs-before-they-track-you/

3 It should go without saying that “cash” means (only) *physical* cash, i.e. physical coins and notes.

IV. ELECTRONIC PAYMENTS

Over the last several decades, electronic payments have gained substantially in market share. For centuries, even banks transacted with each other in cash.[4] Nowadays, most commercial transactions occur via some form of electronic transfer. This always requires an intermediary, such as a credit card company, bank, or other money service provider (often more than one). Each such provider can both track and potentially block the transaction. As a result, there is, by definition, neither privacy nor independence from third-party consent when funds are transferred electronically.

Most consumers are not very aware of these two shortcomings (tracking and blocking) when making payments electronically, as privacy invasions happen largely unnoticed to the end user and third-party consent is currently not too frequently withheld in most Western countries and when it is, it appears benign in the vast majority of cases. However, most people would be devastated if they were aware of the extent to which their most intimate habits and preferences are often known to obscure companies that legally obtain, browse through, evaluate, and sell their data, as well as to bad actors waiting for an opportunity to exploit them. Although third party consent is actually withheld on a somewhat regular basis, the occurrences will appear isolated and/or harmless to most: think of denied credit card transactions, political sanctions, debanking or freezing of bank accounts, the latter of which usually happens at the direction of a government or government agency with

4 https://www.investopedia.com/6-famous-discontinued-and-uncommon-u-s-currency-denominations-4773302

some claim of legitimacy, although sometimes erroneously (tax authority employees make mistakes, too, etc.).

As long as cash is still an option, most third parties (banks, credit card companies, governments) are mindful not to push the envelope too far, as doing so could cause customers to leave or citizens to push back. Hence, aside from accidents, malfunctions and mistakes, many users currently don't tend to experience denials of their electronic transactions very often, as they so far only rarely happen intentionally (except in response to suspected fraud, which is happening with increasing frequency).

Once cash is gone, however, “the gloves will be off” and, because there won't be much people can do about it at that point, there will be little reason for governments or payment providers to restrain themselves from exercising their power to block or control transactions.

Electronic payments are also dependent on three factors working perfectly at all times:

1. Electricity must be available and reliable.
2. Communication needs to always be open and operational between all network components.
3. The network and servers must be secure.

All three components are often compromised, of course, as we will discuss in more detail later, thus making *any* electronic or digital means of payment by definition less reliable than a physical, offline way to transact, aka cash.

V. PROGRAMMABLE MONEY

Electronic payment systems (such as apps or debit cards) generally still represent a transfer of funds in a traditional currency (e.g., dollars, euros, yen). You are basically transferring ownership over conventional currency, and thus the programmability is separate from the currency itself. In essence, you have two separate layers: the programmable payment system and the underlying (not programmable) currency.

Just over a decade ago, a new form of money emerged: *programmable* money. Programmable money is different from other electronic payment systems in that it is both currency and payment system and only exists virtually in the first place. You no longer have separate layers; instead, the currency (in the form of digital "tokens", often misleadingly called "coins", despite only existing virtually) can itself be coded to change characteristics and functionality automatically or to perform a variety of actions autonomously. Thus, a programmable "token" or "coin"[5] may behave differently depending on who uses it. In other words, it won't necessarily allow you to buy the same goods and services as the person who transferred it to you. Likewise, it may not allow you to make the same purchases tomorrow as it does today. It may also automatically continue to partially transfer to a third party, without you doing

5 With electronic money, you do not have actual physical coins or notes. Instead you have database entries. This is basically a unit of a theoretical representation of monetary value, even though it is not necessarily represented by anything tangible at all. To make this completely virtual expression of "money" more palpable (and palatable) for end-users, it is usually called "coin", even though lacking actual coins (or notes) is one of its characteristics.

anything to initiate this separate transfer. This trait is sometimes referred to as “smart contracts” and sold as a positive feature.

Examples of programmable money[6] are: central bank digital currencies (CBDCs), cryptocurrencies (e.g. Bitcoin, Ethereum, etc.), and stablecoins (e.g. Tether, USDC, BinanceUSD, etc.). These are fundamentally different from electronic payment systems such as credit cards, payment apps, or ACH transfers, which are not themselves currency but instead mechanisms to transfer ownership over underlying currency.[7]

Whereas programmability of *payment systems* has existed for a long time, programmability of *money itself* is new. You cannot program a dollar. You can only program the system that transfers it. For example, you can instruct your payment provider to deny certain transactions to prevent fraudulent use of your credit card. In such scenarios, third parties may interfere (for example, a bank or government might deny your transaction for whatever reason), but this will not affect the underlying money itself. And if you physically hold that

6 The terms money and currency are largely used interchangeably in this book to be in line with the way they are most commonly used in the respective contexts these days. However, for the record: there is a difference between the two: simply put: money is currency that also serves as a store of value. We'll discuss the latter aspect in chapter VIII, but the distinction is not relevant for the aspect of programmability. U.S. payment stablecoins, CBDCs, and most cryptocurrencies are closer to programmable *currency* than programmable *money* in that distinction, although legally they are (currently) not currency in the United States either. Unless you are already familiar with the distinction, you can completely ignore it for purposes of this book.

7 For some payment systems, this is slightly oversimplified; for example, if you pay with a credit card, which is an electronic payment system, you are technically creating new dollars out of thin air, and when you pay off your credit card, you are deleting these newly created dollars from existence again. But for purposes of explaining the difference between programmable money and programmable payment systems, this difference is irrelevant. Even when you pay with a credit card, the payee still receives a claim to conventional dollars, which is **not** the case for programmable money.

dollar, how you use it is solely between you and the person you are transacting with. No third party can stop the two of you from exchanging that dollar.[8]

In the case of programmable money, the “tokens” can be programmed, and there is no underlying money separate from the virtual “token.” In such a system, the control that can be imposed is a lot more direct and absolute, as the money itself is the programmable electronic payment system. There is no longer any underlying non-programmable currency that you could use independently of the programmed instructions (such as is possible with cash).

All electronic payment systems always put you individually at the mercy of a third party. You cannot pay for anything or get paid for anything without third parties being aware of it, able to track, record, and sell that data, and potentially prevent you from paying or getting paid at every single step. With programmable money, all of this applies, but there are even graver implications because your money itself can be confiscated remotely, diminished in value, limited in functionality, or simply turned off. For example, to stimulate the economy, your money could be programmed to expire by a certain date if you don’t spend it. Through so-called “smart contracts”, the terms and rules can dynamically change, be embedded in, and enforced through, your money itself.[9]

Payment with programmable money is always an electronic payment; however, not every electronic payment uses programmable money (in fact, as of the writing of this book, the vast majority don't - yet). Both are a threat to your privacy and freedom, but programmable money takes this threat a significant step further:

With programmable money and without cash, the nightmare is perfect as you no longer have a way out. Your digital "coins"

8 Other than with physical force.
9 https://live.solari.com/w/a81qSkjrf5L9y2mC2o3bpm

no longer represent old-fashioned dollars, not even in theory, and you are no longer able to convert your digital "coins" into physical money. Imagine being "de-banked", perhaps for political reasons.[10] The hassle is substantial. You have to find a new bank, fill out mountains of paperwork, take all your money there and update all your payment information. Now imagine being "de-currencied." In this case, you can no longer pay (or get paid) for anything at all. Money itself won't work in your hands. You are literally shut out from daily life.

It is important to note that this can happen both lawfully and intentionally (for example as a result of a bank policy, business policy, government decision, or determination by some algorithm), as well as criminally or accidentally (for example through a cyberattack or IT-flaw).

Furthermore, this capability can be seamlessly integrated with a social credit score system, which can automatically deny certain transactions based on your behavior. This is already reality in China. Even in the United States, some politicians, such as former presidential candidate Andrew Yang, are openly calling for the implementation of a digital social credit system.[11]

10 https://www.whitehouse.gov/presidential-actions/2025/08/guaranteeing-fair-banking-for-all-americans/

11 https://www.pbs.org/newshour/politics/what-does-andrew-yang-believe-where-the-candidate-stands-on-5-issues

VI. SOCIAL CREDIT SCORE

A social credit scoring system rates people based on their behavior. The score then determines an individual's access to various benefits, amenities or even necessities.

Autocratic governments are openly moving toward implementing some version of blacklist or social credit score system. In Western countries, where most governments so far try to maintain at least an appearance of liberty, the de-facto creation of social credit score systems is occurring via the private sector.[12] Obvious examples are the systems used by companies like Uber[13], Lyft[14], or Airbnb[15] to rate their customers.

These ratings are often not visible to the person who is being rated.[16] And just like in the “Black Mirror” episode “Nosedive”, people often give ratings without realizing their score's implications. For example, Airbnb hosts frequently face problems when happy customers rate them with a score of 4 out of 5 stars, not realizing that this may have serious adverse consequences for the host.[17] Combine this with the fact that some people give perfect ratings even for terrible service[18], and

12 https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=2736&context=vjtl
13 https://www.uber.com/eg/en/blog/how-the-uber-rating-system-works/
14 https://www.lyft.com/hub/posts/ratings-and-cancellations
15 https://www.airbnb.com/help/article/3287
16 https://communitycenter.airbnb.com/forum/2d51a5c2-16fb-4016-833b-8f987dae813c/post/bGVnYWN5X2Nj_1161939
17 https://community.withairbnb.com/t5/Support-with-your-bookings/Ratings-amp-Reviews-Guide-for-Guests/m-p/1932122
18 https://www.npr.org/2019/01/08/683144150/why-consumers-systematically-give-inflated-grades-for-poor-service

it becomes obvious how arbitrary or unfair your score may actually be.

For example, while customers leaving a good review with 4 stars may ruin your livelihood, hosts who were criminally investigated after spying on their guests with hidden cameras and filming them in the shower or bed, an issue Airbnb received tens of thousands of complaints about, remained active.[19] This shows that, while such ratings can have a chilling effect on perfectly lawful behavior (insurance companies often charge their customers more or even deny coverage, depending on what activities the customer engages in in his or her freetime[20]), they fail to stop crime.

Less than stellar scores can lead to being banned from a platform.[21] If your ebay ratings go down, for example, you might not find buyers for your used stuff anymore, and if your Airbnb host rating drops below perfect, you may no longer be able to rent out your spare rooms for weekend guests. If you made this your main source of income, you may have to look for a different one.

The implications become more existential, however, when such data is no longer used just to determine your standing with one particular platform, but is combined with data from other sources and used to judge you in a variety of places. This is increasingly the case, and is exactly the way an extralegal (i.e. without any due process or basis in law) social credit score is already being created via the private sector in the West.[22]

Many private companies already collect an enormous amount of behavioral data not only about their customers and users, but

19 https://edition.cnn.com/2024/07/09/business/airbnb-hidden-camera-invs
20 https://www.cbsnews.com/news/how-big-data-gives-insurers-a-giant-edge-over-consumers/
21 https://www.npr.org/2019/05/29/728005817/uber-to-start-banning-passengers-with-low-ratings
22 https://www.fastcompany.com/90394048/uh-oh-silicon-valley-is-building-a-chinese-style-social-credit-system

also about other individuals they can obtain data about.[23] What's more, companies frequently share and sell that data, including to other companies aggregating and analyzing it.[24] Companies use this data, which users often never intentionally shared with them, to create so-called shadow profiles, which they then sell to other parties and individuals who want to leverage that information against you. These shadow profiles are also a treasure trove for cybercriminals and a security nightmare for the person they are about.[25] Numerous business models are based on aggregating and selling data about people, collected from endless sources of data most people constantly allow to be collected about themselves by being careless about their privacy.[26] The conclusions, often made by some algorithm (or AI), can lead to reservations being harder to obtain or services being denied.[27]

In many ways, this is quickly becoming a social credit score in all but name. However, the gravest danger arises when these mechanisms combine with an all-digital payment system as this allows for immediate punishments and rewards for your behavior via automatic modifications to your money's functionality. As the example of China shows, this process does not even require the involvement of a human being; rather, an algorithm (or AI) will automatically condition you and make you submit to the will of a computer, without any recourse.[28]

23 https://www.cbsnews.com/news/how-big-data-gives-insurers-a-giant-edge-over-consumers/

24 https://web.archive.org/web/20260219194234/https://www.thenexus.media/your-phone-already-has-social-credit-we-just-lie-about-it/

25 https://medium.com/@ododo.okpabi/the-stalker-how-shadow-profiles-put-your-privacy-at-risk-a9d4c4008e67

26 https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user

27 https://www.engadget.com/2020-01-17-your-online-activity-effectively-social-credit-score-airbnb.html

28 There may of course, when you are stuck in the middle of nowhere late at night, or in a rush to pay for a ticket to catch the departing train or

Frighteningly, this phenomenon is already no longer confined to China: Even in the West, some payment processors already use the intimately detailed profiles they can obtain about a person, based on the aggregation and evaluation of smartphone data, cameras, online behavior etc. to deny transactions, sometimes in ways that look like a glitch.[29] And every time you pay electronically, you voluntarily provide more data to feed this scoring system.

Slowing personalized data collection and ensuring that you can make payments regardless of such scoring efforts are two more reasons to pay with cash.

www.preservecash.org v.1.1

check out and make it to an appointment, and your transaction is denied, be some website you can go to, assuming you have sufficient reception and battery and your phone has the exact browser version the website wants installed, and then you can search for a hidden option to dispute or investigate. Assuming you are able to solve the myriad of captchas to verify you are not a human, you might get to chat with an AI-bot that does not acknowledge or comprehend your issue or simply tells you to check back during normal business hours, when a higher level AI-chatbot will inform you that your score has fallen below policy-thresholds. If you are really lucky, you might be able to submit a written dispute, assuming you provide ample evidence, and get a formal written answer within 60 business days that a review of your complaint has been completed and your score will not be altered.

29 https://www.gadgetreview.com/digital-prison-how-your-smartphone-quietly-enforces-social-credit-its-already-here

VII. WHY CASH IS THE ONLY OPTION THAT PRESERVES FREEDOM

Cash is the only generally accepted means of payment that is anonymous, works without electricity, and does not allow a third party to block an individual or entity from making or receiving payments.

As already discussed, any electronic means of payment can be both tracked and shut down by a third party.

For example, if your bank, government, or even some algorithm, suspects that you might be engaged in illegal activity, they can simply block your ability to pay electronically. Credit card transactions are denied every day. Tax authorities around the world, such as the Internal Revenue Service (IRS) in the U.S., freeze bank accounts all the time.[30]

However, the denial of transactions is not at all limited to suspected fraud and crime; it is often used for political and ideological reasons as well. In other words, it can be used to make you do something you wouldn't voluntarily do, or to stop you from doing something you want to (and are legally allowed to) do. For example, in 2022, PayPal notoriously announced it would start penalizing its users with a $2,500 fine per violation for "spreading misinformation",[31] and in Canada, prime minister Justin Trudeau froze the bank accounts of Canadians

30 https://www.irs.gov/businesses/small-businesses-self-employed/information-about-bank-levies

31 https://jolt.law.harvard.edu/digest/paypals-misinformation-fine-sparks-backlash

who simply exercised their democratic right to protest his government's decisions.[32]

It makes a huge difference whether *most* or *all* of your funds are frozen. Cash cannot be frozen, so if you have some, you can at least cover your most basic necessities while the issue affecting your electronic funds is worked out. However, if you only have electronic funds and they get frozen, blocked, or you lose access to them in some other way (power outage, hacker attack, etc.), you suddenly can't pay at all. The people in Cyprus (an EU member country with the Euro as its official currency) learned this the hard way in 2013, when bank accounts and electronic transfers were suddenly frozen across the entire country for “bank holidays” that lasted 10 days, after which depositors were “bailed in”, meaning substantial amounts of their deposits were gone.[33]

For so-called stablecoins (a new form of digital money), the GENIUS Act, signed into law in July 2025, states in § 3(h)(2) that the Secretary of the Treasury has the authority "to block, restrict, or limit transactions involving payment stablecoins". In fact, per § 4(a)(6) of that act, ***only*** issuers who have the technological capability to allow for the blocking of individual transactions or users, may even issue payment stablecoins.

This feature of stablecoins is already being used to force political agendas and ideology onto users. For example, Circle (the issuer of the USDC stablecoin) prohibited the use of its stablecoin for the purchase of weapons of any kind, including knives, firearms and ammunition.[34]

32 https://www.newsweek.com/banks-have-begun-freezing-accounts-linked-trucker-protest-1680649

33 https://elischolar.library.yale.edu/cgi/viewcontent.cgi?article=1650&context=journal-of-financial-crises

34 https://www.cryptopolitan.com/circle-reverses-anti-gun-usdc-policy/

Keep in mind that all electronic payments you make are recorded. Those records can be accessed (lawfully or illegally), analyzed, and used to draw conclusions.

Note also that you do not have to do anything illegal to get sanctioned. The Canadians who went to Ottawa and had their bank accounts frozen were acting perfectly within the bounds of Canadian law.[35] Their prime minister simply didn't like what they had to say. The purchase of knives, firearms, or ammunition may have gone against Circle's agenda or ideology (or those of Circle's backers), but it is perfectly legal in most places in the United States. Likewise, PayPal's $2,500 fine for saying something PayPal disagreed with did not require breaking any law for the fine to apply either.[36]

You could think of this as first generation behavior modification through digital control of financial transactions. This is already happening and you are potentially at risk of being subjected to it with any use of digital payment systems.

For the time being, however, use of such first generation behavior modification is still a lot more isolated as it either has to happen with very broad strokes (freezing numerous bank accounts is a more severe penalty than limiting some of your transactions) and/or you have alternatives (namely cash). Trudeau's freezing of bank accounts to end protests against his lockdown and vaccination policies led to fears of bank runs as it caused millions of Canadians to lose trust in banks and withdraw their money.[37] Political backlash ultimately caused Circle to modify its terms.[38] Many users dropped PayPal in

35 https://reclaimthenet.org/court-rules-trudeau-freezing-civil-liberties-protesters-bank-accounts-violated-canadas-charter

36 https://www.thefire.org/research-learn/fire-statement-free-speech-and-online-payment-processors

37 https://farmersforum.com/avalanche-of-bank-withdrawals-bank-failures-unlikely-after-ottawa-froze-convoy-supporters-accounts-retired-banker-says/

38 https://www.thestreet.com/crypto/markets/major-crypto-company-lifts-ban-on-gun-purchase

response to the company's policy, and went to competitors.[39] Over time, however, competition tends to make way for larger and larger monopolists, until eventually, few choices, or even just one, remain.

Once cash is no longer an alternative, both a government or a powerful corporation with a key role in the administration of digital payments can roll out the next generation of behavior modification. China's digital yuan gives you a revealing glimpse of what this looks like. With programmable money and no cash, penalties can be automatically administered on a sliding scale, starting with a few inconveniences; if you continue expressing your opinion or not doing what those in power want you to do, the penalties become more severe and ultimately existential. It may start with not being allowed into a restaurant or onto a plane, next you may be denied access to trains or gas, and eventually it may escalate to groceries, utilities, and rent. Being faced with potentially losing their ability to pay at all, most people will ultimately give in, censor themselves and do as they are told, including acting contrary to their values and their conscience.

Physical cash on the other hand, is not subject to electronic control. If you have a $50 bill, you can spend it. The decision whether to accept that transaction or not is between you and the person you are paying. Nobody else.[40]

39 https://www.usatoday.com/story/money/2022/10/13/paypal-misinformation-policy-sparks-backlash-many-users-delete-app/10486413002/

40 Monetary theorists may correctly point out that even with government-issued cash, there is a so-called "third-party-risk", however, this does not change the fact that the decision about a transaction is solely between the two parties engaged in the transaction. The third-party-risk refers to the stability of the currency itself. More on that later. For now, note that this risk also exists with digital currency and electronic payment methods and is irrelevant for the issue discussed here. The unbeatable advantage of cash is that you have both privacy and transaction freedom.

It is crucial to remember that ONLY with a physical, tangible medium of exchange (i.e. cash, or, in theory, barter or physical gold or silver) can you freely transact with another person *without* needing the consent of a third party. ANY electronic or virtual means of transaction can be denied by a third party, who is not even part of the transaction, but can deny *your* ability to transact!

Most people underestimate the grave implications of the fact that every single transaction they perform electronically is forever recorded and that this transaction history can forever be reviewed and conclusions drawn from it. These conclusions may well be inaccurate or misleading. None of the transactions need to be illegal at all. But they may very well get you into trouble one day nevertheless. Remember that the entire cancel culture was based on actions people took a long time (often decades) ago when they were often a completely different person, and when these actions, such as wearing a certain Halloween costume, were often completely innocent, but decades later, were considered scandalous and being used to destroy people's reputations and careers.

With electronic payments, no human being even needs to accuse you of anything; they can simply pull your purchase history, take some things out of context, and have you destroyed in the court of public opinion. AI may even do this automatically. One day, you may be in someone's way, have access to something they want, or just be unlucky and become a suspect for an actual crime that someone else committed.

Every time you pay electronically, you help to normalize the concept that a third party may question or deny your purchases. Why are you purchasing so much meat, tobacco, alcohol, so many eggs, or canned goods? What did you do in this part of town? You took a trip to Las Vegas, do you have a gambling problem? We see that you paid at Planned Parenthood, at a Cannabis dispensary, or at a Bible outlet store... The insurance company of the guy you got into a crash with at 8:12am might

also find your purchase at 4:03am interesting and conclude that the accident was your fault since you did not get enough sleep.

When I worked as a prosecutor, I have seen defendants who got into the crosshairs of the criminal justice system on accident. A particularly extreme case was that of a defendant who happened to be at the wrong place at the wrong time and had the misfortune that misleading evidence made him a prime suspect. Thankfully for him, I questioned a lot more than my colleagues who decided to indict him did, found crucial flaws in the testimony of the main accusing witness and even heard an exculpating witness (whom none of my colleagues during the investigation questioned) and thus it turned out during the trial that he was actually innocent. This was one of the exceptionally rare cases where the prosecution (me, in this case) requested an acquittal (which the judge, who had the same realization, granted). This defendant could have easily been convicted, and almost would have, had a different prosecutor been less attentive that day.

Now imagine you just purchased supplies for some home repair and yard work, say duct tape, a shovel, etc. And a few days later, you happen to buy gas in the vicinity of a crime scene you are not even aware of...

Completely innocent transactions can look suspicious (or be useful) to a person viewing them out of context or even an AI-algorithm scanning them on behalf of a data broker, political opponent, government agency, or cybercriminal.

In parts 8 and 9 of chapter X, we will also see how this data is already lawfully being used against you to decrease your purchasing power. Your hobbies, lifestyle, habits, preferences, diet, health, beliefs, etc. should be your business and not be blasted to the entire world to be exploited, nor become conditional upon third-party approval. However, only with cash do they actually remain private and independent of the consent of payment providers.

VIII. STABILITY OF VALUE IS SECONDARY TO TRANSACTION FREEDOM

If you cannot access what you thought was “your” money, or if your money only works for transactions other than the one you need to make right now (such as buying your plane ticket home, filling up your gas tank to make it back to your loved ones, or paying for something else that you need immediately), then what good is all the theoretical backing of a virtual currency that is inaccessible to you? If a currency is programmable, it can be frozen by an algorithm or AI! And if an algorithm can freeze “your” assets, then are the assets really yours?

Thus, the first question must be about your uncompromised ability to *ALWAYS* be able to access and use your cash, no matter what. Everything else is secondary! This is probably the most important point of this book.[41]

41 Initially, I considered prefacing this book as follows: "Have you ever thought through what it would be like to live as a slave? Yes, a pre-civil war plantation worker in shackles, or a debt-slave in Sparta, working on building stuff for other people until you are no longer physically capable of doing so, at which point you will be tossed off a building to die...
Would you rather live that way (as an actual slave) and know that your currency is stable, i.e. retains its value, OR: live with inflation and be free? Title: How to Avoid Complete Enslavement; Subtitle: (Why cash is crucial).

A common argument against cash is that it is fiat.[42] It is crucial to separate the question of physical cash versus digital currencies from the question of fiat versus gold-standard.[43] These are two completely separate issues and must not be confused.

Physical cash can be precious metal-backed (as the U.S. Dollar was until 1971) or completely fiat. So can any digital currency.

Both precious-metal backed currencies and fiat currencies have their pros and cons,[44] but those are for a completely different

42 Fiat is Latin for "it shall be." A fiat currency (or fiat money) is a currency which is created by banks or governments without being backed by precious metals or other tangible assets. It has no intrinsic value and derives its value solely from the fact that other people agree on its value and will accept it for said value. Simplified, you could call fiat money the opposite of a gold-standard.

43 ...or bimetallic-, or silver-standard, for that matter. For purposes of this book, I will not differentiate between these, although great arguments can be made for a more silver-based currency (as president Grant found out the hard way when he realized that he had demonetized silver in 1873 without knowing it), but as this chapter stresses, the entire question of a fiat currency vs. a currency backed by something is far inferior in importance to the question of physical vs. digital and this book is solely about the far more important latter. The question of what exactly to back a non-fiat currency with is even another rank lower in the priority list of issues regarding sound monetary policy. Quite important nonetheless, but far less important than the ability to always reliably make payments regardless of a third party.

44 There are, in fact, some quite compelling arguments for a fiat currency, believe it, or not, especially one that is *not* debt-based. For example, with a government-issued national fiat currency and sound fiscal policy, you would, in theory, not need any taxes! Imagine that! Yes, you would have inflation, but the inflation would be instead of taxes. Imagine how unbureaucratic and fair that would be! No tax returns, days of paperwork every year, invasive disclosures, etc. Wouldn't that be worth losing some purchasing power every year? The counterargument is, of course, that governments throughout history have eventually always become quite frivolous with their spending, thus debasing the currency too far. This topic deserves its own debate, however. And again, is completely irrelevant if a third party can shut down your ability to pay altogether! If you want to learn more about the topic of money creation and currency debasement, however, watch

debate. If that topic interests you, you should definitely read Professor Richard Werner's book "Princes of the Yen", which does an excellent job explaining the enormous power that comes with a fiat currency and how, if done right, a responsibly administered fiat currency can actually be very beneficial to a society (due to its flexibility and potential for prosperity-creation), and, despite banks' credit creation, does not necessarily have to cause inflation.[45] As Werner explains in a very pleasant to read and easy to understand fashion, Japan did this extremely successfully for decades and then ironically, later also served as a warning for what happens when credit is misallocated or unnecessarily restricted.[46]

While the question of fiat versus finite supply deserves its own discussion, its implications are primarily for economic growth and stability of value. They have no impact whatsoever on your transaction freedom. This book is, therefore, solely about the far more crucial and fateful question of the physical, offline, anonymous ability to transact, free from discrimination or a "third lock"[47], versus digital, programmable, surveillable forms of transaction. It bears reemphasizing that the prospect of a world without a non-digital way to pay may be the most serious threat to human freedom in history.

Mike Maloney's "Hidden Secrets of Money", especially episode four (https://goldsilver.com/hidden-secrets/episode-4/).

45 "Princes of the Yen", by Professor Richard A. Werner, ISBN 978-3-946333-01-2-Paperback, ISBN 978-3-946333-03-6-Hardback

46 And also how control over credit creation is an essential factor of political power.

47 In a physical cash transaction, the purchaser and buyer each have a "lock", i.e. both of them must consent to the transaction for the transaction to take place. In any electronic form of payment, a third party (the payment provider) also has a "lock" - the "third lock". This means that even if the purchaser and seller agree to the transaction (i.e. "open their two locks"), if the third party, e.g. the credit card company, stablecoin issuer, or other payment provider, does not consent (in other words "keeps their lock closed"), the transaction cannot take place. Only with a physical medium of exchange, such as cash, do you only have two "locks".

A precious metal backed digital currency might promise to retain its value, but what good does it do you if you cannot use it because you have been blacklisted, your social credit score has fallen too low, the issuer considers your latest post "misinformation", or a "pandemic" has been declared and you are not allowed to leave your home?

What matters is whether you can pay during a power outage, cyberattack, or when you have fallen from grace because you criticized the government, didn't take a certain vaccine, purchased the wrong products, or because someone stole your password or compromised or froze your account.

Physical cash is crucial for freedom, because it is offline, anonymous and no third party, neither government, nor private company, nor criminal, can turn it off.[48]

Just like sodium content is a completely separate and independent metric from caloric content, the question of value retention should never be conflated with the analog vs. digital question.

Of course, one can debate about whether precious metal backed cash would be even better as it might be more likely to retain value, but it is impossible to overstate how much less significant that criterion is compared to your ability to freely access and use your currency at any time without interference by a third party.

This diagram might help to visualize the contrast:

48 short of doing so for the entire currency altogether.

	Physical currency	Virtual currency
Precious Metal Backed	under your control	under 3rd-party control
	anonymous (you have privacy)	forever stored on a ledger (no privacy)
	immune to power outages	dependent on electricity
	independent of internet	depends on internet connection
	cannot be programmed	can be programmed
	cannot be turned off	can be turned off
	cannot be hacked	can be hacked
	does not expire	can be programmed to expire
	no negative interest rates	negative interest possible
	under your physical control	risk of custodian failure
	under your physical control	subject to remote seizure / confiscation
	retains value (in theory), BUT	may retain value (*if* set up right), BUT
	potential for debasement	subject to debasement and collateral fraud
Fiat	under your control	under 3rd-party control
	anonymous (you have privacy)	forever stored on a ledger (no privacy)
	immune to power outages	dependent on electricity
	independent of internet	depends on internet connection
	cannot be programmed	can be programmed
	cannot be turned off	can be turned off
	cannot be hacked	can be hacked
	does not expire	can be programmed to expire
	no negative interest rates	negative interest possible
	under your physical control	risk of custodian failure & collateral fraud
	under your physical control	subject to remote seizure / confiscation
	loses value (inflation)	loses value (inflation)

More simply put, this means:

	Physical currency	Virtual currency
Precious Metal Backed		
Fiat		

As you can see, the question of precious-metal-backed versus fiat currency is completely irrelevant for the way more fateful question of freedom versus slavery. What matters for the latter is solely the question of physical versus virtual.

Given that the primary purpose of a currency is to serve as a medium of exchange, the task of value retention does not

necessarily have to be accomplished by the currency itself. To store value, you can put your money into value-retaining assets, such as land, precious metals, or other investments, or invest in your own or your friends' businesses.[49]

Where you get into trouble is when you try to make a currency a store of value and neglect privacy and anonymity. Without anonymity, there can be no freedom. And nothing digital will ever fully be, let alone remain, anonymous, especially if you are trying to have it widely accepted as a means of payment. While you may achieve some relative or temporary privacy with the use of tools such as VPNs or Tor, you can pretty much count on powerful governments having a way to ultimately identify you if they care enough.

If you want to pay for anything in the real, physical world, you need a medium that is universally accepted, such as legal tender. Even if it were possible to design a digital system that allowed for anonymity from a technical standpoint, governments will not let this become a permitted form of payment. The laws governing digital forms of payment in Western countries always come with know-your-customer (KYC) requirements, so with surveillance becoming ever more complete, it is unlikely that someone would be able to get away with breaking laws the government actually cares about, such as the ones governing money, for long. Moreover, if a government declares a means of payment illegal, most vendors won't accept it.

Consequently, nothing digital will ever be able to provide you the privacy and freedom offered by physical, tangible means of transaction. Thus, if you care about human autonomy and do not want governments and private corporations to be able to micromanage every small aspect of your life, the highest priority should be that money remains physical. If you can find people willing to transact in physical gold and silver, great! If you can convince a government to mint its coins from precious

49 Note: this book is not an investment guide or investment advice.

metals again and make their notes convertible to gold or silver again, more power to you. But any digital-only payment system ultimately leads to your enslavement, whether it is backed by some asset or not.

www.preservecash.org v.1.1

www.preservecash.org v.1.1

IX. CONVENIENCE

Most threats to freedom initially are marketed as "conveniences." For example, people used to be able to leave their work at work, but then cellphones became ubiquitous and work started encroaching on at-home time. In autocratic countries, such as the former East Germany, the government not that long ago needed to have agents break into your home and install microphones behind light switches and outlets to listen to you;[50] now, people pay for the "convenience" of being listened to. Some people even buy wearables or smart-home devices that listen to their every conversation and then are shocked when the most intimate details of their conversations become public record in court.

Alternatives to cash are no exception. Swiping a credit card (or even worse: tapping a phone), may seem convenient as long as you haven't experienced the very dark flipside, such as having your account hacked, having your transaction record used against you, or being unable to pay because your transaction is declined and you have no alternative (because cash is no longer accepted), to name only a few examples. Remember that having a cellphone or an email account was optional and even rare not that long ago. The problems arise once you are *expected* to use the once optional innovation and the alternatives go away. Try getting a human on the phone or

50 If you want to get an idea of how even people loyal to the regime could arbitrarily find themselves in the crosshairs of the government in East Germany and have their lives ruined, watch the movie "The Lives of Others" (original title: "Das Leben der Anderen"). You will never use the phrase "I have nothing to hide" again, as having something to hide is not even the criterion. Keep in mind that East Germany called itself "democratic" as well.

living without an email address these days, or finding a payphone...

Just as stability of value does not matter without freedom, convenience does not either. Life in a prison is, in a way, quite convenient: food is provided for, utilities are taken care of, and the days have a structure that is clear and strict. However, you are also subject to arbitrary punishment and violence and have no freedom at all.

An all-encompassing digital payment system might be "convenient" in some ways (that is, until you get hacked, lose your device, don't have power, don't have a stable internet connection, or have your ability to pay suspended), but daily life will be a lot like it is in China, where people are subject to blacklists and are already living this reality. And don't you dare to speak out or fail to do what those who control the algorithms want, or you will feel the consequences quickly!

Further, should cash ever disappear, so will a lot of the convenience you may currently experience with electronic payments. You can expect the frequency of transaction denials based on some AI system finding something about it questionable to increase and the difficulty to get the problem resolved as well.[51] We will go more into the details and reasons in part 12 of chapter X. As long as cash is still an option, few people would put up with days of frustration, answering a million questions and dealing with dozens of passwords and authentications in order to regain access to their electronic payment method. Such an experience would push most people back to cash, which is immune from such nonsense. Without cash, you are locked in; and suddenly, cash will feel a lot more convenient. That's when people will start to really miss cash and regret they didn't use it more when they still could.

51 See Footnote 28.

X. SECONDARY REASONS TO USE CASH INSTEAD OF ELECTRONIC PAYMENTS

Human freedom should, in and of itself, be more than enough reason to use cash. It is certainly the most existential and consequential one. Nevertheless, there are many more reasons to do so. For example, cash is a bulwark against power and internet disruptions, cyberattacks, debanking, fraud, unmindful spending, fees, negative interest rates, surveillance pricing, quishing (scams and malware attacks using QR codes), threats buried in terms and conditions, annoying and deteriorating user experience, discrimination/exclusion and growing financial illiteracy. Cash is also a great way to support local businesses and small farms, keep money in your community and allow the next generation to learn financial literacy. Finally, using cash is good manners. Let's go through those one by one:

1. Resilience against Disruptions

Any electronic means of payment is obviously dependent on power and a stable internet connection. The residents of North Carolina and East Tennessee learned this the hard way when, during Hurricane Helene, the Federal Emergency Management Agency (FEMA) infamously handed out credit cards - in an area that had no power! This occurrence actually motivated key decisionmakers in Sweden and Norway, two of the most cashless countries in the Western world, to think about ways to encourage their citizens to use more cash again, in order to harden their countries against disasters and ensure the ability to pay when there is no power.

Even without a disaster, servers crash, glitch and get hacked all the time. IT issues you are not even aware of can suddenly cause your electronic payment method to fail. With cash, there is no such dependency.

The example of the Eastern Caribbean Central Bank's (ECCB's) DCash shows that IT issues are a very real scenario. Its name notwithstanding, DCash is not cash but a Central Bank Digital Currency (CBDC) launched with the promise of being a “faster, cheaper and safer payment option to physical cash and other payment channels."[52] In early January 2022, after it had been adopted by eight countries, DCash suddenly and without warning stopped working; payments were declined, and funds in DCash were inaccessible.[53] As it eventually turned out, the certificate of the Hyperledger Fabric hosting the DCash ledger had expired. It took over two months for this CBDC to come back online.[54] Imagine being without any ability to pay for anything for two months!

This happened to the ECCB, an international central bank in the Americas. If you still doubt that a large-scale disruption like this could happen in the West and potentially affect something as critical as banking, remember the CrowdStrike update glitch in July 2024, which grounded flights around the world and affected governments and businesses across practically all sectors, including emergency services and, yes, banks. As NPR reported:

> "A technological meltdown left employees of airlines, banks, hospitals and emergency services around the world staring at the dreaded 'blue screen of death' on

52 https://www.eccb-centralbank.org/blogs/the-eccb-s-digital-currency-dcash-is-a-critical-step-in-the-buildout-of-a-digital-economy-in-the-eccu

53 https://www.eccb-centralbank.org/news/region-wide-service-interruption-of-dcash-platform

54 https://www.caymancompass.com/2023/02/16/caribbeans-central-bank-digital-currency-experiments-slow-to-take-off/

> Friday as their computers went inert in what is being described as a historic outage."[55]

When an AT&T server building was severely damaged on Christmas 2020 due to a bomb in a vehicle parked in front of the building, millions of people across the southeastern United States lost their ability to communicate electronically. Stores across three states went cash only[56] without warning,[57] as electronic payments were impossible.[58] In some areas, it took several days for electronic payment systems to be available again.[59]

In February 2021, Winter Storm Uri did serious damage to the Texas electricity grid and left 4.5 million homes and businesses across four states without electricity, some for several days.[60] On January 7, 2026, activists intentionally sabotaged a power station in Berlin, Germany, leaving thousands of businesses and tens of thousands of households without electricity for several days.[61] A few weeks later, an ice storm hit the southern United States, causing loss of electricity in several states affecting tens of thousands, in some states even hundreds of thousands.[62] It took over two weeks for power to be fully restored.[63]

55 https://www.npr.org/2024/07/19/g-s1-12222/microsoft-outage-banks-airlines-broadcasters
56 https://www.wkrn.com/news/local-news/cash-only-walmart-says-some-stores-affected-by-att-outage-from-nashville-explosion/
57 https://www.nytimes.com/2020/12/29/us/nashville-bombing-telecommunications.html
58 https://www.dallasnews.com/business/local-companies/2020/12/31/the-nashville-bombing-put-a-spotlight-on-atts-network-vulnerabilities/
59 https://en.wikipedia.org/wiki/2020_Nashville_bombing#cite_note-32
60 https://en.wikipedia.org/wiki/2021_Texas_power_crisis
61 https://www.reuters.com/business/energy/berlin-restore-power-after-arson-attack-causes-record-outage-2026-01-07/
62 https://en.wikipedia.org/wiki/January_23%E2%80%9327,_2026_North_American_winter_storm#Southwest_2
63 https://newschannel9.com/newsletter-daily/nes-says-power-restoration-on-track-for-as-frustration-grows-among-customers-lawmakers-winter-

Disruptions and disasters can come in many forms at any time, for many reasons and usually do so without warning. Still being able to buy necessities or pay for transportation makes a huge difference when you find yourself in such a situation. Just as you should always wear a seatbelt, as you don't know in advance when you will get into an accident, you should ***always*** carry cash as you will not get advance notice of an internet or power outage. The same way one usually can't sign up for insurance to cover an accident after it has happened, you may not be able to get cash from an ATM during an internet or power outage. So make sure you're never without it.

On a societal scale, cash can mean the difference between inconvenience and complete societal breakdown. Not being able to pay for necessities causes desperation, which often leads to a spike in crime and can cause civil unrest. Events in Nigeria in 2023 showed that abolishing cash can easily trigger ugly situations and cost many lives.[64] It is, therefore, in the interest of public safety to keep and preserve physical cash, helping to ensure that disruptions in utilities like power or internet won't escalate into mayhem.

2. Resilience against Cyberattacks

Aside from accidents and disasters, electronic means of payment, as well as *any* digital assets, are also vulnerable to bad actors, looking for an opportunity to steal people's digital wealth. With cash, you may lose the money in your wallet, i.e. the amount you have on you that moment, but if someone manages to hack your account, gets access to your crypto-wallet or steals your identity, that person can take *everything* virtual from you.

storm-nashville-tennessee-power-outages

64 https://www.coindesk.com/policy/2023/02/24/why-nigerians-arent-turning-to-the-enaira-despite-crippling-cash-shortages

Since electronic "money" consists simply of electronic database entries, if those entries change, so does your wealth. This danger is very real and threatening *anything* electronic!

Once you become the victim of a cybercrime, the damage is usually irreversible. Your chances of the criminal getting caught and you getting your assets back are actually way higher in the case of in-person crimes, such as someone stealing your physical belongings,[65] than in the case of someone taking your digital assets.

FBI anti-cybercrime pioneer Scott Augenbaum says that through the thousands of cybercrime cases he worked on, he noticed a pattern he now calls The Four Truths:

1. Nobody expects to become a victim.
2. You're probably not getting your money back.
3. The bad guys probably aren't getting arrested.
4. A majority of cybercrime can be prevented.[66]

If a cybercriminal manages to get access to your account, or if a server glitch or other IT issue causes your account to be wiped or frozen on accident, all the "money" you thought you had in your account won't help you to pay your bills, buy gas, food or a ticket home. Keep in mind that this can happen due to someone else's mistake which is completely out of your control. This is the sobering caveat to Augenbaum's fourth truth. If a third party has your data and is careless in its protection of it (e.g. an employee at a corporation which has your data, such as your payment provider or a cloud storage service), a cybercriminal may obtain all the information needed to harm you, without any negligence on your part at all. Think of how often you hear about data breaches...

65 and they aren't too encouraging even then.

66 "The Secret to Cybersecurity", by Scott E. Augenbaum, published by Forefront Books, 2019. ISBN 978-1-948-67708-0

For example, Chinese hackers managed to get access to the U.S. federal government's databases storing personal information of millions of Americans, including their social security numbers and biometric information, such as fingerprints.[67] If you use biometric information to log into your device or to make payments, keep in mind that a hacker with access to this information can access anything you thought protected with your biometric information. Worse, you won't ever be able to change that information! In a well-publicized data breach, hackers were able to compromise the private records of 147.9 million (!) Americans by gaining access to the database of American credit bureau Equifax[68] - a gold mine for identity thieves and potentially a ticking time bomb for the electronic assets of anyone with an American credit history! About a year ago, Chinese hackers gained remote access to workstations at the U.S. Treasury Department.[69]

It is fair to say that these well publicized high-profile data breaches are only the tip of the iceberg, as the companies affected have an interest in staying quiet about them to avoid the bad publicity and legal liability. And yet, any of those could give a cybercriminal the ability to empty your accounts and lock you out of your electronic payment systems. This may happen tomorrow, in a couple of years, or never, but chances are it will hit you by surprise and without warning. If you rely solely on electronic payment methods, you now have a serious problem.

Cash, that you already have, will make a world of difference in such a situation, until you and your financial institution (hopefully) figure out what happened and how to resolve it (keep truth #2 in mind, though).

67 https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach#Theft_of_fingerprints
68 https://en.wikipedia.org/wiki/2017_Equifax_data_breach
69 https://apnews.com/article/china-hacking-treasury-department-8942106afabeac96010057e05c67c9d5

As far as the dangers of bad actors getting access to the programmability of your money are concerned, we are largely in uncharted territory, given that programmable money is a brand-new phenomenon, and it is therefore hard to estimate the exact potential for blackmail, coercion, ransomware attacks, etc. However, as Augenbaum points out, while the money spent on cybersecurity and fighting cybercrime grows year after year, the damage caused by cybercrime grows even faster.

Criminals love new tools as much as anyone else does and will use them to further their own goals. The ability to program money itself (as in the case of stablecoins, CBDCs and cryptocurrencies) offers unprecedented potential for blackmail and extortion. Think of a hacked "smart contract" which automatically moves your money out of your control the second you receive it! Or ransomware affecting your ability to perform certain transactions or siphoning off part of every transaction you make.

Any ability the government has in regards to programmability can always potentially be exploited by any other party with knowledge of and access to it as well. Your nightmare is, of course, a cybercriminal's dream. And most of us are asleep.

The silver lining and the simple truth is: physical cash cannot be hacked, anything digital can.

3. Resilience against Debanking

Debanking for ideological reasons has become an increasing problem in recent years, which ultimately led state legislators, such as Senator Erin Grall and Representative Bob Rommel in Florida[70], and Senator Jack Johnson and Representative Jason

70 https://laws.flrules.org/2023/28

Zachary in Tennessee[71] to enact legislation to offer bank customers protection against this practice.[72]

As of the writing of this book, there is no federal law in effect, offering comparable protection to that of Florida or Tennessee.[73] This means that if you live in a state that has not passed a similar law, you continue to be at risk of finding yourself without the ability to cut checks or issue electronic payments, including using your debit or credit cards.[74] Americans who have been vocal about their political opinions have in recent years increasingly found themselves without access to critical banking services for the sole reason that they espoused political beliefs which differed from those of powerful decision makers in corporate headquarters. Even the President of the United States, as well as several of his family members have found their credit cards denied, their accounts canceled and themselves blacklisted from opening a bank account with about a dozen financial institutions.[75]

In other countries, the situation is even more dire: hundreds of thousands are debanked in the United Kingdom every year and the recent trend shows a concerning increase.[76] A high-profile example was Nigel Farage, a British opposition politician who had his bank accounts terminated without being given a reason and was refused a bank account by seven more banks in the

71 https://solari.com/hero-of-the-week-may-13-2024-tennessee-senator-jack-johnson-and-representative-jason-zachary/
72 https://publications.tnsosfiles.com/acts/113/pub/pc0746.pdf
73 Although President Trump issued executive order 14331 on August 7, 2025, which reverses the course of the previous administration and "Operation Chokehold". The order does offer some protection within the scope of the President's executive authority; however, this authority is limited compared to that of Congress and an executive order can be reversed by the next president with the stroke of a pen.
74 https://web.archive.org/web/20251011224557/https://www.mountainstatespolicy.org/debanking-needs-a-federal-solution
75 https://treasury.ms.gov/2025/08/15/the-destruction-of-debanking/
76 https://www.telegraph.co.uk/money/banking/half-million-customers-debanked-avoid-expensive-payouts/

UK. He later obtained a report from his bank which indicated that his political views were considered.[77]

In Thailand, over 3 million Thai citizens woke up to find their bank accounts frozen.[78] Vietnam didn't even bother to freeze bank accounts, it gave its citizens and businesses two months to submit to a biometric surveillance system, which, aside from the privacy problems, is an impossibility for many, or face losing their bank accounts altogether.[79] According to the Central Bank of Vietnam, 154 million bank accounts were deleted as of October 2025.[80]

Cash gives you a simple way to continue to pay your bills and make everyday purchases, even if your bank does not like what you say, do, believe, or whom you vote for. Political debanking should also serve as a chilling reminder that control over your money *is* (and thus *will* be) abused, not just by governments, but also by private entities to force their own beliefs onto you.

4. Fraud

Some people carry no or almost no cash with them out of fear of getting robbed or losing their wallet. For that same reason, however, it is actually a lot more prudent not to take credit cards with you and not have any contactless payment method with you either. As we are about to see, the risk of becoming a crime victim is actually lower with cash these days than with electronic payment methods.

For one, contactless payment methods can be read out by bad actors, standing in line behind you or otherwise walking

77 https://www.bbc.com/news/articles/czx79161e2wo
78 https://www.binance.com/en/square/post/32916944571050
79 https://www.sebsauerborn.com/insights-english/vietnam-thailand-banking-control
80 https://en.vneconomy.vn/some-154-million-bank-accounts-cleaned-and-569-million-in-suspicious-transactions-blocked.htm

closely past you.[81] This is often referred to as "Ghost Tapping." You won't even know it happened until one day you find fraudulent charges on your account (assuming you even notice - if you use your credit card a lot, you may easily miss a random unauthorized payment among the many transactions you initiated yourself). For criminals, the likelihood of success with this new method is a lot higher, the stakes dramatically lower, and the risk of getting caught substantially smaller as well, which is why incidents of Ghost Tapping are exploding,[82] while robbery rates have fallen over 70% during the last few decades, one of the steepest declines of any crime type.[83]

Secondly, if a vendor accidentally or intentionally charges you the wrong amount, you are a lot less likely to notice if you simply tap or insert a credit card (or your phone). In this scenario, you actually authorized the transaction (even though you thought it was for a different amount), which dramatically reduces your chances of your payment provider reimbursing you.[84] Scams exploiting these vulnerabilities of "tap to pay" have increased so much[8586] that some banks are now openly warning to think twice before using this payment method and if you do, to ensure not to be distracted at all while you are authorizing the payment[87] (something that is almost impossible to ensure 100% in today's world full of distractions). If you pay with cash instead, you are inevitably aware of exactly how

81 https://www.fox7austin.com/news/bbb-warns-ghost-tapping-scam-which-triggers-contactless-charges-through-tap-to-pay
82 https://www.consumeraffairs.com/news/tap-to-pay-ghost-tapping-scams-are-rising-heres-how-to-protect-yourself-040926.html
83 https://www.opencrime.us/robbery-statistics
84 https://www.gao.gov/blog/if-youre-victim-payment-scam-does-your-bank-have-help
85 https://www.usatoday.com/story/money/personalfinance/2026/07/30/tap-to-pay-scam-checklist/91099280007/
86 https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf
87 https://www.bankofireland.com/about-bank-of-ireland/press-releases/2026/think-before-you-tap-bank-of-ireland-warns-consumers-about-card-payment-overcharging-scams/

much you are paying as you have to hand over physical notes and/or coins.

Thirdly, whenever you lose, have to cancel, or replace, a credit card, you spend a lot of time, calling your bank/credit card company and all the companies you use it with (e.g. for automatic payments) updating your information. You have to wait for several days to receive the new card, don't have one in the meantime etc. And you may want to ask yourself: how much is your time worth? Additionally, you may come to find that getting reimbursed for that fraudulent charge may not be as easy as you thought.[88]

Anytime you provide your payment information to a new merchant, this crucial data lands in more hands. And the more people have this information, the more people may get tempted to use it fraudulently or become victim of a data breach. Any waiter walking away with your credit card can write down your card info for herself. Any database this information gets added to can get hacked. This danger is not theoretical: the European Association for Secure Transactions (EAST), for example has tracked a 1,500% surge in relay-based attacks exploiting the transmission of electronic payment information which cybercriminals then use to create illegitimate charges to credit cards and other electronic payment methods.[89] Thus, every time you pay electronically, you increase your chances of becoming the victim of fraud.

If you install payment apps on your phone, you are exposing yourself to a whole new dimension of risks altogether: In addition to the already mentioned risks of Ghost Tapping, you are both allowing the payment app to have access to all the intimate data on your phone, and vice versa, exposing the payment app to a myriad of IT-security risks posed by every

88 https://www.bankrate.com/credit-cards/advice/bank-refuses-fraudulent-charge-refund/

89 https://www.inetco.com/ghost-tap-phantomcard-the-haunted-frontier-of-fraud/

single other app installed on your phone. It should thus come as no surprise that malware infecting smartphones to exploit payment apps is on the rise.[90] Malware can infect your phone through a malicious or corrupted website you visit, a link you click on (especially in an email), an app you download, or even a QR code you scan (as we are going to explore in more detail later).

Uninstalling payment apps from your phone, leaving your credit cards at home, and only taking cash with you, is the safest way to protect yourself against all the just mentioned ways of becoming a victim.

5. Saving Money

Did you ever notice how spending physical cash feels differently from swiping a card or tapping a phone? When you pay with cash, you can sense the cost of something. If you spend a lot, it can almost feel a bit exhausting. In any case, you are aware that and how much you spend. Spending $180 feels very different from spending $10. With electronic payments, that feeling is barely noticeable or nonexistent. As neurological studies confirm, a swipe or tap feels the same, whether it is for three dollars or three thousand dollars, while handing over a larger amount of cash feels very different from a smaller amount.[91]

Some people, who have gotten very used to paying everything electronically, claim the opposite: that when they have cash, they spend it right away and more carelessly. However, there is a mind-trick behind this: the reason is the lack of value appreciation they associate with the paper (or metal) money as a result of changed habits, and their habit to dispose of it at the earliest convenience. If that is you: consciously only pay cash

90 https://www.infosecurity-magazine.com/news/ghost-tap-malware-remote-nfc-fraud/

91 https://pmc.ncbi.nlm.nih.gov/articles/PMC6856651/

for a few weeks and you will notice a complete reversal in your perception (which will save you a lot of money).

It thus comes as no surprise that decades of studies[92] have found consumers spend more when they pay cashless.[93] In fact, this emotional connection is so real that, as studies have shown, people who pay cash even feel better about their purchase afterwards than people who pay electronically.[94] No wonder money expert Dave Ramsey keeps encouraging people to get rid of their credit cards and use cash instead.[95]

If you pay cash, you are also more likely to catch if you are being charged more at checkout than if you just tap your phone or swipe a card. Several corporations have become very creative in finding ways to lure customers into a buying decision and then charging them more in the end, including through deceptive tactics such as "drip pricing", where substantial hidden fees and extra charges are added to the originally advertised price.[96] When you pay with cash, you have a final conscious confirmation in the end of how much you are actually spending.

This awareness can also cause more customers to reject such rip-off methods and thereby cause businesses to rethink their practices and be more honest with their customers.

6. Fees

Companies offering electronic payments, such as credit card companies, generally charge fees to finance their services and make a profit. To the consumer, these fees are usually hidden,

92 https://www.sciencedirect.com/science/article/pii/S0022435924000216
93 https://www.apa.org/pubs/journals/releases/xap143213.pdf
94 https://academic.oup.com/jcr/article-abstract/42/5/688/1857957?redirectedFrom=fulltext&login=false
95 https://www.ramseysolutions.com/debt/cash-vs-credit-card
96 https://groundworkcollaborative.org/work/nickel-and-dimed-by-design-how-corporations-rig-the-rules-of-pricing/

as they are charged to the vendor instead. This is the reason why some vendors offer cash-discounts. Given how much some electronic payment providers charge them, it makes perfect economic sense both for them and for the customer to use cash instead.

This is at the same time also the limiting factor to electronic payment providers' ability to to raise their fees. If they raise their fees too high, more vendors will offer more incentives to customers to pay cash, or even stop accepting certain means of electronic payment altogether. Cash thus acts as a way to keep fees charged by payment providers in check.

Without cash, the ability to extract higher transaction fees increases. This could easily accelerate inflation as vendors will be forced to pass these higher fees on to customers, especially since, without cash, they no longer have an alternative to steer customers to.

7. Negative Interest Rates

Negative interest rates are another aspect which most consumers have never considered, thanks to the prevalence of cash in the Western world. In fact, cash is the single reason, banks have not charged retail customers negative interest rates, i.e. penalized them for leaving money in a bank account.[97] The reason is simple: if a bank would decide to do so, its customers would quickly withdraw most of their deposits rather than watch them shrink. As a result, the bank would soon face serious liquidity problems. However, once customers can no longer withdraw their money, all banks have to do is simply to agree to charge negative interest rates industrywide and customers have no escape left (not to mention that many people only have one bank account and opening another bank account is a lot more work than simply withdrawing money).

97 https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200826~77ce66626c.en.html

The European Central Bank (ECB) proved this point when it adopted negative interest rates in 2014. It did so very cautiously and closely watched what happened. The results were clear: except for large corporate accounts, where banks made the calculation that substantial conversion into physical cash would be impractical for the corporate customer, negative interest rates were hardly passed on to the customer. Despite the ECB charging banks negative interest rates, retail banks by and large did not pass negative interest rates on to retail customers, as holding physical cash would then have become more attractive to customers, rather than giving their money to the bank. The ECB took notice and also realized that this fact put a serious limit to the viability and sustainability of negative interest rates, as well as to how far it could raise them.[98] It should come as no surprise that the ECB has become a vocal proponent of digital money (specifically the "Digital Euro", a classic CBDC) as a result. With a CBDC, negative interest can be directly applied to your money itself.

8. Surveillance Pricing

We still take for granted that we see a price tag in a store and we all pay the same for the same product. However, the ubiquity of smartphones and increasing use of digital payment methods has led some stores to implement a new way to skim some extra dollars out of their customers: based on what the company knows about you, they will calculate the maximum price their algorithm understands you will pay.[99] The more data you allow them to have about you, the more expensive their products will become for you. And their algorithms become ever more accurate to charge you exactly what you *will* pay, i.e. as much as they can without you walking away.[100]

98 https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200826~77ce66626c.en.html

99 https://www.yahoo.com/news/surveillance-pricing-retailers-may-track-195735551.html

100 https://jacobin.com/2024/07/surveillance-personalized-pricing-data-collection

If you shop online, there is a significant chance you are already charged a different price than another person buying the very same item from the very same store. A study conducted by nonprofit groups Groundwork Collaborative, Consumer Reports, and More Perfect Union involving shoppers viewing Instacart prices found that “Some shoppers found grocery prices that were up to 23% higher than prices available to other shoppers for the exact same items, in the exact same store, at the exact same time".[101]

This concept is not entirely new: airlines have notoriously charged customers very different prices for tickets on the same flight. If you checked the price for a particular flight, and then checked that price again a few hours later, they would quote you a higher price as they understood that you likely had made the decision to book in the meantime and would begrudgingly accept paying more now.

Tech companies that require you to install an app in one of your most private places, i.e. your phone, which has all your most personal information, have access to disturbingly detailed information about you and don't shy away from using it to get more money out of you. For example, Uber has figured out that users are willing to pay more if their phone's battery is low. Unlike traditional taxis, for which you can pay with cash, app-based rideshare companies have constant real-time access to your phone's information, including, but nowhere near limited to, battery charge percentage, and will charge you different prices depending on how much they know you are willing to pay.[102]

On the other hand, we are used to all paying the same in a brick-and-mortar business. Even if discounts were available,

101 https://www.reuters.com/legal/litigation/ftc-investigating-instacarts-ai-pricing-tool-source-says-2025-12-17/

102 https://www.forbes.com/sites/amitchowdhry/2016/05/25/uber-low-battery/

such as coupons, happy hours, sales, or loyalty programs, those would usually apply to all customers using them identically as well. However, if you install an app on your phone to receive such perks, you also allow the company to see and evaluate your most intimate habits and preferences, including location and browsing history, payment apps, device ID, make, and model, contacts, call and text history, social media, other apps you installed, etc. This enables them to know you better than you know yourself.[103] Don't be surprised if they will use this data to get the maximum amount of money out of you; after all, that's the very business they are in. The incentives you receive via an app are thus highly targeted and very different from the ones somebody else will receive. Hence, it will be them making more money on you, not you saving money when shopping with them.[104]

The willingness of many shoppers to install bulky, invasive apps on their smartphones for shopping purposes has led some retail chains, such as Walmart[105] to remove price tags from their products and require customers to install an app[106] to see prices.[107] Don't be surprised if these prices keep changing for you as a result![108] The Leadership Center for Attorney General Studies has recently warned about the potential for, and dangers of dynamic pricing in retail stores and called on Attorneys General in the United States to protect consumers against this practice.[109] Furious customers of major retail chains are now reporting that exactly what AG Studies has been warning about is happening at a number of retailers and

103 https://www.judiciary.senate.gov/committee-activity/hearings/your-data-their-profit-the-consumer-cost-of-ai-surveillance-pricing
104 https://www.rd.com/article/problems-with-loyalty-apps/
105 https://www.the-sun.com/money/15086246/walmart-confirms-new-price-policy-shopper/
106 https://www.reddit.com/r/mildlyinfuriating/comments/1pw8h87/i_am_not_about_to_download_a_store_app_just_to/
107 https://www.themarysue.com/walmart-forcing-app-customers/
108 https://www.themarysue.com/walmart-dynamic-pricing/
109 https://agstudies.org/publications/digital-price-tags-and-watching-eyes-retail-techs-impact-on-your-wallet-and-privacy/

that people will get charged differently, down to the price of groceries or socks, based on, for example, what brand and model of phone they use.[110]

Some state legislators are laudably trying to address the issue of surveillance pricing,[111] such as Representatives Karen Camper and John-Ray Clemmons and Senators Paul Bailey and London Lamar in Tennessee (unfortunately their bills did not become law, however, thus leaving Tennesseans unprotected against this predatory practice).[112][113] As of the writing of this book, Maryland[114] and Connecticut[115] are the only states that have enacted laws against surveillance pricing (although several have introduced similar bills). If you live in a state without such legal protection, the most powerful means to stop digital abuses such as surveillance pricing, is customers walking away, deleting their apps and only paying cash.[116] If the companies you do business with know everything about you and will adjust their prices based on how badly you want their product or service and how much you can afford, it may at some point become futile to look for a better job or work hard for a raise, as every extra dollar you make will be taken from you through surveillance pricing and every purchase will leave you with the uneasy question whether you paid more than your friends and colleagues.[117]

110 https://nypost.com/2026/07/11/lifestyle/how-companies-use-your-data-to-charge-you-more/
111 https://innovation.consumerreports.org/How-U.S.-States-are-Tackling-Algorithmic-Pricing.pdf
112 https://wapp.capitol.tn.gov/apps/BillInfo/Default?BillNumber=HB1468&GA=114
113 https://wapp.capitol.tn.gov/apps/BillInfo/Default?BillNumber=SB1998&GA=114
114 https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0895?ys=2026RS
115 https://cga.ct.gov/2026/ACT/PA/PDF/2026PA-00130-R00HB-05563-PA.PDF
116 https://cybernews.com/privacy/walmart-shoes-surveillance-pricing-ai/
117 https://jacobin.com/2024/07/surveillance-personalized-pricing-data-collection

It is up to you whether you support this trend by downloading an app and paying electronically, or whether you take your business to a store or restaurant that respects your privacy, accepts cash, and is honest and transparent about its pricing. Note that if you pay with anything other than cash, you are providing valuable data about yourself to a number of entities beyond just the store or restaurant you are paying at, which will be used by third parties to add even more granular information about you, your habits, and preferences to your profile, which you probably don't even realize exists.

As U.S. Senate Judiciary Committee Chairman Josh Hawley pointed out in an August 4th 2026 hearing on surveillance pricing:

> "Did you know that your neighborhood grocery store is amassing your data and tracking your purchases, all for their profit? For example: take Kroger. Kroger is not just a grocery store [...] it is a data-selling mega-corporation. [...] One Kroger customer got a copy of his shopping profile recently; do you want to guess how long it was? 62 pages! 62 pages of personalized data on this one person based on his shopping history. Last year, Kroger earned over $500 million from selling, yes selling the data that it harvests from its loyal customers and giving it to other corporations."[118]

As a complaint issued by the Federal Trade Commission shows, data brokers analyzing and selling your information use their access to "harvest consumer information and sensitive location data - including visits to health clinics and places of worship" and then sell the data "to third parties to be used for targeting advertisements and other purposes."[119]

118 https://www.c-span.org/classroom/document/?26482

119 https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2025/01/surveillance-pricing-update-work-ahead

Just as in court anything you say can and will be used against you, expect the same to happen with any data you give away about yourself. After all, the developers programming these algorithms and the companies running the data centers storing and analyzing all this information about you, are in the business of making money themselves. And they do so by selling someone an unfair advantage over you. This could include someone intentionally embarrassing you,[120] using your data against you in court,[121] or an insurance company raising your premiums or denying your claim or coverage altogether.[122]

Aside from companies purchasing and collecting information about you to manipulate you and make you part with your money, the larger of a data footprint you leave, the easier you also make the life of criminals waiting to scam, extort or impersonate you. The simplest, and ultimately the only reliable way to reduce your exposure to this risk is to appreciate the value which your data has (the companies and criminals going out of their way to obtain it are *very* well aware of its value), and guard it accordingly. Ideally by not unnecessarily sharing it to begin with, as, once it is out there, it is often a matter of time until criminals get access to it as well,[123] as countless data breaches remind us all the time.[124] As the electronics review Tom's Guide advises: "Reduce your digital footprint so it can't be used against you"![125]

120 https://www.mirror.co.uk/lifestyle/neighbours-doorbell-camera-caught-embarrassing-37576902
121 https://www.restonyc.com/can-alexa-recordings-be-used-in-court/
122 https://legaldesire.com/health-app-data-in-court-the-terrifying-truth-about-insurance-evidence-and-your-privacy/
123 https://www.cnet.com/news/privacy/thousands-of-ring-owners-had-personal-info-exposed-in-data-leak-report-says/
124 https://www.digitalcameraworld.com/cameras/security-cameras/after-that-viral-warning-did-your-ring-camera-actually-get-hacked
125 https://www.tomsguide.com/computing/online-security/scammers-are-now-using-your-data-to-craft-personalized-attacks-heres-how-you-can-fight-back

9. Surveillance Wages

Determining exactly how much they can charge you before you walk away is not the only way data-hungry corporations use your electronic payment history against you, however. Some companies are now even determining how much (or rather: how little) to pay you based on where, when, how often, what for, and for how much you tap your phone or credit card.[126]

Prospective employees who have credit card debt or make certain purchases end up receiving less pay for the very same work. The reason is that their employer, or some tech-company whose services the employer uses, can see your electronic payment history and determine if you might be more desperate to take the job than someone else.

For people who compete for each shift or gig assignment with other prospective workers, personalized pay often even gets adjusted for each assignment.[127] However, thanks to the widespread availability to your electronic payment history and the increasing prevalence of AI-companies using your electronic payments and other data they can obtain about you, the phenomenon of surveillance wages is no longer limited to app-based employment.[128]

So ironically, if you have to pay for a large expense (or a number of smaller ones) and you use your credit card or payment app to do so, you may end up earning even less afterward. If you end up carrying a balance on your credit card, it may now take you a lot longer to pay off that debt.

126 https://www.marketwatch.com/story/employers-are-using-your-personal-data-to-figure-out-the-lowest-salary-youll-accept-c2b968fb
127 https://rooseveltinstitute.org/publications/uber-for-nursing/
128 https://equitablegrowth.org/how-artificial-intelligence-uncouples-hard-work-from-fair-wages-through-surveillance-pay-practices-and-how-to-fix-it/

Paying with cash and being protective of your data and your privacy can literally keep you from going broke or becoming part of the "working poor."

10. Quishing

Scammers and other criminals have noticed the growing prevalence of QR codes as well. Most people who are willing to scan a QR code don't think twice about the risk they expose themselves to by doing so. Aside from the nauseating amount of intimate data you reveal about yourself by scanning one,[129] which third parties are then often legally allowed to use and sell, criminals love getting your data as well. And they have figured out a variety of ways to do so whenever you scan a QR code:

One common method, and one of the simplest ways of doing so, is by replacing the QR code you are scanning. For example by switching out the sign, menu or sticker people are going to scan, or putting up a fraudulent QR code sign, menu, sticker, etc. to begin with, without the legitimate owner being aware. Also popular is the method of putting a sticker with a fraudulent QR code over the legitimate one.[130] When you then scan the code, you will be taken to a website that looks like the one you expect (assuming you even have an idea what to expect), but is actually a phishing site, i.e. a lookalike site run by a fraudster, looking to get your data. You then voluntarily enter all the information a scammer needs in order to defraud you, such as your payment information and possibly even other valuable personal information (license plate, name, phone number, email address, physical address, etc.).[131] To make matters worse: since you actually provided your information yourself in this scenario, you are even less likely to get reimbursed for fraudulent charges by your payment provider.

129 Potentially anything stored on, or ever accessed with, your device.
130 https://consumer.ftc.gov/consumer-alerts/2023/12/scammers-hide-harmful-links-qr-codes-steal-your-information
131 https://www.cloudflare.com/learning/security/what-is-quishing/

In Baltimore, for example, this problem has already become so prevalent that the city advised people simply not to scan QR codes at all.[132]

Unfortunately, the dangers of scanning a QR code are not limited to voluntarily giving your payment information to a bad actor. The website you are taken to may even download malware onto your device.[133] In some cases, the code will actually take you to the website you expect, but will do so via a malicious domain first, which will then intercept your data. The effect is the same. And, even beyond the visible actions your device takes when you scan a QR code, it may perform actions in the background which you are not even aware of.

This is possible, because, unlike traditional barcodes, which can only represent a very limited amount of information (more than a couple of words or about 20 characters or so will make the barcode awkwardly long and impractical to use), QR codes can store enormous amounts of data, including trackers, executable code and other software designed to compromise your privacy and device security. There are numerous ways in which scammers and cybercriminals are harming people who scan QR codes[134] and their creativity seems to know no limits.

A more sophisticated method used by some advanced criminals is to install malware on your device as soon as you scan the QR code.[135] The risk is even higher if you are asked to install an app in order to make your payment, park, or do whatever else you are trying to do. An app installed on your device can run in the background and potentially access and leak all your most

132 https://www.wbaltv.com/article/parking-meter-qr-code-scam-baltimore-city/46619631

133 https://www.nbcnewyork.com/news/local/qr-code-warning-what-is-quishing-and-how-to-avoid-getting-scammed/4776488/

134 https://www.kaspersky.com/resource-center/definitions/what-is-quishing

135 https://www.tomsguide.com/computing/online-security/new-qr-code-threat-can-infect-your-phone-as-soon-as-you-scan

intimate information on your device without you even noticing it. That includes your photos, location history, movement profile, browsing history, contacts, texts, phone logs, etc. All just for the convenience of paying "cashless."

An even more advanced method to abuse people's naïve willingness to use QR codes is by hacking the actual generation of the QR code. In this scenario, say the parking lot owner, restaurant, or other person who wants to create a QR code, has no bad intentions, but a third party hacker has intentionally corrupted the software generating the QR code.[136] This may have happened through malware on a device somewhere along the process, through targeted hacking of the specific program or in a variety of other ways. However, when the QR code is then generated, it has the malicious features explained above "baked in" to the QR code from the beginning, without either the user or the person who initiated the generation of the code being aware of it. Thus, in this scenario, the sign or menu is actually the original one, but is still malware-infected.

Unlike when you type a url into a browser, you have no idea where a QR code is going to take you and what all else it might be doing. Some advanced QR code malware can hijack your phone as soon as you scan the code, due to raw HTML and JavaScript embedded into the QR code, using data uniform resource identifiers.[137] Scanning a QR code can automatically make your phone do a number of things in the background without you even noticing; including making calls, giving away all your contacts, your identity, your files, photos, texts, location data, login credentials, and more.[138] If your phone becomes inoperable and you don’t have a physical SIM card, you cannot even send or receive texts or make calls anymore.

136 https://www.wbaltv.com/article/qr-code-safety-scam-quishing/69511048

137 https://www.tomsguide.com/computing/online-security/new-qr-code-threat-can-infect-your-phone-as-soon-as-you-scan

138 https://www.forbes.com/councils/forbestechcouncil/2020/06/01/i-dont-scan-qr-codes-and-neither-should-you/

Proceed at your own risk (or, if you want to be safe: don't)![139]

11. Terms and Conditions

Few nonlawyers ever read terms and conditions before they sign a document or click on “I agree”. Unfortunately, even if you don’t read the terms and conditions, once you click on the consent button, you are legally bound by a contract, the content of which you are not even aware of. And the consequences of doing so can be far-reaching, especially for the safety of your personal information![140]

This can create a serious nightmare for you down the road, should your personal information end up in the wrong hands. Terms and conditions regularly include the right to share and sell your information. Any entity thus lawfully obtaining your information may not only use it against you, but also become victim of a data breach. As discussed before, especially in the sections on cyberattacks and surveillance pricing, the more people and entities have your data, the higher your risk of being harmed, both legally or by criminals.

Even if you have been careless with your data in the past, it is *always* good practice to stop digging your hole deeper and not sharing even more.

Another problem with terms and conditions when applied to payments is that these allow a third party to have a say in what you spend your money on, as well as where, when and with whom. As controversies over the last several years have shown, many companies don’t shy away from forcing their ideology onto their customers (see the part on debanking above) or penalizing their customers for exercising their constitutional rights.

139 https://itfoundations.com/blog/why-you-shouldnt-scan-qr-codes
140 https://denvermonthly.com/how-clicking-i-agree-can-affect-your-personal-information/

For example, to use PayPal, you have to agree to their terms and conditions, which then subject you to their rules, which, beyond their restrictions on speech, also prohibit transactions involving all kinds of lawful items PayPal disapproves of.[141] And other payment providers employ similar practices, restricting what you can spend your money on.[142] As mentioned, stablecoin issuer Circle buried a clause in their terms and conditions (which was later modified), that prohibited the use of their stablecoin USDC for the purchase of "weapons of any kind, including but not limited to firearms, ammunition, knives, explosives, or related accessories."[143] PayPal still has almost the same restriction in its "acceptable use policy" as of the writing of this book.[144]

As terms and conditions frequently change (and usually become more consumer-unfriendly) it is quite possible for more provisions you may not like to find their way into them, such as hidden fees, penalties, expiration clauses, limitations, etc. All of those will continue to erode the autonomy of the user.

Nobody needs to agree to terms and conditions to use physical cash. But to use digital means of payment you do. These terms usually require all kinds of duties, restrictions and responsibilities you have to agree to, as well as liability protections and rights to use and share your information for the provider of the payment method. You generally never get a chance to negotiate these terms. They are usually offered on a take-it-or-leave-it basis. If you want to protect your safety and autonomy, you may want to leave it. And use cash instead.

141 https://www.paypal.com/us/legalhub/paypal/acceptableuse-full

142 https://www.thefire.org/research-learn/fire-statement-free-speech-and-online-payment-processors

143 https://www.thetruthaboutguns.com/nssf-warns-circle-usdc-gun-purchase-ban/

144 Section 2.(j) prohibits using PayPal for activities that relate to transactions involving "ammunition, firearms, or certain firearm parts or accessories" see: https://www.paypal.com/us/legalhub/paypal/acceptableuse-full

12. Enshittification[145]

Internet based services and platforms, as well as more recently a diverse variety of goods and services connected to the internet, are increasingly experiencing a frustrating phenomenon called enshittification (or occasionally called crapification, or platform decay, to reduce censorship).[146] This term, which is now widely used in the industry and among users, describes how online platforms and services, as well as apps, initially offer a compelling, useful and convenient experience, only to then become less and less user-friendly, cluttered with advertising, and, as they attract more users, deteriorate to data-harvesting tools which offer less and less value, while simultaneously requiring more and more patience as you have to put up with a growing amount of ads and commercials, glitchiness, tech debt, captchas, and overall nonsense.

Do you remember the internet before cloudfare, captchas and cookie consent notices? Or the time before YouTube and Rumble videos kept getting interrupted by commercials? How about when checked bags were included in airline tickets and breakfast and parking in hotel stays? You used to be able to watch Hulu without registration, login, or subscription (financed by commercials only) in the past. And while

145 I want to apologize to the reader unfamiliar with the term for the fact that the word "enshittification" may appear vulgar. It was not my choice of words and some of my friends warned me that some readers stumbling across this word might understandably find it somewhat offensive, and that is not my intention. However, given that the term "enshittification" has become a technical term which is widely used and recognized in the industry, often cited, including by mainstream media, has its own emoji and Wikipedia, as well as dictionary and encyclopedia, entries, which less vulgar alternative terms, such as "platform decay" and "crappification", do not to a comparable degree, and even became the word of the year 2023 (and has raised substantial awareness of and discussion about the phenomenon), I believe it would do readers a disservice to omit the official term here.

146 https://en.wikipedia.org/wiki/Enshittification

facebook was a data-harvesting nightmare from the beginning, it didn't use to have anywhere near the amount of advertising in the user experience as it does these days.

Nowadays, for some online services, you have to watch a commercial first, before you can proceed with what you actually want to do. Then, as you proceed, you are, after a short while, interrupted by another commercial. Or you won't be able to do what you need to do at all without providing your email address first, which then gets flooded with spam, potentially causing you to miss important emails in the white noise of marketing.

I recently tried to set up a new phone and couldn't even install apps without watching a commercial first. I then had to solve multiple captchas to sync my account.

This trend is sadly not even limited to "free" services or products. Many gas pumps now blare commercials at you and Samsung just confirmed that its $1,800+ smart refrigerators will start displaying ads on your expensive refrigerator door in your own home soon.[147]

As a 2024 Financial Times article warned, "'Enshittification' is coming for absolutely everything".[148] This realization is widely echoed[149] and bemoaned[150] throughout the industry.[151] The term even became the word of the year 2023.[152]

147 https://fortune.com/2025/09/19/samsung-family-hub-refrigerators-advertisements/

148 "'Enshittification' is coming for absolutely everything" - February 7, 2024, by Cory Doctorow in: Financial Times, https://web.archive.org/web/20240208152542/https://www.ft.com/content/6fb1602d-a08b-4a8c-bac0-047b7d64aba5

149 https://cybercultural.com/p/enshittification/

150 https://www.andrew-turnbull.com/enshittification-ux-product/

151 https://cybercultural.com/p/enshittification/

152 https://web.archive.org/web/20240206230815/https://americandialect.org/2023-word-of-the-year-is-enshittification/

Don't you just love clicking through blurry images of boats, fire hydrants, buses and crosswalks, only for some "artificial intelligence" to then present you with more images and eventually tell you that your response was incorrect? By the way: are you a robot? Please wait, this may take a few minutes to verify... Sorry, your attempt to connect to this page has been blocked!

The price in lost nerves, time, and quality of life is real. It is highly unlikely that this trend will spare digital money or payment systems. The very fact that *all* electronic payment methods are situated between the buyer and the seller (aka the "third lock") means such services are actually the prime candidates for exactly this phenomenon: As Cory Doctorow, who is widely credited with coining the term "enshittification" explains:

> [I]t is a seemingly inevitable consequence arising from the combination of the ease of changing how a platform allocates value, combined with the nature of a "two-sided market," where a platform sits between buyers and sellers, hold [sic] each hostage to the other, raking off an ever-larger share of the value that passes between them.[153]

Doctorow accurately observes that

> [t]he once-glorious internet has degenerated into "platforms" that rose to dominance because they delivered convenient and delightful services efficiently and reliably. But once we were locked in to those services, the tech bosses turned on us, relying on our dependency to keep us using the services even as they got worse and worse.[154]

153 https://web.archive.org/web/20230601004832/https://www.wired.com/story/tiktok-platforms-cory-doctorow/

154 "Enshittification: Why Everything Suddenly Got Worse and What to Do About It", by Cory Doctorow, ISBN: 978-0374619329

Imagine having to watch a commercial, agree to updated (more invasive) terms of service, or solve a captcha before you can pay! Or waiting in line while the person in front of you needs to update her browser or payment app and is running into technical roadblocks, preventing her from paying and thus the line from proceeding. Please verify that you are human in order to complete this transaction! Sorry, too many attempts! Please try again later.

With physical cash, you won't have to worry about this.

It is likely that the experience using digital payment methods will deteriorate a lot faster should physical cash ever disappear. The reason is that while cash exists as an alternative, issuers and operators of digital payment methods have an interest in not making the user experience too frustrating as their users may well switch back to using cash if paying cashless becomes too annoying. In fact, even according to developers, users' ability to ditch an app, service, or platform altogether appears to be about the only factor keeping the intentional deterioration somewhat in check.[155]

However, once cash is no longer available, you won't have a choice but to submit to any nuisance the user interface demands.

Even most tech enthusiasts would probably give up and pay cash instead if they had to go back and forth with an AI chatbot at 2am in the morning to buy a bus- or train ticket while approaching the departure time. Once cash is gone, you will be waiting as long as the AI makes you - even if the last train for the night is leaving.

Once you are stuck with that reality, you will miss the days when you could pay cash and you'll realize that going to an

155 https://www.humix.be/blog/enshittification-the-slow-decay-of-online-products-and-how-to-avoid-it

ATM or handling change pales in comparison to the inconveniences that await you in an all-digital-payment world. Your decision to pay cash today could help save us all from this constant frustration becoming reality.

13. Save Small, Independent Businesses

Using cash as opposed to credit cards or other electronic payment methods makes a serious difference for the profitability of a business. That's because credit card and other payment providers charge a fee for every transaction. This fee is usually not apparent to the consumer, as it is charged to the business and most businesses don't pass this fee on to their customer; but for the business, these fees add up. While some large national chains can pass those extra costs on to their customers by charging higher prices and cutting costs on personnel and quality, many small businesses are not in a position to do so. And for them this can make the difference between whether they can afford to stay in business or have to eventually close forever.

Visualize it this way: if you buy something for, say $100 including tax, and you pay cash, your favorite restaurant or mom&pop shop gets $100. If you pay with a credit card, they only get $95.[156] However, keep in mind that they have to buy the product they are selling you, pay their staff, their rent, their utilities, fees, licenses, business taxes and other overhead, plus the sales tax, all out of the $100. So their profit may only be $10, if that. Paying with credit card thus cuts their profit in half!

156 The exact percentage varies depending on the credit card company, the merchant and the details of their contract. But think about how much some credit card companies offer you in cashback; sometimes that can be up to 5%, then add the other perks they offer you, plus their own expenses and the profit they make. All of that comes out of what they charge your merchant.

If you want your favorite shop or restaurant to stay in business, keep this in mind and consider paying cash to ensure they can still afford to be open tomorrow. This is especially important as these businesses contribute substantially to national employment, as well as to the federal, state, and local tax base. If you have a grievance or suggestion and bring it to the local store owner who personally knows or at least recognizes you, he'll likely consider it to keep a regular customer happy. Try this at a national chain outlet and they'll tell you: "This is coming from corporate."

Being able to do business with people who know and trust you and whom you know and trust can literally be a life saver.[157] As Catherine Austin Fitts, publisher of the Solari Report, loves to point out: “The currency of the future will be relationships of trust.”

14. Save Small Farms and Retain Access to Trustworthy Food

Using cash, rather than electronic payment means, may also protect your ability to obtain food from sources you can trust. Most of us have become dependent on an anonymous, corporate supply chain, feeding us animal products full of hormones, antibiotics and other substances we would rather not indiscriminately ingest, as well as a myriad of chemicals, heavy metals and other ingredients that adversely affect our health.

While supporting local farmers and healthy food should be common sense, not all policymakers agree that people should have access to the food of their choice or autonomy over what to put into their bodies, as vaccine mandates and resistance to legislation allowing people to purchase Ivermectin[158] or raw

157 https://bobsullivan.net/cybercrime/why-banana-bread-is-the-solution-to-the-worlds-fraud-problem/

158 https://tnga.granicus.com/player/clip/26823?view_id=610&meta_id=668866&redirect=true

milk[159] have shown. In fact, numerous municipalities and homeowners associations across America are outright banning people growing their own food, a basic human right we used to take for granted.[160] This situation has become so problematic that, for example in Tennessee, Senator Frank Niceley, and most recently Representative Michele Reneau, proposed a constitutional amendment to protect people's right to grow their own food. Both times, the measure failed in committee, however.[161] While Florida, Illinois, and Maine passed laws to ensure people are allowed to grow their own garden, similar measures in other states have met enough resistance not to pass.[162]

In light of the ongoing hostility to food autonomy, which includes decades of legislative changes and lawfare to concentrate food production in the hands of a few large corporate monopolies,[163] how are you going to get food from your local farmer or your neighbor, if every single transaction is monitored and can be algorithmically blocked before going through? Remember that Michigan at one point even banned the sale of plants and seeds.[164] When someone else controls when, where, how, with whom and what for your money works, then you will only be able to purchase what someone

159 https://www.organicauthority.com/energetic-health/no-raw-milk-for-montana-bill-fails-by-one-vote

160 In fact, my grandparents' backyard was, as was common at that time, calculated to be large enough to grow enough food for a family to survive. This measure was actually encouraged by local governments just after WWII, as food shortages and defunct supply chains were commonplace. Remember grocery store shelves in 2020?

161 https://wapp.capitol.tn.gov/apps/Billinfo/default.aspx?BillNumber=SJR0861&ga=112 https://wapp.capitol.tn.gov/apps/BillInfo/Default?BillNumber=HJR0780&ga=114

162 https://civileats.com/2022/08/20/two-states-right-to-garden-laws-local-food-community-nutrition-security-illinois-florida/

163 https://www.citizensforjustice.org/monsanto-war-against-farmers/

164 https://www.forbes.com/sites/nicksibilla/2020/04/16/michigan-bans-many-stores-from-selling-seeds-home-gardening-supplies-calls-them-not-necessary/

else decides you should. Without cash, you are then back to either barter or potentially not getting the goods and services you need.

15. Budgeting

If you are ever trying to save money, be that because you are struggling to make ends meet, had expenses go up, or a source of income fall away, lost your job, are trying to repay debt, or want to invest and build wealth, budgeting is a powerful habit. The easiest way to do this is by allocating specific amounts of money to each category of expense and then putting physical cash into containers (for example glass jars, cigar boxes, paper envelopes, or sheet protectors in a binder) with corresponding labels. Money guru Dave Ramsey highly recommends this technique to anyone trying to save money and explains it in detail on his website.[165]

Such a system can be set up for free at home and allows you to effortlessly and intuitively see at any point how much money you have left in each category. The psychological effect of seeing and feeling your money as you spend it (see 5. above), plus the exciting feeling when you manage to have unspent cash left in a container at the end of the month, will harness your brain's reward system to instinctively save money.

This is due to the simple fact that when money is physical, you can feel and see its limits. Digital money is virtual and therefore does not have that same edge. Plus, you cannot stuff virtual money in envelopes or piggybanks.

16. Discrimination and Exclusion

Charities in the United Kingdom recently pointed out to members of parliament that for people in abusive relationships,

165 https://www.ramseysolutions.com/budgeting/envelope-system-explained

whose spouses used a bank account to track and control their spouse's movements, access to cash was oftentimes their only means to actually accessing essentials for themselves and their children and to escape their abuser.[166]

Further, not everybody can even get a credit card or even a debit card. In fact, a survey by the Federal Deposit Insurance Corporation (FDIC) found that millions of households in the United States remain unbanked and that "lower-income, less-educated, Black, Hispanic, disabled, and single-parent households continue to be significantly more likely to be unbanked." The survey further found that the majority of these households rely entirely on cash.[167]

This problem affects not only people with bad credit scores, but also many foreign nationals, such as exchange students, tourists, and anyone who is not old enough yet.

What made this point concrete was when a group of children visited an aquarium with their grandmother and stopped by at the gift shop after their visit to buy some souvenirs. Excited and equipped with some dollar bills, they each had received as pocket money, they thoroughly checked out what all the store had to offer. They then each picked out something within the price range they had money on hand for. Some had to decide between a couple different items and prioritize which one they wanted more and which ones not to buy. Some of the kids were learning the math of what they could afford and what was too expensive. It was fascinating how the older ones helped the younger ones learn money and basic math.

Eventually, they each chose something they wanted to buy and gleefully proceeded to the checkout. Unfortunately, the aquarium's managers had recently decided to "go cashless" and reject legal tender. Humiliatingly, the children were told that

166 https://www.bbc.com/news/articles/c1el81lenq1o

167 https://www.fdic.gov/household-survey/2023-fdic-national-survey-unbanked-and-underbanked-households-report

they could not buy anything. You can imagine the disappointment of a bunch of five to ten year olds leaving the shop empty handed after looking forward to their purchase they had given so much thought (and how the grandmother must have felt, too).

If businesses continue to "go cashless" and customers put up with it, this can soon be the experience for anyone for their entire childhood and adolescence. The prospect these children are facing is to be less and less able to participate in even small-item commerce until they reach the age of 18, which is an eternity away when you are twelve, let alone eight. How is this future generation ever supposed to learn responsibility?

17. Crucial Education

As the previous point shows, a cashless society means that children will never get to experience cash and may not even have money of their own at all. Those of us who grew up with cash take its educational value for granted and don't even realize how crucial it was for forming our understanding of money.

If the first interactions with money are tactile, such as feeling the weight of a coin, its sound when it falls into a piggybank or a vending machine, when you see and feel money that you save physically accumulating and experience it diminishing when you spend it, you form crucial memories that make currency concrete. You keep those memories with you, even when you sometimes pay by other means later, but these experiences have formed a deep understanding of money. These experiences make it a lot easier for children to learn vital skills, such as self-regulation and budgeting.[168]

168 https://www.cashmatters.org/blog/childhood-cash-learning-money-sense/

Moreover, parents who give their children a cash allowance will likely talk to them about spending and saving. Such conversations are a lot less likely to occur without cash.

The prospect of children growing up in a cashless world is not only depressing, but once children who grew up cashless finally reach their eighteenth birthday, these young people will then suddenly be thrown from having no financial rights, responsibility or experience at all into full unrestricted financial responsibility without any preparation or transitional period. Never having learned to budget (be it just with allowances of pocket money) or experienced running out of money when the stakes were as low as not being able to afford a toy or a comic book, they will now almost immediately have to make decisions such as taking out student loans which may indebt them for the rest of their lives. This concept is hard enough to comprehend for today's 18-year olds; imagine this is one of your first encounters with financial decisions at all!

18. Courtesy

Being able to throw in some money for a tip, sharing the expense of something your friend or colleague buys for someone you both care about, or providing immediate reimbursement or reward for something someone does for you or an expense they incur on your behalf, is simply a matter of good manners. If your friend runs to the store, drive through, or gas station, and you ask her to grab you a hamburger, pack of cigarettes or to pick up some more beer, ice, food, or napkins for the party, giving her cash to do so up front is just the right thing to do.

If someone helps you, it’s not right to force that person to accept problematic and invasive terms and conditions of some digital payment provider (and potentially subject them to problems as a result), have them wait, cash a check, or worse: mooch on them altogether. "I'll pay you back later" but that payback requiring them to jump through hoops or keep

begging you is pretty rude and people will remember. You are also more likely to forget to pay them back if you can't do it right away, which won't look good on you.

In 2026, the IRS made good on its long announced threat to crack down on popular payment apps, such as Venmo and Zelle, and the IRS's new AI-driven audit alarms are now flagging birthday-gift transfers, split checks, and other innocent payments as potentially unreported business income.[169] Reimbursing your friend via an app may thus trigger an audit for the very person who advanced the cost for an expense for you, which probably won't exactly help the friendship.

Assuming your friend can come up with all the paperwork (which means she will have to beg you yet again, to state in a notarized letter to the IRS that the payment was indeed a reimbursement for an expense she fronted for you), she will ultimately get through the audit after weeks or months of paperwork and anxiety-inducing correspondence, but it will cost a lot of time and nerves. And all it would have taken to prevent this would have been to instead give her $25 in cash for a $50 gift she bought for your mutual friend's anniversary.

If someone is kind enough to help you and, in a way, lend you money, you should not make them go through something like that. Always having some paper bills on you solves many problems and is simply polite.

19. Drain on the Economy

We already discussed the fees which payment providers take out of each and every transaction and the fact that for small businesses, this can make the difference between profitability and bankruptcy. Few people appreciate the full extent of the

169 https://www.newsbreak.com/saving-advice-319227098/4441627790031-irs-warning-the-2026-audit-alarms-triggered-by-routine-venmo-and-zelle-transfers

devastation they are causing to their community whenever they make a digital payment instead of using cash, though.

The problem is that the drain of capital compounds with every single transaction. The above mentioned fees thus take an enormous amount of wealth out of our society.

If you hand a $20 bill to your food truck owner, she gets $20. She can then give the $20 to her farmer, who still receives $20. He can turn around and buy fuel and the gas station receives... $20. If you swipe a credit card instead, and the fee is, say 3.5%, the food truck owner only gets $19.30. If her farmer accepts payment by credit card, he'll get $18.62 and the gas station will only get $17.97. Within just five everyday digital transactions, only $16.74 remain, after ten, only $14.- are left!

The money taken out in fees did not go to the food truck owner, the farmer, or the gas station, like the $20 bill would have, it left the community entirely.[170] Next time you notice potholes, homelessness, disrepair and blight, and catch yourself wondering what happened to the prosperity our country once experienced, remember this math example! It is no coincidence that average Americas were financially way better off when most people used cash. Merchant swipe fees alone amounted to $148.5 billion in 2024.[171] Every single time you swipe, insert, or or tap a credit card instead of paying cash, you are literally contributing to the decay of our society's wealth.

170 https://www.theepochtimes.com/opinion/when-cash-disappears-so-does-something-else-5982988

171 https://www.fool.com/money/research/average-credit-card-processing-fees-costs-america/

www.preservecash.org v.1.1

XI. ARGUMENTS AGAINST CASH - AND COUNTERARGUMENTS

The main reasons against cash I hear people bring up are the following:

1. Risk of getting robbed,
2. Theft by employees,
3. Convenience,
4. That's where the trend is going.

Let's go over those one by one:

1. Risk of getting robbed

We already addressed this one in the previous chapter X in part 4. It is true that if you get robbed, you lose the cash you have on you. But you also lose the credit and debit cards that you have in your wallet, which means that your nightmare is just about to begin and may take days or weeks to clean up as you are spending countless hours on the phone with banks etc. canceling your cards, requesting new ones, updating your payment information, monitoring your account for fraudulent charges, fighting to get reimbursed for those fraudulent charges, etc.

Additionally, carrying contactless payment methods with you, whether that is a credit card with an RFID chip, or a smartphone with a contactless payment app, is extremely risky due to the increasing prevalence of “tap-to-pay” scams, ranging from overcharges to people standing or walking near you

www.preservecash.org v.1.1

reading out your contactless payment information,[172] as we discussed (so-called Ghost Tapping).

As discussed in the previous chapter, this is today the far more attractive method for criminals to get your money than robbing someone; and your risk of becoming a crime victim is significantly higher with electronic payment methods these days, especially with contactless ones, than with physical cash. For that very reason, I actually often don't even take credit cards with me at all. And for the cybersecurity reasons listed in the previous chapter, I do not use payment apps on a phone, nor would I scan a QR code.

2. Theft by employees

The right HR policies (hiring and terminating based on integrity) and operating procedures (verification, supervision, documenting) can actually seriously mitigate this problem or largely prevent it from occurring in the first place. A camera filming the drawer of the cash register is another simple and efficient way to prevent theft of cash, if the employer feels that need. In fact, there are many ways to address and and solve the problem of theft by employees.

For electronic payments, there is actually a much more common and larger problem which you do not have with cash payments at all: chargebacks. Chargebacks are what occurs when a customer disputes a payment with the payment provider (e.g. credit card company) and the transaction is reversed. Customers regularly do this, sometimes because the charge description looks cryptic on their statement and they don't recognize it, sometimes because they were dissatisfied with the product or service and, rather than communicating this directly to the business, they decide to dispute the charge. Sometimes it happens outright with intent to defraud. In any case, the merchant not only loses both the product and the pay

172 https://www.bbb.org/all/consumer/scam/how-to-spot-and-avoid-tap-to-pay-scams

for it, but is also charged processing fees and penalties, which can amount to 2.5 times the original charge.[173] For that reason, accepting electronic payments is actually a lot riskier than cash, where the transaction is complete and final once payment with physical cash has occurred.[174]

Criminally minded employees actually have other ways to steal, whether your business accepts cash or not: one such method is so-called refund fraud, where the employee processes a refund from a payment or point-of-sale (POS) terminal and pockets the refund or shares the credit reimbursement with the customer.[175]

Another is potentially even a lot more harmful to your business, as it affects your reputation as a business and may lead to bad reviews: an employee enters a (potentially significantly) higher charge or extravagant tip amount into the payment system, banking on the customer not checking the display (or even casually covering it while handing it to the customer).[176] The unsuspecting customer then authorizes the payment and won't notice until checking her statement days or weeks later, at which point you will have an understandably upset (former) customer on your hands.

Since the most reliable way for customers to protect themselves against such scams is simply paying with cash, not accepting cash is rightfully considered a red flag by many.[177]

173 https://www.netsuite.com/portal/resource/articles/accounting/chargebacks.shtml
174 unless both parties agree to reverse it.
175 https://www.uschamber.com/co/run/finance/prevent-credit-card-scams
176 https://www.usatoday.com/story/money/personalfinance/2026/07/27/tap-to-pay-donation-scam/91064460007/
177 https://www.usatoday.com/story/money/personalfinance/2026/07/30/tap-to-pay-scam-checklist/91099280007/

3. Convenience

The price for the short-term convenience is a long-term dystopia. As discussed in chapter IX above, one could view living in a digital prison convenient, but for most, there will come a point where the constant violation of one's autonomy will feel very uncomfortable and actually inconvenient. So the question here is again whether one is willing to sacrifice long-term freedom for short-term laziness.

And even in the short term, not using cash can get very inconvenient very suddenly and unexpectedly, as we have seen in chapter X. All it takes is a minor unforeseen event and cash would be the much more convenient option or could have prevented serious problems.

4. That's where the trend is going

Trends are not irreversible and history is not linear. Eastern Europe, from East Germany to the Soviet Union, was on a clear track to more and more surveillance and less and less freedom until things radically changed in 1989. In the West, crime and pollution were on a seemingly unstoppable upward trajectory around the same time, but things likewise changed in the 1990s. Universal vaccine mandates and various other restrictions seemed inevitable in 2020/2021 and freedom seemed lost already. Central Bank Digital Currencies (CBDCs) were on a fast track around the globe, but have been met with unexpected pushback.

Cash is even experiencing a renaissance in many ways.[178] In the UK, for example, the percentage of purchases made with cash recently started to climb again for multiple years in a row.[179] Especially younger people are increasingly demanding

178 Multiple states have recently passed laws, requiring universal cash-acceptance, and several governments are taking steps to ensure that a cash infrastructure is being preserved.

179 https://www.bbc.com/news/articles/c1el81lenq1o

to have cash as an option and are embracing it in much larger numbers than older generations.[180] We will talk more about this trend in chapter XV. In fact, as the world's leading banknote-printer Koenig&Bauer notes:

> "To the surprise of many and despite the digitalisation of bank accounts and other internet transactions, the banknote is still alive and well. Every year, production increases by 2-3%. There are many reasons for this. Banknotes offer the greatest independence and freedom to their users. 1.6 billion people in the world do not have bank accounts. Cash also offers unparalleled security in contrast to the need for the protection of data collected by digital actors and their sometimes questionable use. Importantly, the banknote does not involve any charges. Worldwide, 75% of person-to-person payments are made in cash."[181]

Making people feel powerless and making bad trends appear inevitable is in the interest of those who want to control you, but it is a lie and not helpful. Instead, decide what future you want to live in and want future generations to grow up in, then embrace your responsibility for it and do whatever is in *your* power, no matter how insignificant it may seem to you. Lead by example! Imagine everyone acting the way you do and then live in such a way that this seems like a desirable scenario to you. Or, more tritely put: Be the change you wish to see in the world.

180 https://www.paymentsjournal.com/gen-z-is-embracing-cash/

181 https://banknote-solutions.koenig-bauer.com/en/news/articles/article/90-of-the-worlds-banknotes-are-swiss/

www.preservecash.org v.1.1

XII. ARE THERE ANY FREEDOM-PRESERVING ALTERNATIVES TO CASH?

1. Cryptocurrencies?

Cryptocurrencies, such as Bitcoin and Ethereum, were actually the first form of programmable money. Hence, they ushered in one of the two very factors that make digital currencies so dangerous to human freedom. In fact they created it in the first place. Until cryptocurrencies, while there were programmable payment systems, currency itself was never programmable (see chapter V above). The programmablitiy of virtual currencies was initially lauded by tech geeks as an innovative feature, enabling, for example, smart contracts, but has since gotten power hungry control freaks even more excited, as it allows to have endless constraints, ifs, and buts, built into the very fabric of your money.

Programmability of your money, regardless of who has the ability to program it, be that a government or private entity, is always an existential threat to your freedom!

Cryptocurrencies have actually been a driving force in the war on cash! One reason is that they provide excuses for policymakers to push for CBDCs, the other is that they distract people from defending cash, having them parrot the talking point that cash is going away, rather than opposing this policy.

While the argument for cryptocurrencies was initially that these are independent of governments, governments have since

shown that cryptocurrencies are not immune to regulation, legislation and confiscation either. For example, about ten years ago, the United States Department of the Treasury classified cryptocurrencies as assets, not currency. As a result, they are subject to capital gains tax. This means that you have to declare every transaction and pay taxes on it, or be committing a felony (tax evasion). As a result, cryptocurrencies (other than stablecoins - see next paragraph) largely lost their usefulness as a means of payment and have since primarily been a speculative investment, rather than a currency.

The capital gains issue was the motivation behind creating so-called stablecoins, i.e. cryptocurrencies which are pegged to the value of another currency or asset. If pegged to the value of the U.S. Dollar, for example, buying or selling that coin won't incur you any capital gains in the U.S.

However, stablecoins are both surveillable and programmable. These are the two most dangerous features of digital currencies, including CBDCs. In fact, in the United States, federal law subjects stablecoin issuers to the same customer identification rules as apply to banks in relation to their customers (see § 4(a)(5) of the GENIUS Act). It is one thing, however, for your bank to know how much is in your bank account, because once you withdraw it, they don't know where, when, with whom and what for you spend it; and it is a very different thing for a stablecoin issuer to know exactly where every single stablecoin or token is coming from and going to at all times, thus exactly what you spend it on, where, when and with whom.

This means that, by definition, there is no privacy with regard to stablecoins. The GENIUS Act further requires stablecoin issuers to have the ability to deny individual transactions (see § 4(a)(6)). You can read a more detailed analysis of the pros and cons (including the very real danger to your freedom) of stablecoins and the law governing them, in my article "The

GENIUS Act and its Implications for Financial Transaction Freedom" on solari.com.[182]

Even the cryptocurrency publication Cryptonews acknowledges that “The line between freedom and control is growing thinner, forcing a deeper look at how much influence politics should hold over the supposedly free world of stablecoins” and that “Circle’s controversy has drawn parallels to the same issues critics have raised about government-backed digital currencies.”[183]

It should thus be abundantly clear that stablecoins are no alternative to cash when it comes to your freedom. In fact, they are just as dangerous in that regard as a CBDC. They are simply issued by private issuers instead of a central bank. In the U.S., they are by law required to be subject to a Treasury mandated system of sanctions, blacklisting or seizure. With the Treasury financially dependent on the Federal Reserve system, central bankers have at least indirect control. Plus, in addition to central banks and the government, private banks and corporations can additionally subject them to their own rules for how, when, where, with whom and for what you can use this "money". Hence, you could call stablecoins a Private Bank Digital Currency, or PBDC. And while the Federal Reserve Bank is at least theoretically subject to Congressional oversight and thus supposed to respect the Constitution, private banks and companies have a lot more freedom to infringe upon your rights.

So what about other (non-stablecoin) cryptocurrencies? Aside from the mentioned legal pitfalls of inevitably committing tax evasion when you use them and don't declare your gain and loss for every cup of coffee, book, pizza, car ride, etc. you purchase or get paid for, it is crucial to understand that

182 https://solari.com/the-genius-act-and-its-implications-for-financial-transaction-freedom/

183 https://cryptonews.com/news/circle-reverses-usdc-gun-ban-political-pressure-stablecoin-control/

cryptocurrencies are not an alternative to cash when it comes to the most crucial aspect: protecting human freedom. The main reason is that they are both surveillable and programmable. Every transaction conducted with cryptocurrency is, by design, forever part of a public ledger. This is the *opposite* of anonymity!

While some cryptocurrencies have encrypted ledgers (hence the name), cracking an encryption is always just a matter of how much computing power you can throw at it, and code that was impossible to crack ten years ago can be decrypted within a matter of seconds today. This is due to a phenomenon called "Moore's Law", per which computing power increases exponentially. Just think back of how primitive computers were, say in the 1980s, let alone 1960s. and how outdated even computers from the early 2000s are today.

Given the advancement in technology, computing power and omnipresent surveillance, it is absurd to assume that cryptocurrency is immune to government control (or theft by cybercriminals, for that matter - keep in mind that any "backdoor" existing for a government can also be exploited by a criminal who has knowledge of its existence). In fact, the U.S. government openly admits its successful seizure of cryptocurrency,[184] proving that this possibility is no longer hypothetical.

Imagine for a moment, though, that there was a hypothetical cryptocurrency that achieved the impossible and was actually completely anonymous and secure,[185] how are you going to pay with it? You will need some form of smart device to transact at

184 https://www.justice.gov/opa/pr/justice-department-announces-seizure-over-28-million-cryptocurrency-cash-and-other-assets

185 As discussed, this is impossible to achieve 100% from a technical standpoint, and even if it were, all it takes is one transaction for which your identity is revealed (e.g. your initial purchase of that currency, or you using it for something where you are also showing your ID, signing up by name or paying for something delivered to your address, etc) and the rest of your transactions can be identified.

the point of sale (store, checkout, ...). The moment you tap, scan or otherwise connect that device with the point of sale's terminal, your identity is known.

From a legal standpoint, if you are a U.S. citizen, or residing or engaged in commerce in the United States, you only have two lawful options for transacting in cryptocurrencies: either 1: declare every single transaction (due to the capital gains taxation), or 2: avoid incurring any capital gains at all. Option 1. obviously destroys any anonymity. Option 2. is only possible with a cryptocurrency that does not incur capital gains, because it is always worth exactly the same when measured in U.S. Dollars, in other words: a payment stablecoin. But for payment stablecoins, federal law mandates surveillance in the form of Know-Your-Customer (KYC) and Know-Your-Transaction (KYT) requirements, as well as the ability for a third party to block individual transactions under the GENIUS Act.[186] Payment stablecoins without these two features have been outlawed by the GENIUS Act. And if you transact in a cryptocurrency other than a stablecoin and don't declare the transaction, you are committing tax-evasion, which is a felony.

Thus, even if one could overcome the impossibility to have a completely anonymous and secure cryptocurrency from a technical standpoint, you would be committing a felony by using it without declaring it.

Additionally, cryptocurrencies are dependent on large data centers, IT-integrity, and availability of electricity and internet. See part 1 of chapter X above for the implications of such vulnerabilities.

The enormous power consumption of cryptocurrencies goes directly against the stated policy goal of many countries to *reduce* energy demand.[187] A single bitcoin transaction uses as

186 https://solari.com/the-genius-act-and-its-implications-for-financial-transaction-freedom/

187 https://www.eia.gov/todayinenergy/detail.php?id=61364

much energy as hundreds of thousands of credit card transactions,[188] or, to make it easier to visualize, as much as leaving your stove on 24/7 for about two years. The total energy consumption of bitcoin already exceeds that of several countries, such as The Netherlands, Poland, Thailand, or the Czech Republic,[189] despite only representing a minuscule share of total transactions. This makes it seem unlikely that cryptocurrencies will be tolerated for much longer by governments willing to go to extreme measures to cut emissions. And as digital IDs, facial recognition software, "age verification" (meaning personal identification of everyone), etc. become more and more omnipresent,[190] it is unrealistic to expect governments to remain unaware of your crypto-transactions. Hence, once a government outlaws cryptocurrencies, you are unlikely to evade enforcement.

On June 26th, 2026, the European Banking Authority (the European Union's financial services oversight agency) published details about its proposed penalty plan for cryptocurrency issuers that do not comply with the European Union's digital asset laws.[191] The penalties are intentionally designed stiff enough to deter even the world's largest digital-asset operators. This move has already led some major cryptocurrency exchange operators, such as Binance, to start suspending their services in the EU[192], demonstrating that the key players in the cryptocurrency industry are well aware that once powerful governments crack down on cryptocurrencies, there will be no evading their rules and enforcement.

188 https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/

189 https://digiconomist.net/bitcoin-energy-consumption

190 aside from the near-impossibility to obtain and maintain an unidentifiable device (for more information, search for "device fingerprinting")

191 https://cointelegraph.com/news/eu-watchdog-eba-details-big-crypto-fines-as-landmark-laws-bite

192 https://cointelegraph.com/news/eu-watchdog-eba-details-big-crypto-fines-as-landmark-laws-bite

Finally, the very nature of a "blockchain", i.e. the permanent public ledger that cryptocurrencies are built on, is ultimately irreconcilable with privacy and anonymity. As mentioned, even encryption of this ledger only means that one will have to make more of an effort to decrypt it, an effort that, as discussed, becomes technologically easier, faster, and less expensive with time. While effective marketing has been selling distributed ledger and blockchain technology as a new shiny toy, it is actually a building block for surveillance and programmability and thus poses a very real threat to your freedom.

In summary: cryptocurrencies are no substitute at all for cash in terms of privacy, freedom, resilience and accessibility.

2. Checks?

Obviously, checks do not provide as much freedom and privacy as cash, however, they do have a few serious advantages at least over digital payment systems. For one, unlike with credit cards, which skim several percent off the payment which the payee receives, someone whom you pay with a check receives the entire amount. And unlike with programmable money, with a check you are still transferring regular non-programmable dollars.

Of course, unlike with cash, you can still be debanked, i.e. your bank can close your account if they don't like you or don't like what you say or do (see part 3 of chapter X above). A government could likewise trudeau your account.[193] There is also always a potential for fraud.

However, there is actually something to be said for a healthy banking landscape with independent, accountable, small banks. It is always good advice to know your banker. If you do not

193 https://edmontonjournal.com/opinion/columnists/david-staples-federal-court-stands-up-for-canada-in-rejecting-trudeaus-freezing-of-bank-accounts

have a specific person at your bank whom you are usually dealing with, or worse, cannot get a hold of an actual bank-employee at your actual branch, it is time to look for a different bank. If, on the other hand, you know your banker and your banker knows you, there is a host of problems you will probably never even face, or you will be able to quickly resolve them with a simple phone call or in-person visit. Responsible banks also play an important role in keeping the economy healthy and alive (through credit creation) and in ensuring your easy access to physical cash (through branches and ATMs).

A check facilitates the transfer of an amount from one bank account to another. Thus, both banks and both parties to the transaction know the identity of the parties involved. However, you are not sharing your identity (and vast amounts of other data) with obscure tech companies and data brokers in the process. Thus, checks are at least relative to electronic payment methods a lot more private.

Finally, checks are made from paper and signed with a pen. This makes them one of the only alternatives to cash that is not dependent on the internet or electricity. The banks involved will of course at some point utilize computers to transfer the funds, but you can pay or be paid with a check, even during a power outage or internet disruption.

Therefore, checks, bank deposits, and electronic bank transfers, are no substitute for physical cash; however, they are a very important complement, especially for purchases for which cash is *actually* impractical, such as buying a house or paying someone you cannot physically meet.

3. Debit Cards?

While debit cards have the one advantage over credit cards that you don't incur debt by using them, in a way they are actually more dangerous than credit cards, as they provide direct access to your bank account. Hence, if your debit card information is

compromised (and remember, you add vulnerability to it being stolen, even from a third party over which you have no control, every time you use your card, be that online or in person) you are way less protected against fraudulent charges than if someone fraudulently charges your credit card.[194] Additionally, if there is a fraudulent charge to your credit card, the issuer usually fights to get *its* money back; if there is a fraudulent charge to your debit card, you will fight to get *your* money back.[195]

Once a fraudulent charge is placed on your debit card, that money is gone from your account. Thus, in addition to the fraudulent charge itself, other payments from this account (such as automatic bill-pay you may have set up to pay for recurring charges etc.) may bounce and you may get hit with penalties, late fees, and face suspensions of the services for which the charges were declined due to insufficient funds in your account. The domino effect of problems resulting from a single fraudulent charge to a debit card can be enormous.

For that reason alone, it is highly advisable **never** to use a debit card! The only exception might be in order to use an ATM, but even for that purpose, you are a lot safer off if you ask your bank to issue you an ATM card instead. This way, you won't have to worry about losing your debit card, having it stolen, or someone walking past you with an RFID-reader stealing your card information via the card's contactless payment features.[196]

On the issues of privacy and control, debit cards are just as problematic as any other method of electronic payment. Every transaction is recorded, can be denied by a third party, and your

194 https://www.usatoday.com/story/money/2024/10/09/fraud-protections-debit-credit-cards/75211559007/

195 https://www.nerdwallet.com/credit-cards/learn/credit-card-vs-debit-card-safer-online-purchases

196 If your bank won’t issue you an ATM card, at least have them deactivate any function of the debit card, except for its ATM-functionality. That way, it’ll be a lot harder for a bad actor to put fraudulent charges onto your account.

identity is immediately known. This information can be used to create a disturbingly accurate profile of your movements, purchases, preferences, habits, views, health, vices, etc. Don't be surprised if it will one day be used against you.

4. Apps?

The absurdity of this one will be either obvious or intuitive to most readers at this point. Nevertheless, companies do succeed in tricking people into believing that certain payment apps might be superior, e.g. by distracting them with the fiat vs. metal-backed debate, or by highlighting some feature that might alleviate one (though not most) of the shortcomings of other electronic payment systems.
Obviously, like with any other electronic payment method, you don't have privacy, and you are dependent on the consent of a third party. But payment apps are actually a lot worse in that they live on your smartphone.

Anything installed on your smartphone introduces a number of added vulnerabilities and privacy nightmares, even compared to other electronic payment systems. Consider the sheer amount of highly valuable personal data (photos, contacts, texts, location history, body-sensor data, browsing history, etc.) that is combined in your smartphone! Tap your phone to make a payment and the intimacy of information you might reveal about yourself for buying a meal or some gas is hard to fathom. Plus, you are making your phone even more of an attractive target for hackers. And you are trusting some obscure developers to not access all your other valuable data and to ensure no bad actor can exploit their app to do so either.

A public service announcement issued by the FBI in March 2026[197] should make it abundantly clear that any app you install on your phone puts your data at risk! Further, many popular apps you likely have installed already can compromise other

197 https://www.ic3.gov/PSA/2026/PSA260331

sensitive data on your phone, as the FBI points out. Hence, anything you can access with your phone, a bad actor on another continent can potentially access as well; this includes any payment app you install.

5. Gold and Silver?

Physical gold and silver have the great advantage that they are extremely stable in purchasing power and you can physically hold and exchange them, just like cash, without power or internet and without the approval of a third party. However, they are not exactly useful for everyday transactions. This might change in a total apocalypse, but currently, almost every vendor will accept a $20 bill, but most people won't know the spot price for silver, let alone be willing and able to give you change for gold. Aside from not knowing the daily exchange rate, most people would also not be able to tell a fake gold or silver coin, let alone round, bar, or ingot, from a real one and would understandably be worried about assuming the risk of giving something of value in exchange for worthless counterfeit.

For that practical reason, physical gold and silver are a great, crisis-proof investment to retain value, but are currently not a practical replacement for cash when it comes to daily transactions. You should probably have some for an emergency, especially if you have spare funds, but you still need cash to pay at the grocery store, gas station, or restaurant.

It is also worth noting that if you are using gold and silver as currency, you have to be really careful to ensure compliance with applicable tax laws. Per the Constitution for the United States[198] the [federal] Congress has the right "To coin Money

198 The correct preposition here is indeed "for" – see the preamble to the Constitution for the United States (although many publishers mislabel this important document on their unofficial covers), which makes perfect historical sense, as it was the states that created the federal government after organizing matters without one for the first eleven

[and] regulate the Value thereof,"[199] and "No State shall [...] coin Money; emit Bills of Credit; make any Thing but gold and silver Coin a Tender in Payment of Debts".[200] This means that gold and silver coin are actually the *only* thing states *can* declare legal tender and only the federal Congress can declare anything else legal tender (which it has done in 31 U.S.C. § 5103).

Not all states have exercised their right to declare gold and silver coin legal tender, however. Tennessee tried this year with the Hulsey-Niceley Legal Tender Act,[201] which was named after the two legislators, Representative Bud Hulsey and Senator Frank Niceley, who four years prior also sponsored the bill that removed the sales tax on precious metal coins.[202] As of the writing of this book, Arizona[203], Arkansas[204], Louisiana[205], Oklahoma[206], Utah[207], and Wyoming[208] successfully passed legislation declaring gold and silver coin legal tender. Many of these have also included the caveat that you cannot be compelled to accept gold or silver as payment, though.

In other states, gold and silver are often still subject to sales tax and/or capital gains tax. Aside from potential state taxation,

---

years of the nation. When they decided to create a federal government, they wrote the Constitution *for* it. The incorrect preposition "*of*", which is often used on covers of reprints, suggests that the federal government gave itself that Constitution (which would mean that the effect came before the cause).

199 Art. I § 8

200 Art. I § 10

201 https://wapp.capitol.tn.gov/apps/BillInfo/Default?BillNumber=HB2038&ga=114

202 https://publications.tnsosfiles.com/acts/112/pub/pc1092.pdf

203 https://www.azleg.gov/legtext/53leg/1R/laws/0316.pdf

204 https://www.arkleg.state.ar.us/Home/FTPDocument?path=%2FACTS%2F2023R%2FPublic%2FACT595.pdf

205 https://www.legis.la.gov/legis/ViewDocument.aspx?d=1380842

206 https://www.oklegislature.gov/cf_pdf/2013-14%20ENR/SB/SB862%20ENR.PDF

207 https://le.utah.gov/xcode/Title59/Chapter1/C59-1-P15_1800010118000101.pdf

208 https://www.wyoleg.gov/Legislation/2018/HB0103

you also have to ensure to be compliant with federal capital gains tax law. Efforts to completely repeal federal capital gains taxation on gold and silver coins (which would be logical to pass, given that these are legal tender per the Constitution, if a state declares them such) have as of the writing of this book not yet been successful. Should they ever be, and should you find people who are willing to accept gold and silver coin as payment, then physical gold and silver are probably the closest possible alternative to cash when it comes to the two critical criteria: 1. privacy/anonymity, and 2. no requirement of third-party-consent. Plus physical gold and silver do not depend on electricity, internet, or integrity of servers, databases, and hackable electronic devices either. In this scenario, you would then, of course, also have the stability of value advantage at the same time.

The advantages just mentioned (works offline, privacy, independence of third party consent, retains value), of course only apply to *physical* gold and silver that you actually have possession of, or can at least reliably access at any time, regardless of bank closures etc. "Digital gold" or "digital silver" are basically just another form of electronic payment method with all the above stated risks and disadvantages, including the ability for governments and corporations to turn off your access to "your" digital gold or silver.

In fact, while electronic transfers of ownership in minute quantities of gold solve the problem of paying for small everyday purchases with "gold"[209], which would be impossible to accurately measure at every gas station or grocery store (although you could physically do that with silver and copper, as was the case with U.S. coins, which consisted mostly of copper and silver until the early 1960s), you don't solve the problem of digital control this way *at all*. If anything, you are creating a trap that may lure people confusing the fiat vs. gold debate with the cash vs. digital question into simply another

209 The reason I put “gold” in quotation marks here is that you are *actually* paying with a *claim to gold* in this scenario, not with gold itself.

form of traceability and control (see chapter VIII above). Do you think any government in the world would allow a payment provider to set up a way to transfer "digital gold", say with a credit card or the like, without subjecting them to the same "know your customer" rules as any other payment provider?

6. Barter?

When you happen to find yourself in a situation where the person whose goods or services you need happens to want something you can provide, barter may actually be a great option. In that scenario, currency is unnecessary. Currency was, in fact, invented out of the need to cover circumstances where barter was *not* practical. Several conditions have to be met for barter to work, though: both parties happen to have goods or services the other party wants at the same time and those goods or services are of comparable value.

This can certainly be a great way to build and strengthen community. For specific commercial deals this can be feasible as well, especially given the possibility to work out details in a contract substantial enough to merit negotiating a specific exchange of goods or services. Especially if substantial time is going to pass between signing and fulfilling the contract and if you are dealing with different markets and currencies, this option may be more attractive to parties than exposing themselves to the risk of substantial currency fluctuations. For this reason, barter is actually a lot more common in business to business and international trade than one would think.[210]

Outside of such scenarios, barter tends to be rather impractical in everyday life. Say you are an architect and your farmer does not need a new house or barn, you might go hungry. And how many gallons of milk is your car worth? Will you be able to drink them before they go bad? If you go to a store, especially a chain, let alone try to order something online, chances are

210 https://www.eurasiareview.com/01112024-the-development-of-global-barter-trade-analysis/

your eggs, realtor services, vintage shirt, or baseball card collection won't be accepted as payment.

Nevertheless, should our money, aka cash, ever be taken from us, we may not have much of a choice. If your social credit score falls too low and your programmable money stops working, your only way to get food, shelter, services and whatever else you need, may be through direct exchange for something you have to offer and that the other person needs or wants. This is exactly the situation countless people in China are facing under the current blacklist system[211] and over a hundred million people in Nigeria found themselves in after CBDCs were forced on them.[212]

To create some more viable exchangeability, people have historically often used common, easily recognizable and quantifiable goods, such as cigarettes, coffee, ammunition and alcohol as substitute currencies when official currencies failed or were abolished. Governments tended to crack down on such efforts, but they were often people's last resort to obtain necessities.

Given that cash is currently up for a vote (as mentioned, every transaction is a vote for the preservation or the abolishment of cash), it is currently in your hands, whether you (and all of us) may have to resort to barter in the near future or hope that someone will give you something for the promise that you'll repay him or her later (which only works with people who know you well and generally requires having built a long history of trust first) the moment there is a power outage or internet disruption. If you use cash, you won't have to.

211 https://reinettesenumsfoghornexpress.substack.com/p/dethroning-big-brother-chinas-social?r=slkvn

212 https://mises.org/mises-wire/how-cbdc-created-chaos-and-poverty-nigeria

www.preservecash.org v.1.1

XIII. HOW CLOSE ARE WE?

As of 2026, the majority of countries are researching, developing or pilot-testing digital currencies.[213] Despite the unpopularity of CBDCs, many central bankers[214] and some power-hungry individuals in various governments and NGOs around the world (to be clear: many regular bankers and many politicians are passionately opposed to CBDCs and digital control - they are some of our greatest allies!) keep pushing for them and for abolishing cash, as cash allows citizens to be too autonomous.[215]

Disastrous results in the countries that have rolled out CBDCs did not discourage those whose goal it is to use programmable money to make people do things they would never voluntarily do. The goal of these influential individuals and organizations (which includes the World Economic Forum, which openly praises the Chinese digital yuan as a model for Western countries) is to ultimately establish a system of total digital control globally, as even mainstream media is now acknowledging.[216] If that seems hard to believe (or unrealistic to succeed in a Western society), consider the following:

213 https://www.atlanticcouncil.org/cbdctracker/

214 https://www.reuters.com/sustainability/boards-policy-regulation/ecbs-lagarde-urges-eu-lawmakers-speed-up-digital-euro-law-2025-06-23/

215 https://www.berliner-zeitung.de/wirtschaft-verantwortung/ursula-von-der-leyen-macht-druck-im-kampf-gegen-das-bargeld-li.2283503

216 https://www.skynews.com.au/insights-and-analysis/how-the-world-economic-forums-elitist-vision-for-decentralised-banking-threatens-to-turn-the-west-into-a-high-surveillance-prison/news-story/9ca7302fbeb6984190bbf5bcbc6f028b

One: The invasive control and surveillance devices, often euphemistically called “license plate readers”, even though they usually capture, record, and analyze way more than just license plates[217] (Flock-cameras currently being the most notorious, though far from only, example), which councilmembers and mayors are putting up across cities and neighborhoods without asking you (and which are already notoriously being used by employees, criminals, and even law enforcement officers, to stalk people[218]), should give you an idea. The records, including movement profiles and unchangeable biometric information that private companies obtain (and which both governments and private entities have access to) this way and which allow to forever track you globally and to note whether you violated an edict not to meet anyone for Thanksgiving, had a friend over despite a "lockdown", or attended the wrong political rally, not to mention when you are and aren't home, who your friends are, who your doctor is, where you worship, work, shop, and spend your freetime, whether you smoke, whom you date, etc. etc, are beyond disturbing. Keep in mind that the entities who obtain and store this data about you get hacked and lose that data to cybercriminals, but they also have a strong financial incentive to monetize this data by selling it to third parties.

As discussed in chapter VI, surveillance and data collection create the data for the social credit score system. A cashless society provides the enforcement mechanism to ensure you can

217 For example, audio, video, exact device identifiers of every smart device passing by (smartphones, bluetooth-devices, smartwatches, etc.) facial recognition data, a person’s gait, identifying features of vehicles, such as dents, etc. If you want to learn more about the dangers of, and concerns about, Flock-cameras and similar devices by other companies, and especially the databases they create, T.Rex Arms released some very educational videos about this subject on its T.Rex Labs channel, especially:
https://www.youtube.com/watch?v=N2-bxmWOH4U
https://www.youtube.com/watch?v=8OuBWAmoxE8 and
https://www.youtube.com/watch?v=gUgwdV7SeKs

218 https://www.aclu.org/news/privacy-technology/despite-new-updates-flocks-creepy-cameras-remain-major-civil-liberties-threat

be punished for the pettiest deviation from the rules the people or algorithms setting the rules create for you.

And two: To take it straight from the horse's mouth: the general manager of the Bank for International Settlements, (BIS), Augustín Carstens, made unmistakably clear what the goal is:

> "For the general use, we tend to establish the equivalent with cash. And there is a huge difference there. For example in cash, we don't know, for example, who is using a one-hundred dollar bill today, we don't know who is using a 1,000 peso bill today. A key difference with a CBDC is that the central bank will have absolute control on the rules and regulations that will determine the use of that expression of central bank liability, and also, we will have the technology to enforce that! Those two issues are extremely important and that makes a huge difference with respect to what cash is."[219]

In other words, the stated goal is for central banks to know exactly who holds every single dollar (or peso, pound, or yen, for that matter) in existence at all times and control exactly what you can spend your money on.

Despite the coordinated push for total digitization, surveillance and control, however, the war on cash keeps falling behind schedule.[220] The European Central Bank (ECB) was originally planning to roll out the digital Euro by October 2025.[221] Now the goal is 2029.[222] Ecuador and Senegal have already canceled

219 solari.com/kfce

220 And thankfully, more and more people are also pushing back against the stalking devices that film them everytime they enter or exist their neighborhood.

221 https://thecoinomist.com/news/digital-euro-launch-october-2025-ecb-president-lagarde/

222 https://www.reuters.com/business/finance/ecbs-cipollone-eyes-2029-digital-euro-launch-2025-09-23/

their CBDCs. The Eastern Caribbean Currency Union's DCash is currently inactive (again) and the ECCB is researching a new CBDC. Nigerians took to the streets, voted their president out of office, the country's central bank governor, Godwin Emefiele, was arrested on June 10, 2023, and the new president, Bola Ahmed Tinubu, eventually made cash more accessible and the eNaira (Nigeria's CBDC) more optional again.[223] In the Bahamas and Jamaica, adoption of their respective CBDCs is way below expectations.[224]

In the U.S., the explicitly stated presidential policy on a United States CBDC until January 23, 2025 was to place "the highest urgency on research and development efforts into the potential design and deployment options of a United States CBDC."[225] Both awareness and resistance grew, however, and before these efforts could come to fruition, a new President was elected, who revoked this executive order and prohibited his government from "undertaking any action to establish, issue, or promote CBDCs within the jurisdiction of the United States or abroad."[226] Several bills have been filed in Congress to codify this policy and prohibit the Federal Reserve Bank from issuing a CBDC.[227] Every single one of these faced enormous resistance from powerful legislators in Congress, however. It took several years and multiple failed efforts until a federal law, banning CBDCs in the United States, at least temporarily, finally passed.[228] Unfortunately, even that law is set to expire

223 https://mises.org/mises-wire/how-cbdc-created-chaos-and-poverty-nigeria

224 https://onlinelibrary.wiley.com/doi/10.1111/ecaf.12621

225 Executive Order 14067 of March 9, 2022, § 4(a)(i)

226 Executive Order 14178 of January 23, 2025

227 See, for example H.R.1430 by Representative Andy Ogles (https://www.congress.gov/bill/119th-congress/house-bill/1430/text), H.R. 1919 by Representative Tom Emmer (https://www.congress.gov/bill/119th-congress/house-bill/1919/text), S. 464 by Senator Mike Lee (https://www.congress.gov/bill/119th-congress/senate-bill/464/text), and S. 1124 by Senator Ted Cruz (https://www.congress.gov/bill/119th-congress/senate-bill/1124/text).

228 Although not as a standalone bill, but as an amendment to the "21st Century Road to Housing Act." See: https://www.cato.org/blog/cbdc-

after less than three and a half years, thus reopening the door for a dystopian CBDC in America on January 1st 2031.

To date, the United States is the only country that has officially banned CBDCs, at least temporarily (plus by a very vulnerable presidential executive order[229] and, with varying details, by several states, such as Florida[230], Montana[231], Tennessee[232], and Utah[233]). The presidential executive order could, of course, once again be revoked by the next president (as happened before on this very issue). And while CBDCs may be off the table in the U.S. for the moment, the push for programmable money has simply shifted to the private sector, as the passage of the GENIUS Act shows.[234]

If CBDCs, which arguably have the potential to extinguish human freedom altogether, weren't bad enough, one could actually argue that programmable stablecoins (aka PBDCs) might be even more dangerous, as, in addition to the government, the private entities issuing them can also use them to force their own policies and ideologies onto you. And while the Fed is, at least in theory, still subject to congressional oversight and supposed to observe the U.S. Constitution, there are far fewer such constraints for private entities and Congress has way less authority to demand transparency from them.

Whether programmable money is issued by a private or government-controlled entity, the threat to your freedom is existential. **The door closes when you lose cash.** Any all-digital payment system without physical cash means the

banned-united-states

229 https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/

230 https://laws.flrules.org/2023/80

231 https://mca.legmt.gov/bills/mca/title_0300/chapter_0240/part_0010/section_0030/0300-0240-0010-0030.html

232 https://publications.tnsosfiles.com/acts/113/pub/pc0694.pdf

233 https://le.utah.gov/~2024/bills/static/HB0164.html

234 https://solari.com/the-genius-act-and-its-implications-for-financial-transaction-freedom/

permanent end of human freedom. At that point, an AI-algorithm can tell you exactly what to do or your money won't work.

So the more cashless we become, the closer we are to complete digital slavery. We are still moving in that direction, unfortunately. However, the pace changes and whether or not (and how far) we will continue, in other words, whether we will ultimately lose cash and thus our basic human rights, is not a given.

Just a few years ago, the situation looked a lot more hopeless: the war on cash was enjoying a lot more enthusiasm among governments and corporations.[235] Most people didn't think twice before swiping their credit card or tapping their phone to pay, rather than using physical cash. Sweden showed that this was not the end of the road: as early as over a decade ago, people in Sweden started to get chips implanted in their hands to replace keys and cash.[236] Mainstream media in Sweden was openly advertising chip implantation.[237] By 2018, with thousands of Swedes already willingly chipped to have their health information, contact information, and payment methods stored in an implant in their hands,[238] this technology started getting suggested to consumers in other Western countries, including by mainstream media in the U.S.[239]

Developments such as countries reversing their anti-cash policies and re-encouraging cash, show that this road is not linear. Our actions matter. If we are lazy, we are a lot closer

235 https://money.visualcapitalist.com/global-war-on-cash/
236 https://tv.aftonbladet.se/video/61726/nu-vill-jag-bara-gaa-ut-och-borja-blippa-saker
237 https://www.aftonbladet.se/nyheter/a/dd8pEO/clara-33-har-ett-mikrochip-i-handen
238 https://www.lu.se/artikel/tusentals-svenskar-skaffar-mikrochip-implantat-detta-ar-forklaringen-varfor
239 https://www.npr.org/2018/10/22/658808705/thousands-of-swedes-are-inserting-microchips-under-their-skin

than if we take action to preserve and protect the freedoms our ancestors sacrificed so much for.

We must, however, be aware that threats often simply shift forms or labels: facial and gait recognition technology, along with evermore surveillance, is already making it possible to uniquely identify people. Combined with a digital ID, an inescapable digital prison may well be on the horizon and no longer even require people to be chipped for its implementation. While you can refuse to get chipped, you may not be able to opt out of algorithms identifying your face and gait.

Likewise, a shift from central bank digital currencies to private digital currencies is a Pyrrhic victory as the actual issues of programmability and lack of privacy (plus dependence on electricity and IT) are the same.

www.preservecash.com v1.1

www.preservecash.org v.1.1

XIV. IS IT TOO LATE?

No. As long as physical cash is still in circulation and is still legal tender, you have something to fight for and a fighting chance. And be aware that you have allies![240] People around the world are waking up and realizing that while digital ID and cashless societies are marketed by central banks, the IMF and the WEF as "inclusive",[241] the reality is the opposite, as the experiences in India[242], Nigeria,[243] China[244] and the UK[245] show.

Keep in mind that every single transaction you make, every single time you pay for anything anywhere, you vote: either for the preservation of cash and freedom, or for an all-digital payment system that will control every intimate aspect of your life as soon as cash is gone.

---

240 A growing number of legislators with integrity at the local, state, and federal level is willing to carry legislation to stop CBDCs and, most importantly, to protect cash. Organizations such as the Human Rights Foundation and the Cato Institute are advocating against CBDCs. And there is a wealth of information on how you can advocate for cash at Solari.com.

241 https://www.skynews.com.au/insights-and-analysis/how-the-world-economic-forums-elitist-vision-for-decentralised-banking-threatens-to-turn-the-west-into-a-high-surveillance-prison/news-story/9ca7302fbeb6984190bbf5bcbc6f028b

242 https://www.dhakatribune.com/world/south-asia/9396/farmer-suicide-banks-call-in-police-as-india

243 https://mises.org/mises-wire/how-cbdc-created-chaos-and-poverty-nigeria

244 https://reinettesenumsfoghornexpress.substack.com/p/dethroning-big-brother-chinas-social?r=slkvn

245 https://www.britishservices.com/2025/08/13/britcard-the-uk-s-new-digital-id-is-more-dangerous-than-people-realise/

What you do today may well come back to haunt (or save) you tomorrow.

We are at a crucial crossroads right now. And the good news is that we have been here longer than those who want to take our freedom away from us had planned. From here, the road could go in either of two directions: further toward surveillance and cashlessness, or toward growing awareness, pushback and reclaiming of our basic human rights, including privacy and transaction freedom which requires the preservation of physical cash.

Concerningly close as we are to an inhumane dystopia devoid of human autonomy, it would be counterproductive, and actually too early, to be hopeless. The following chapter will evaluate several encouraging indicators of potential trend-reversals. Some of those may surprise you. They prove that the future is not lost yet.

www.preservecash.com 1

XV. A CASE FOR HOPE

Awareness is growing. While there are indeed still businesses who think it is OK to be cashless (and some will even give you some flimsy arguments why this may be a good idea and why cash is bad), more and more people are starting to realize how essential it is to protect cash and insist on its acceptance. If this trend continues, it will become too costly for businesses to send away all the customers who only pay cash. You can be one of them and make a difference! In fact, I have personally seen businesses give up on their cashless policies and start to accept cash again, especially after customers demanded it.

Never buy into the narrative that a trend is irreversible! Several years ago, Apple decided to save some money by cheaping its customers out of having a 3.5mm audiojack. Since most people don't question, many just accepted it as "the future". This never convinced me as having an audiojack just made sense.[246] For years, people told me that the ship of audiojacks has sailed. Now, nearly a decade after Apple tried to kill it,[247] the headphone jack is making a comeback with a

246 You can immediately, without setup, connect any device with a 3.5mm audiojack with any other audiodevice, such as a speaker, amplifier, headphone, microphone, etc. This requires no pairing (which can become onerous when you have paired with multiple devices in the past), the connection won't randomly drop, you don't need a battery or charger, won't run out of power, don't experience latency, save resources (and money) and don't need an antenna right next to your brain. It simply makes sense. There are countless more reasons for having a 3.5mm audiojack in *any* device, *especially* a telephone that simultaneously serves as a media player, but this is not what this book is about.

247 https://www.headphonesty.com/2025/01/headphone-jacks-slowly-making-comeback/

vengeance,[248] as more and people realize that in many daily applications, this simple low-tech solution is far superior to all the workarounds you have to put up with if your phone doesn't have one.[249] Interestingly, it is not just older people demanding features they got used to before Apple tried to tell them they couldn't have them anymore, but also, and especially, Gen Z who is increasingly buying phones with audiojacks preferentially.[250]

Modern technologies have their utility in some applications. To shop online, you need electronic payments and there are situations where a bluetooth connection may be preferable over a wired one, but that is different than being forced to use the complex high-tech way for a simple task, and the simple low-tech option being taken away altogether. For many everyday uses, proven simplicity is often superior in many ways people don't even notice or appreciate until they are gone. But as the encouraging (and to many surprising) return of the audiojack proves, it is very possible for people to create enough demand to bring something back that continues to be important, but was facing extinction.

It is actually in our hands, whether cash goes the way of the payphone or the way of libraries, printed books, railroads, stoves, and acoustic instruments. Despite serious competition form newer innovations, which have substantially decreased their market share, enough people have realized their utility and kept them alive, as some of their strengths simply cannot be replaced by their newer, more technologically advanced alternatives.

248 https://www.audioconcierge.co.uk/the-return-of-the-3-5mm-jack-why-wired-audio-is-making-a-powerful-comeback/

249 https://blog.son-video.com/en/2025/01/the-unexpected-return-of-the-headphone-jack/

250 https://www.slashgear.com/1918344/wired-headphones-coming-back-thanks-to-gen-z/

The awareness of the dangers of digital currency and for the fact that it is *by design* irreconcilable with human freedom and cannot be designed to protect privacy or freedom the same way good old-fashioned low-tech cash does, is arriving in the mainstream. When Forbes magazine publishes an article titled "CBDCs Are Instruments Of Control" and explicitly states that "all non-autocratic governments should avoid creating one",[251] when the Scandinavian pioneer countries of cashless societies[252] are reversing course as they realize that they have become too vulnerable to power or internet outages for their payments and are re-encouraging physical cash-usage, when even the Reserve Bank of New Zealand is starting to speak up in favor of cash[253], there is hope after all.

The successful (for the moment) pushback against CBDCs in the U.S. is at least an encouragement, as it goes against a trend that seemed unstoppable. Keep in mind that the previous administration was pushing hard for a digital dollar. This success proves what grassroots action can accomplish even in the face of powerful adversaries like the WEF. Just three years ago, a U.S. CBDC seemed inevitable. At the time, most Americans didn't even know what CBDC meant, let alone the life-altering consequences it would have for them and everyone they love. Courageous leaders in various states,[254] such as Senators Bill Powers and Frank Niceley, and Representatives Jeff Burkhart and Jason Zachary, have filed or passed

251 https://www.forbes.com/sites/digital-assets/2024/06/17/cbdc-are-instruments-of-control-and-theyre-here/

252 While we have talked a lot about Norway and especially Sweden, given their recent prominent advocacy for cashlessness and Sweden's demonstrated willingness to go to bizarre lenghths in this regard, Finland is often overlooked, but experimented with what some call the first CBDC (I would argue that for technical reasons, Finland's Avant project may not qualify as one) as early as the 1990s. See https://onlinelibrary.wiley.com/doi/10.1111/ecaf.12621

253 https://www.stuff.co.nz/money/360900781/reserve-bank-warns-access-cash-getting-too-hard-launches-depot-trial

254 https://www.ledgerinsights.com/11-states-have-pending-anti-cbdc-legislation-south-dakota-votes-in-favor/

legislation to stop CBDCs in their states.[255] Awareness grew. And soon thereafter, Donald Trump stated that there would not be a CBDC with him.

While this won't suffice by itself unless we preserve cash, the pushback against CBDCs and the reemerging appreciation for physical cash is encouraging and shows that the completion of the digital concentration camp is not inevitable. We *do* still have a fighting chance.

Some of the most cashless countries in the western world, including Norway and Sweden, have realized that they went too far and made themselves too dependent on uninterrupted electricity and internet for the mere ability to pay. Senior politicians in both countries are working on ways to re-encourage the usage and acceptance of physical cash. Several states in the U.S. have enacted laws clarifying that businesses must accept cash. Congressman John Rose of Tennessee has also introduced federal legislation (the so-called "Payment Choice Act") to do the same nationwide.[256] The Senate version (S.2326) was filed as a bipartisan bill by Senator Kevin Cramer, a Republican from North Dakota, and Senator John Fetterman, a Democrat from Pennsylvania.[257] Legislative efforts on the state level likewise show that protecting cash is a strong bipartisan issue. Switzerland even enshrined cash in its constitution.[258]

The increasing understanding of the advantages of cash, especially for privacy and budgeting, among younger generations, is especially encouraging and a surprisingly strong driver of the popularity of cash experiencing a comeback.[259] Just as we are learning with their growing demand for

255 https://solari.com/heroes-of-the-week-september-30-2024-tennessee-state-senator-bill-powers-and-representative-jeff-burkhart/

256 H.R.1138 of 2025 https://www.congress.gov/bill/119th-congress/house-bill/1138/text/ih

257 https://www.congress.gov/bill/119th-congress/senate-bill/2326/cosponsors

258 https://www.admin.ch/en/cash-initiative-and-counter-proposal

audiojacks on smartphones, younger generations are a lot more independent in their thinking than older generations tend to give them credit for and don't always blindly continue a trend that previous generations all too willingly followed. In fact, history suggests quite the opposite.[260]

Ironically, while for many Baby Boomers, Gen-Xers, and Millenials technical innovations appeared so cool, new, and trendy that a lot of them all too eagerly not just embraced them, but often also silently agreed to give up crucial proven backup options without giving it much thought, generations Z and α grew up with a painful awareness of the shortcomings the newer high-tech methods come with, as well as a yearning for the privacy previous generations enjoyed and took for granted.

Looking at the proven reliability of mature systems and technologies, such as wired headphone connections, dumbphones, or cash, they often have a much-needed fresh mindset when looking at the options and see that there are useful applications for both. They use digital media, such as mp3, but are re-embracing physical media, such as books, tapes and vinyl records as well. They tend to appreciate the option to wirelessly pair their phone to a bluetooth speaker at a party or to shop online, but they are, quite reasonably, not happy to give up the ability to use the more low-tech option where it is superior, such as simply plug a headphone or audio cable directly into their phone, take a break from constant trackability and social media bombardment, or hand someone a $20 bill without having to risk data breaches, judgment by third parties, or technological hiccups and hassles, when a simple

259 https://www.cashmatters.org/blog/gen-z-shows-that-cash-belongs-in-the-future-of-money/

260 Demographer Neil Howe and historian William Strauss studied and explained this phenomenon in detail in their excellent book "Generations: The History of America's Future, 1584 to 2069", published by Harper Collins in 1991, ISBN-10: 0-688-08133-9; ISBN-13: 978-0-688-08133-1

exchange of physical cash would do the trick. In essence: they demand both options. We could all learn from that.

Gen-Z appears to also be a lot more aware of the psychological effects described in part 5 of chapter X, which make spending feel more real when done with physical cash, thus making saving and budgeting a lot easier, which is also why they are embracing "Cashstuffing" more enthusiastically than previous generations.[261] Per a study conducted by Creditkarma in 2023, 69% of Gen-Z used cash more often than the previous year and nearly a quarter of that generation used cash for most of their purchases.[262] Ironically, only about half of Generation X did so and only 37% of baby boomers.[263] On the one hand, Millennials, Gen-Z, and Gen-α are tech-savvy and considered "digital natives", but they are also often "digitally fatigued" and increasingly embracing the analog world.[264]

These observations show that the future is not settled yet, and a cashless future is, thank God, still far from certain. But each of us plays a role in deciding which direction we are heading.

www.preservecash.com

261 https://www.investopedia.com/gen-z-s-and-the-cash-stuffing-trend-11731846

262 https://www.creditkarma.com/about/commentary/cash-is-king-for-gen-z-as-cash-stuffing-trend-catches-on

263 https://www.paymentsjournal.com/gen-z-is-embracing-cash/

264 https://www.dieboldnixdorf.com/en-us/banking/insights/blog/why-gen-z-still-value-physical-money/

XVI. WHAT LEGISLATORS CAN DO

Note: even if you are not a legislator yourself, you can talk to legislators and ask them to sponsor legislation to protect cash. You can even help them pass such legislation, by talking to committee members, writing talking points, offering to testify before committees, bringing in others to testify, etc.

1. Laws Requiring Cash Acceptance

The key priority is clarifying that businesses and government entities must accept cash and that nobody can be forced to accept payments other than in cash. Several states and cities have already passed such legislation.[265] Massachusetts was the first state to do so all the way back in 1978.[266] At least eight additional states plus the District of Columbia have enacted similar laws in the last decade.[267] Two more have passed more

265 https://www.atmmarketplace.com/articles/is-cash-legislation-making-a-comeback/

266 https://malegislature.gov/Laws/GeneralLaws/PartIII/TitleIV/Chapter255D/Section10A

267 These include:
Connecticut:
https://www.cga.ct.gov/current/pub/chap_420l.htm#sec_21a-434
New Jersey:
https://pub.njleg.state.nj.us/Bills/2018/S3000/2785_R2.PDF
Colorado: https://leg.colorado.gov/bill_files/54231/download
Oregon:
https://apps.oregonlegislature.gov/liz/2022r1/Downloads/MeasureDocument/SB1565/Enrolled
New York: https://legislation.nysenate.gov/pdf/bills/2025/s4153a
Delaware: https://delcode.delaware.gov/title6/c025h/index.html
Montana:
https://mca.legmt.gov/bills/mca/title_0300/chapter_0140/part_0020/section_0280/0300-0140-0020-0280.html

limited scope versions.[268] If your state hasn't passed a law protecting cash yet, it is time to do so.

As just mentioned, bipartisan federal legislation to that extent, H.R.1138 / S.2326, is pending as well.[269] This bill needs to pass! If you are reading this book after the 2026 election and H.R.1138 / S.2326 has not passed,[270] a new bill like it needs to be reintroduced. Given the plain language of 31 U.S.C. § 5103, which reads "United States coins and currency (including Federal reserve notes and circulating notes of Federal reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues.", this one should be an easy vote. More Representatives and Senators should sign on to this bill.

Keep in mind that whether people have and can use cash when the power or the internet go out, especially if they stay out for a few days, can make an existential difference for how well your district will be able to cope in case of a disaster and whether people will become desperate or able to remain civilized.

From a policy standpoint, it is therefore helpful to view cash the same way we view backup generators, fire departments, roads, or other critical infrastructure: we cannot afford to neglect them or let them atrophy. If our pipes, power lines, or roads are not maintained, we will eventually face major problems. If we allow the infrastructure for cash to disappear, we will sooner or later come to regret that just as bitterly.

Rhode Island: https://webserver.rilegislature.gov/BillText19/HouseText19/H5116A.pdf District of Columbia: https://code.dccouncil.gov/us/dc/council/laws/23-187

268 Idaho State Representative Heather Scott, for example, passed a bill (HB 417 in 2024), which clarifies that government entities must accept cash and are not allowed to charge an extra fee to anyone paying with cash: https://legislature.idaho.gov/sessioninfo/2024/legislation/H0417/

269 https://www.newsweek.com/new-cash-law-would-change-stores-nationwide-full-list-of-cosponsors-11107722

270 At publishing time, it appears all but certain that this bill won't pass before the election, as there hasn't been any movement on it in over a year and the election is days away.

Both when it comes to public safety and when it comes to anti-discrimination, it is standard for the legislative branch to pass laws ensuring businesses don't violate basic standards. You cannot open your doors to the public without a fire inspection or without having a parking lot for disabled people. You have to abide by fair trade practice laws. Having to accept legal tender is no different.

Such legislation is actually very popular with the voter base, too. The Siena Research Institute conducted a survey on behalf of the Payment Choice Coalition, which found that 85% of voters said they would support legislation requiring retailers to accept cash, and 68% of respondents reported they plan to use at least the same amount, or more, cash in the next five years.[271]

2. Create Incentives for Cash Usage

One option is to exempt in-person cash transactions from sales tax. The challenge here is, of course, that this may reduce revenue for the state. On the other hand, tax cuts often turn out to, counterintuitively, increase revenue,[272] as they actually encourage spending and therefore have a stimulating effect on the economy and, consequentially, revenue. Examples of such legislation are Tennessee's HB 1247 by Representative Michele Reneau,[273] SB 1095 by Senator Joey Hensley,[274] and SB 1734 by Senator Frank Niceley.[275] Among the many advantages of this approach is that it leaves more money in the pockets of citizens, especially those who need it the most. This option might be the most powerful incentive legislators can create for citizens to start using cash more frequently again.

271 https://cashforever.org/articles.html?id=c38a64c6-55ed-4acb-ae6f-cd4fbaf64857
272 https://budget.house.gov/press-release/despite-cbos-predictions-trump-tax-cuts-were-a-boon-for-americas-economy-and-working-families
273 https://capitol.tn.gov/Bills/114/Bill/HB1247.pdf
274 https://capitol.tn.gov/Bills/114/Bill/SB1095.pdf
275 https://capitol.tn.gov/Bills/113/Bill/SB1734.pdf

Another option is to create tax-breaks for businesses that offer cash-discounts or whose percentage of cash-transactions is above a certain threshold. This then encourages businesses to encourage their customers to use cash.

A third (more penal) option, would be a surcharge for businesses that refuse to accept cash.

3. Put Guardrails on Programmable Money

The next step is to limit, and, at the very least, put guardrails on, programmable money. Utah, under the exemplary leadership of Senator Keven Stratton and Representative Jason Kyle, just passed a bill which did just that.[276] Legislators in other states, such as Representative Heather Scott and Senator Tami Nichols with HB 750 in Idaho,[277] and Representative Bud Hulsey and Senator Bo Watson with HB 2039 in Tennessee,[278] have filed similar legislation.

The main purpose here is to enshrine in the code that nobody can be forced to pay with or to be paid with programmable money. In other words, keep it optional before it becomes the only option. If programmable money becomes commonplace before such legislative protections are in place, you will soon find yourself unable to use your money as you please and instead be a slave to corporate policy and the decisions of AI which determine what you are and aren't allowed to buy today. Programmable money without the explicit and legally protected right to always instead use a non-digital alternative at no extra cost, will inevitably lead to a social credit score, as we saw in chapter VI, whether that score is implemented and administered by a government, private entities, or both.

276 https://le.utah.gov/Session/2026/bills/static/SB0298.html
277 https://legislature.idaho.gov/wp-content/uploads/sessioninfo/2026/legislation/H0750.pdf
278 https://capitol.tn.gov/Bills/114/Bill/HB2039.pdf

The second goal of such legislation is to prohibit decurrencying[279] based on ideological or political reasons. The bills just mentioned accomplish both goals and serve as a great template if you are considering to file a similar bill in your state (or federally).

If you want to learn more about programmable money, its dangers, origins, and implications, the Solari Report just released a publication going into this very topic in a lot more detail.[280] Beyond the legislative strategies mentioned there, it is important to note that the strongest protection against programmable money is the right to use, be paid in, and always and everywhere be able to pay with: physical cash.

4. Protect the Right to a Non-Digital Life

Citizens should never be forced to submit to digitization, especially given that both corporations and government entities have proven time and time again that they cannot be trusted with our data - neither to resist the temptation to sell it or use it against us, nor to keep it safe from cybercriminals and data breaches. When government agencies force you to buy new hardware and install invasive apps and other software on your devices, just to fill out forms and interact with them, citizens need legal protection against this abuse. Legislators can provide this protection by passing laws that require government agencies to always provide a non-digital way for citizens to interact with them. No account, username, password, authenticator-apps or QR codes. Just pen, paper, physical ID, and a counter where you can talk to a person.

279 Decurrencying is another problem that only exists with programmable money. Everybody is free to use physical cash. A virtual currency on the other hand, especially a privately issued one, can be programmed in such a way that certain individuals or entities can be excluded from its use and will simply be unable to receive or spend it.

280 "Programmable Money" by the Solari Report, 2026, ISBN 978-1-956682-19-9, purchasable at https://solari.com/product/2nd-quarter-2025-wrap-up-programmable-money/

Two cantons in Switzerland, Geneva[281] and Neuchâtel,[282] recently enshrined this right in their constitutions. Similar initiatives exist in other jurisdictions, including the U.S. They need support! Passing a law to protect people's right to live an offline life if they so chose, and to interact by non-digital means, is now more urgent than ever, as the infrastructure for real-world interaction largely still exists, but is disappearing rapidly. Adding this right to the Constitution is obviously even more powerful.

5. Prohibit Surveillance Pricing

Consider legislation against surveillance pricing and requiring pricing transparency. Physical price tags, which don't require an electronic device or other identifying means to read, need to be mandatory. For free-market advocates, it is important to remember that pricing transparency is the very foundation of an informed market.[283] Without it, the market cannot function, meaning that there is not really a market. Just like the protection of cash, this is (and should be) a bipartisan issue, as some of the legislation to address it shows.[284] As of spring 2026, at least 24 states have filed legislation to this effect.[285]

281 https://www.ge.ch/votations/20230618/doc/brochure-cantonale.pdf
282 https://www.ne.ch/sites/default/files/migration/autorites/GC/objets/Documents/Rapports/2023/23108_Decret_2e_lecture.pdf
283 https://www.theglobeandmail.com/business/commentary/article-why-shops-are-removing-price-tags-and-why-this-is-bad/
284 Take, for example, Tennessee's HB 1468 by Representative John Ray Clemmons (D) and Senator Paul Bailey (R) which had 62 cosponsors (out of 99 Representatives) from both parties. See: https://wapp.capitol.tn.gov/apps/BillInfo/Default?BillNumber=HB1468&GA=114
Connecticut's HB 5563, which passed on June 4, 2026, was likewise a bipartisan bill.
285 https://www.insideprivacy.com/emerging-technologies/state-lawmakers-introduce-new-wave-of-personalized-algorithmic-pricing-bills/

6. Bring Back Larger Denomination Bills

On the federal level, it is about time to bring back larger denomination bills. $500, $1,000, $5,000 and $10,000 bills are still legal tender, but haven't been printed since 1969.[286] As a result, they have become rare collector items and practically disappeared from circulation. Of course, due to decades of inflation, they would be much more useful (and are much more desperately needed) today than when they were discontinued in 1969.

To ensure cash does not become useless by virtue of inflation, starting to print larger denomination bills again is common sense and becoming more urgent every year. Therefore, other than legislation to protect the acceptance of cash, this one is probably the most meaningful legislative proposal to ensure physical cash does not disappear.

The standard argument against larger bills is, of course, money laundering and organized crime. But that is the old argument against any freedom. Law enforcement has other (very sophisticated) tools at its disposal to fight these crimes and neither has to nor should resort to eroding your personal freedom and privacy to do so! We were fine in 1969 when paying with cash even for large expenses, such as a brand new car, was normal. Somehow, we have since then become conditioned to perceive this as suspicious. The tools law enforcement has at its disposal to fight organized crime today are way more advanced than the ones they had back then.

If you want to sell your car, or buy a used one, especially from a private person, there is a lot to be said for the transaction being completed right then and there, as is the case with cash. If you issue the seller a check, and the seller forgets to cash it and then deposits the check months later, you may not have enough money in your account (and may be facing felony

286 https://www.investopedia.com/6-famous-discontinued-and-uncommon-u-s-currency-denominations-4773302#citation-39

charges if the check bounces). If you are selling your car, on the other hand, you probably want certainty that the buyer's check does not bounce before he drives off with your vehicle. With cash, you get paid right away and can spare yourself that uncertainty. Of course, as $100-bills lose more and more purchasing power, you increasingly need a lot of them to pay for a car or similar expense (say certain appliances, etc.). These days, a $100-bill is sometimes not even enough anymore to cover a grocery-trip for a family or a dinner for a few people.

If your legislator is serious about protecting freedom, he or she should consider introducing a bill to start printing larger denomination bills again. If you agree: call, email, or meet up with your Congressman and Senator!

www.preservecash.org

XVII. WHAT INDIVIDUALS CAN DO

1. Pay Cash Only. Always.

This is the most important, and simultaneously thankfully the easiest thing you can do as an individual. Please make this one a principle.

Keep in mind that every time you pay for anything, you vote. As the percentage of transactions conducted in cash drops, it becomes easier to justify abolishing cash altogether. No business will stop accepting cash if half the transactions happen with cash; but the lower that percentage, the more likely they are to say "well, nobody uses cash anyway" and go electronic-only. If you feel like you cannot always pay cash, for example when traveling or shopping online, use it as often as possible. Every time counts.

This is not limited to grocery stores, by the way. Whether you are at the mechanic, doctor's office, restaurant, street vendor, or a government office, it is important to pay cash, including for larger purchases. If that means getting a bunch of $100 bills, so be it. It is important to keep cash alive and its use normal. Don't be too hard on yourself if you cannot immediately go 100%. Keeping cash alive is a marathon, not a sprint. Just know that every transaction matters.

If you primarily pay electronically, be aware that others who pay cash are buying you time before the completion of a dystopia while you are, knowingly or not, contributing to bringing us closer to it. On the other hand, if you start paying

cash as often as you can (ideally always and everywhere), you are helping to protect all of us.

While the percentage of cash transactions has been in steady decline in the U.S. for a while, that trend is not irreversible. Some businesses have started accepting cash again after enough customers walked away when their greenbacks were rejected. In 2022, the Federal Reserve ordered a record number of $50 bills, as demand for physical cash was increasing.[287]

Policymakers take note of the percentage of transactions conducted in cash vs. by electronic means as well. Especially in countries with democratically elected legislators and heads of government, elected officials have an interest in being in touch with popular trends. You and I determine what that trend is at checkout. Every single one of us moves the needle every time we pay for something. Let's be aware of our responsibility when we do.

2. Refuse to do Business with Businesses that Don't Accept Cash.

Don't feel obligated to cater to a store, restaurant or other business that refuses to accept your legal tender. In fact, if you already sat down for a meal, filled up your shopping cart, or otherwise showed serious interest in doing business with them and then walk out when they tell you that they don't accept cash, your actions are much more likely to have an impact than if you cave, pay electronically and simply never come back. If you explain why you won't shop or eat there if they don't accept cash, you might even get them to think about this issue from your perspective for the first time. Especially if you are friendly, courteous, and well-informed.

287 https://www.federalreserve.gov/paymentsystems/2022_currency_print_orders.htm

3. Don't Fall for Red Herrings.

Crypto won't protect you from digital slavery (see part 1 of chapter XII). Only cash will. If you buy the narrative that the disappearance of cash is inevitable, you have already lost. Understand why only physical offline means of transaction protect your rights, privacy and freedom. That includes resilience against infrastructure disruptions, cybercriminals and social credit scores.

Understand the difference between stability of value and transaction freedom (see chapter VIII above). Don't confuse the two. Help others, who bring up the goldstandard vs. fiat debate to keep these two issues separate as well. Understand that investments and store of value are different from everyday payments. Physical gold and silver are actually a great store of value, but (due to their lack of acceptance) currently not very helpful for everyday payments; and non-electronic everyday payments are what matters for your freedom (see part 5 of chapter XII).

4. Don't Scan QR Codes. Ever!

Consider the stakes: every time you scan a QR code, you are opening yourself up to having your phone infected with malware or ransomware and having all the data on your phone compromised or stolen. If your phone stops working as a result of commands embedded in the QR code that cause your device to experience issues, you may lose the ability to make and receive phone calls, or send and receive texts.

This is especially risky if you are using a so-called "eSIM" instead of a physical SIM-card, as you won't even be able to put your SIM card into a different device (such as an old cellphone) and keep receiving calls and texts. Is that worth it? To see the menu? If a restaurant is too cheap to give you a paper menu, go elsewhere. And tell them why.

If a parking lot does not let you pay for parking without exposing yourself to having your phone compromised and your data stolen, park elsewhere (you'll also save yourself dealing with surprise charges later on).

Re-read part 10 of chapter X and if you want to learn more about QR-code related risks, do your own research into it. The links in the footnotes give you a good starting point.

Consumers have power. If we exercise it. It's called supply and demand. It works just like voting. So make your voice heard!

5. Don't Get a Digital ID! Ever!

The digital prison or concentration camp, from which there is nowhere to escape, requires two components:

1: A digital ID, and
2. Programmable money.

Without either of those two, total control is a lot harder to implement. Refuse to participate in either!

Explaining the risks and dangers of a digital ID in detail would take its own article, but a digital ID is basically a centralized platform that consolidates various personal data points, including biometric information, health records, travel history, financial details, employment and rental status, and even online activity, all accessible through a single application.[288] Whatever remnants of privacy you may have left, are gone with a digital ID. If you have it stored on your smartphone, the potential consequences you may be dealing with as the result of a cyberattack or data breach are hard to fathom.

288 https://www.britishservices.com/2025/08/13/britcard-the-uk-s-new-digital-id-is-more-dangerous-than-people-realise/

If you want to learn more about what a digital ID is and why it is so dangerous, T.Rex Arms did an excellent 25-minute video summarizing and visualizing this on the occasion of the British government moving to implement this in the UK. The video is titled "What You Aren't Being Told About Digital IDs"[289]

While a Real ID is not a digital ID, you may not want to get a Real ID either, and should insist on your DMV issuing you a conventional driver's license instead (including if they have already issued you a Real ID). Be prepared that a lot of the front-line DMV employees may not know the law and may falsely tell you that it is mandatory (it is not). For travel, you can simply use a passport or a passport card (both of which are acceptable instead of a Real ID).[290]

Given some of the characteristics of the Real ID, there are concerns that it may serve as a stepping stone toward a digital ID. This would especially be the case, should the underlying databases be extended to include additional sensitive information, such as vaccine status, social media activity, or creditworthiness. The lower the adoption of the Real ID, the more effort it will take to implement or demand a digital ID (although the two do not *necessarily* have to be connected).

A digital ID is yet another level of privacy nightmare altogether.[291] With a digital ID on your smartphone, everything you do will be tracked and identified. Your most intimate data will end up in so many hands that practically anyone will be able to know anything about you and the damage that a hacker or other bad actor can do with that information is unimaginable.[292] Needless to say that dissent or conduct

289 https://www.youtube.com/watch?v=uXQrBP_O1CU
290 https://travel.state.gov/content/travel/en/passports/need-passport/card.html
291 https://www.aclu.org/news/privacy-technology/digital-ids-might-sound-like-a-good-idea-but-they-could-be-a-privacy-nightmare
292 https://www.securitymagazine.com/articles/101605-real-id-enforcement-in-effect-what-does-this-mean-for-biometric-data-security

undesired by those in power will be immediately noticed. Imagine if this would have been in place during the draconian Covid-policies! If you cannot imagine that a government would abuse such power (and think that the Covid-years weren't that bad), ask the citizens of Cuba or North Korea. If you cannot imagine this to happen to a democratically elected western government, well it happened twice in Germany during the 20th century; and several western European countries, including Germany, France, and the UK are now arresting people for criticizing their governments again. And what is acceptable to say today, may get you banned, deplatformed, or arrested next year.

6. Make a Conscious Decision Where You Bank.

Banking with a well-governed and well-managed bank where you can have a personal relationship with people you trust and who know you makes a huge difference. You are always better off if your local banker has the authority to make a decision him- or herself, e.g. whether to give you a loan or waive a fee, than if those choices are restricted to corporate policy or AI. If there is a fraud attempt, your banker knowing you may prevent it before it even happens. If you are having a problem, being able to get a real human being on the phone who knows you, rather than a computer prompt trying to get rid of you and, if you are persistent enough, connecting you to a call-center in India, will make your life *a lot* easier. Additionally, a good bank should provide you easy access to physical cash, both at a branch and 24/7 at ATMs, and respect your safety.[293]

293 If your bank posts stickers on the door, declaring the branch a "gun-free-zone", be aware that criminals looking to mug someone or to steal a firearm from a car, are much more likely to break into your car once you walk into that bank or to mug you when you leave the building, as they very well know that their chances of succeeding are much higher in locations where you are forced to disarm. Whether you ever carry a firearm or not: avoid such locations at all costs! Even if you are unarmed, you don't want anyone to know, unless you want to advertise yourself as an easy victim. And if your bank shows this level of disregard for the safety of both its customers and employees, who are

If you don't like to move to programmable money, don't support the large banks who are pushing it. If you feel uncomfortable leaving your money with a financial felon, check your bank's criminal history (you might be surprised)![294]

Banks play a central role in determining the direction of an economy by deciding whom to grant credit to and which businesses flourish. They thereby shape a country and society. This is precisely the lever Japan pulled in order to mobilize first an unprecedented war machine and then an economic miracle literally from ruins.[295]

Fractional reserve banking means that a bank's ability to grant loans is dependent on its deposits. Hence, where you bank matters a lot! Unlike what was the case in Japan for a long time, banks in most Western countries today make their own policy choices, including which industries, businesses and individuals to lend to. This means that where you bank is another powerful continuous vote.

Researching whether your bank contributes to the funding of the control grid or is instead supportive of more liberty-oriented vibrant small business communities is another step you can take to make your capital work for the protection of liberty, rather than the destruction of it. Banks who are furthering the tightening of the control grid are often not shy about it.[296]

---

also more likely to get robbed if a would-be robber knows that they cannot defend themselves, then you may want to chose a different bank. Such policy decisions are usually a good indicator of other poor decisions and policies.

294 https://www.justice.gov/archives/opa/pr/five-major-banks-agree-parent-level-guilty-pleas

295 Princes of the Yen, by Professor Richard A. Werner, ISBN 978-3-946333-01-2-Paperback, ISBN 978-3-946333-03-6-Hardback

296 https://www.jpmorgan.com/payments/payments-unbound/volume-3/building-a-smart-grid

If you want to evaluate whether your bank is a good choice for you, or if you are trying to find one you feel comfortable with, the Solari 4-part series on building a successful relationship with a great bank is a good starting point.[297]

7. Be Conscious What You Fund.

Any resource allocation serves as a vote. We just discussed the importance of whom you bank with. On that same token, you can also reassess what you fund with your investments. If your savings (including 401(k), retirement funds, etc.) are invested (whether directly, e.g through stocks, or indirectly, e.g. through mutual funds that invest in these stocks) in companies that build the very control grid you are concerned about, you may want to consider pulling your capital out of those and investing it instead in stocks of companies that provide goods and services you like, provide working conditions you agree with and are good stewards of the environment and our society.

Even better: if you personally know business owners you like and trust, including friends and family members, you can invest in their businesses. I have personally seen parents who invested in their children's startups and whose children created successful companies with many employees as a result.

Think of your capital as energy that fuels whatever it is invested in. It can fuel freedom or tyranny, your friends and family or anonymous entities. Some publicly traded companies actually do good deeds and benefit society, others cause great harm and suffering. It is important to discern. You don't have to invest every single penny into a 100% perfect project. It is perfectly OK to diversify and I would actually consider it prudent to keep some funds liquid and have some in stable, but not necessarily productive investments (e.g. land, precious metals, bonds, etc.). But it is important to make a

297 https://solari.com/building-a-successful-relationship-with-a-great-bank-the-four-part-series/

conscious and informed decision about each investment and to be aware what you are funding.

8. Shop in Brick and Mortar Stores.

If you want to maintain the ability to purchase goods with cash, anonymously, without your every purchase forever being recorded (and that information sold to those who may use it against you), make sure the stores that enable you to do so still exist tomorrow. Hence, buy in real brick-and-mortar stores, rather than online. If there is a local non-chain store in your area, support them first, even if they are a bit more expensive than the big chain-store. Chances are, you will get way better service there anyway, and, unlike the far-away managers and shareholders of a big corporate chain, the local owner of a mom-and-pop business is much more likely to listen to your feedback and requests. The relationships you build with the people owning and running the store may one day save you!

9. Educate Those Around You.

Whether that is a business refusing to accept cash, friends, relatives, neighbors, or people in your community. Tell them about the importance of cash. Give them this book or send them the link (www.preservecash.org). Many people have never thought about the consequences of a cashless society. So raising awareness is critical.

You can find some creative ideas on solari.com, especially in the 60-day-cash-challenge section.[298] For example, you can print or order stickers saying "Stop Digital Control - Use Cash" or "Cash = Freedom".[299] You can also hand out coins and dollar bills for Halloween, instead of candy. Attach a note or put them in a bag with a sticker, and you are guaranteed to start

298 https://solari.com/the-solari-60-day-cash-challenge/

299 https://solari.com/solari-60-day-cash-challenge-printable-stickers-and-diy-bumper-stickers/

a fruitful conversation.[300] People who tried this out last Halloween reported how children often understood this quicker than their parents and went on to tell their parents to use cash. This can be powerful!

Remember that it is a lot easier to take something away from someone who doesn't understand its value or importance. Hand a toddler a $100 bill and the toddler will gladly trade it back for a piece of candy or one-dollar toy. Try to propose that deal to a teenager! Hence, the more people understand how fundamental cash is for their very freedom, the harder it will be to take it away.

10. Talk to Your Legislators.

Get to know your state representative and senator. Talk with them about cash and legislation to protect it. See chapter XVI for examples of state bills that have already been passed, and, if you live in a state that hasn't passed a universal cash-acceptance bill yet, ask your state legislators to introduce one. If they are willing to carry such legislation, try to help them get it passed. They'll usually gladly tell you how to do that. You can, for example, call, email, or meet committee members of the committees where the bill will be heard and convince them why they should vote for it. Become a resource to them!

Call and/or email (or if you get a chance: meet) your federal congressman and senator and ask them to co-sponsor Congressman Rose's H.R.1138 (or, after the 2026 election, to introduce or cosponsor a similar bill themselves). Ask them to introduce legislation to bring back $500, $1,000, $5,000 and $10,000 bills.

300 https://solari.com/action-of-the-week-october-5-2025-get-ready-to-promote-cash-on-halloween/

11. Sign a Petition to Protect Cash.

Petitions are a great tool to raise awareness and show elected officials that there is popular demand. There are petitions in several countries, including Australia, the US, UK, the EU and EU member countries to protect cash and access to cash. Find out what petitions exist in your country to protect cash and sign one. Even better: collect signatures for one! If there is none in your country, start one.

12. Support Businesses that Offer Cash Discounts.

Many businesses, especially small local ones, offer cash discounts. This helps the business remain profitable, allows the customer to get a better deal and keeps the money that would otherwise go to swipe-fees in the community. Some businesses openly advertise this, others will tell you when you ask or simply deduct a few cents or dollars at checkout. If your local business does not advertise offering a cash discount, you could ask about it or suggest it, especially if you know the owner or manager. Then specifically support that business and tell your friends about it.

If you are a business owner yourself, consider offering a cash discount. Even if the discount is small, it may encourage some customers to use cash more often and save you money on fees as well. If you decide to do this, put up a sign at or near the register or counter telling customers about the cash discount.

If you live in South Dakota, https://sdcashdiscount.com/ is a great resource, put together by cash advocate Susan Luschas, to look for businesses you can support. If you live somewhere else, you could consider putting a similar list together for your state, city or area.

Supporting cash discounts is a great way to help reverse the cashlessness trend and encourage people who usually pay electronically to consider using cash instead.

13. Consider Getting a Dumbphone.

For most people used to being glued to their smartphones, this may be too radical of a step to take all at once. And it does come with loss of convenience. However, the benefits in improved mental health, presence in the real world, quality of social interactions, sleep quality, and many other facets of life, are enormous. Plus this is one of the most significant steps, aside from paying cash, you can take to protect your privacy and slow the implementation of a total surveillance grid. It will also tremendously reduce your risk of malware from a compromised app, QR code, or malicious website rendering you unable to make and receive phone calls or send and receive texts.

This one is, admittedly, the most radical step, and it is optional (although helpful), as far as the protection of cash is concerned. So don't be too hard on yourself if you are not yet ready to take this one. However, since it has such profound benefits for your privacy and mental health, in addition to providing you "immunity" to QR codes and their dangers (as well as countless other cyber-vulnerabilities), I decided to include it at least as a "food for thought" suggestion. If you continue to use a smartphone, you may at the very least want to delete payment and shopping apps and QR readers, and thoroughly go through the permissions you grant each app that you keep. The more apps you have installed, the more data leaks and security vulnerabilities you introduce to your device.

Just like with cash, market demand plays a major role. The higher the percentage of people without smartphones, the harder it is to force invasive and risky QR codes and apps on people. Encouragingly, dumbphones are actually experiencing a renaissance, as a growing number of people are tired of being

tracked and having their attention and mental health deteriorate.[301] And this trend is interestingly not even led by older people but by younger ones, especially Gen Z![302]

An option to consider, especially if you have gotten too used to, or dependent on, the apps on your smartphone, is to start with a part-time switch where you leave your smartphone at home more often and take your dumbphone with you for emergencies. This is a strategy more and more people (especially younger people) are choosing in order to wane themselves from their smartphones and regain control over their lives and their privacy.[303]

Many people notice a surprising improvement in attention-span, memory, presence in the moment, human interactions and overall quality of life, once they got back into the habit of not having a smartphone on them.[304]

And if someone tries to push you into scanning a QR code, be that to pay, or for any other reason, you have the perfect excuse (although, if more people were aware of the dangers of QR codes, you wouldn't even need an excuse, as discussed in part 10 of chapter X). Flashing a flip-phone (or other non-smart-phone) in response to a request to surrender your privacy and to risk your device's security, is not only increasingly cool, as the trend among young people shows, it also sends a powerful message.

www.cashonly.cash.blue v1.1

301 https://www.usatoday.com/picture-gallery/life/health-wellness/2026/07/09/people-are-ditching-smartphones-for-dumb-phones-flip-phones-landlines/90853022007/

302 https://www.punkt.ch/blogs/editorials/dumb-phone-popularity

303 https://www.gadgetreview.com/why-young-americans-are-trading-smartphones-for-dumb-phones

304 Way better battery life, less weight to carry around, improved awareness of one's surroundings, vision, and spacial orientation, are among the countless other benefits.

14. Share and Spread this Book as Much as You Can.

The more people learn about how important cash is and why, the better our prospects for our future as free human beings. Some people who have read this book had never given much thought to the importance of cash and the implications of it potentially disappearing before. I was pleasantly surprised to see the transformation after they read this book, learned about the issue, and switched to using cash themselves. Moreover, some of them became advocates for cash themselves.

Every person who spreads the word and talks to others about it serves as a multiplier. You can download the .pdf for free at www.preservecash.org and you can also purchase physical copies of this book there. Please forward the link to as many people as you can! I obviously appreciate if you purchase a physical copy (maybe even as a gift for someone?) and thereby support my work. However, most important is that as many people learn about the importance of cash as soon as possible. That is why I am making this material available for free and do not mind at all if you share it freely. In fact: please do!

15. Turtle Forward[305] and Never Give Up.

In light of what our forefathers had to sacrifice for us to enjoy the blessings of our lives today, our duty today is really very easy. We don't need to die in a battlefield trench or stand up to the King of England. We just need to use cash instead of being lazy!

People had to overcome worse odds. The pressure on Churchill to capitulate to Hitler was enormous and few people in England thought there was a point in continuing the fight. The American colonists had to pick up (and make and

305 The term "to turtle forward" refers to moving forward relentlessly and regardless of adversity, even if the odds seem hopeless.

purchase) their very own weapons and create a militia out of ordinary civilians to defeat the colonial superpower they sought independence from (a key reason for the Second Amendment); they had to defeat the world's most powerful military that way! Rosa Parks' cause appeared pretty hopeless at first. The end of the Cold War, Germany's reunion and the fall of the Warsaw Pact seemed utopian in 1988. It was peacefully brought about by people refusing to go along with the totalitarian regime any longer. And remember what all was on the agenda and seemed inevitable in 2020 and 2021! Never underestimate the butterfly effect your actions can have!

As the old saying goes: "It is the greatest of all mistakes, to do nothing because you can only do little."

www.preservecash.org v1.1

www.preservecash.org v.1.1

XVIII. USE IT OR LOSE IT

Even if you never use cash yourself, the fact that other people still do for the time being somewhat protects you from some of the worst consequences of a cashless society. For now. For example, electronic payment providers still have an interest in keeping the user experience pleasant and convenient as long as users could otherwise simply return to cash. You can still give your grandchild some coins for her piggybank or put paper money into an envelope or a Christmas- birthday- or thank-you-card. You can escape an abusive spouse or buy a surprise gift for your awesome spouse and neither will show up on a bank account or credit card statement; and what you and your spouse spend your money on won't be visible to anyone who purchases or hacks and leaks your data. Your bank won't charge you negative interest rates, someone can give you a tip or contribution, you can put cash aside for a disaster situation and decide to go to an ATM or use cash again at any point. And should your accounts get hacked, your device stolen, or the internet crash, you can still participate in society.

The moment cash no longer exists, however, your life will change noticeably. As already discussed, especially in chapter X, the user experience using any kind of electronic payment is likely to get a lot worse very quickly once cash is gone.

I cannot over-stress the fact that every single payment you make counts as a vote. That is because it either shifts the percentage of transactions conducted with cash up or down. And that percentage is a deciding factor for businesses and governments when making decisions on how much to protect and preserve cash, or whether to abandon it altogether.

Hence: if you don't use it, you will lose it!

Whenever you see the word "approved" show up on a display after paying electronically,[306] remember what this means and let it be a warning about the future you just voted for: you have given up your autonomy as a human being and have voluntarily subjected yourself to the humiliating approval of a third party! You are asking a non-present person or entity for permission, whether you are allowed to buy groceries! If you are 18 or older: ask yourself: haven't you outgrown the need to do so a while ago? If you want to buy gas, a pack of cigarettes, a pound of beef, or a new scope for your rifle, that decision should be between you and the vendor. Why are you asking a third party for permission?

Use it or lose it applies both to your option to use cash, which will go away if you don't exercise it often enough, as well as to your other choices discussed above, such as not to scan a QR code, not to get a digital ID, get a dumbphone, or support the businesses you love. They only exist as long as there is enough demand for them. Obviously, in the case of cash, the implications of this are fundamental.

306 And if you read this far and are still doing so in the first place, you may want to read this book again; and I want to apologize for having failed to convey the message compellingly enough.

XIX. CONCLUSION

Unlike our forefathers, we currently don't have to kill and get crippled in a bloody war to protect our freedom and the freedom of future generations. But we do have to preserve physical cash. If we are too complacent to do so, we will lose everything that was so costly obtained for us and we will have to answer to our children and grandchildren why we squandered their basic human freedom by being too lazy to simply use cash.

While what is demanded of us today pales in comparison to what our ancestors had to go through, we still have to accept and be willing to live with certain inconveniences lest we want to lose everything, including our dignity and basic autonomy. Remember that mask and vaccine mandates, racial segregation, and other violations of civil liberty, were not defeated by those who complied with them either, but by those who were willing to stand up against what they knew was wrong, despite doing so being very inconvenient at the time.

Let's not be distracted by red herrings such as debates about cryptocurrencies or gold standard vs. fiat. None of that matters if an algorithm won't allow you to buy bread. Let's not unnecessarily ask obscure third parties (electronic payment service providers) for permission to make an everyday purchase. Let's pay with cash instead and keep that decision between us and the vendor alone. Let's not waste our time and energy on irrelevant arguments about nonsense, including about political issues and news events designed to distract us from the real issue of personal human freedom. Instead, as Solari-founder and financial freedom advocate Catherine

Austin Fitts said: "just start using cash everywhere and anywhere you can and if enough people do it, we stop the control grid."[307]

So use cash and be vocal about its protection!

That responsibility is on every single one of us. Every day. With every transaction.

www.preservecash.org v.1.1

307 https://solari.com/want-to-push-back-against-the-control-grid-use-cash/

www.preservecash.org v.1.1

Acknowledgments

In addition to the aforementioned Catherine Austin Fitts, Claire Viadro, Sullivan Wyndham, Proctor Teague, Taylor Gallagher, Susan Luschas, Andreas Maier, Paul Howson, Isaac Botkin, and Ralf Werner, I want to also thank Elizabeth Murphy, Reese and Elizabeth Thompson, Joshua and Kimberly Edwards, Ricardo Oskam, Rebekah Ross and Carolyn Betts for inspiration to write this book and/or their help and support with aspects of bringing this project to completion.

I also want to explicitly thank the following legislators (in alphabetical order) for sponsoring brave and important legislation to preserve the fundamental human right of financial transaction freedom (and apologize to anyone I may have missed): Senator Mark Abraham, Representative Mia Ackerman, Senator Omar Aquino, Senator Paul Bailey, Representative Gary Banz, Senator Michael Bergstrom, Representative Christopher Blazejewski, Representative Jeff Burkhart, Representative Karen Camper, Representative Wlnsvey Campos, Representative Joseph Chaplik, Representative Tyler Clancy, Representative John-Ray Clemmons, Representative Michael Cloud, Representative William Conley, Senator Kevin Cramer, Assemblywoman Catalina Cruz, Senator Ted Cruz, Senator Nilsa Cruz-Perez, Representative Tom Delnicki, Senator Jonathan Dismang, Representative Doug Dublitsky, Representative John Edwards, Representative Roy Edwards, Representative Tom Emmer, Senator Walter Felag, Senator John Fetterman, Representative Mark Finchem, Representative Craig Fishbein, Representative Monty Fritts, Senator Hanna Gallo, Representative Brad Galvez, Representative Jane Garibay, Representative Edgar Gonzalez, Representative Mark Green, Representative Rusty Grills, Senator Erin Grall, Representative Kenneth Gucker, Senator Bobby Harshbarger, Representative Cedric Hayden, Senator Joey Hensley, Representative Bud Hulsey, Senator Scott Jenkins, Assemblywoman Angelica Jimenez, Senator

Jack Johnson, Senator Clark Jolley, Representative Renea Jones, Senator Michael Kennedy, Representative Dennis Kucinich, Representative Sabi Kumar, Representative Jason Kyle, Senator London Lamar, Senator Akasha Lawrence Spence, Senator Mike Lee, Representative John Lively, Senator Frank Lombardi, Representative Robin Lundstrum, Senator James Manning, Senator Spiros Mantzavinos, Representative Joseph McNamara, Representative Nicholas Menapace, Senator Bob Menendez, Senator Paul Moriarty, Senator Shane Morigeau, Representative Eric Morrison, Senator Frank Niceley, Senator Tammy Nichols, Representative Andy Ogles, Representative Donald Payne, Senator Marie Pinkney, Senator Nellie Pou, Senator Bill Powers, Senator Floyd Prozanski, Representative Michele Reneau, Assemblywoman Verlina Reynolds-Jackson, Senator Robert Rodriguez, Representative Bob Rommel, Representative John Rose, Senator James Sanders, Representative Heather Scott, Senator James Seveney, Representative Joseph Shekarchi, Senator Steve Southerland, Representative Clay Staires, Senator Keven Stratton, Senator Brent Taylor, Representative Joe Towns, Representative Alex Valdez, Senator Bo Watson, Senator Ken Yager, Senator Jeff Yarbro, Representative Jason Zachary, Representative Tami Zawistowski, and Senator Daniel Zolnikov.

www.pfeffer-group.com

About the Author

Tobi Maier is an attorney, entrepreneur, firearms instructor, and paramedic. He holds law degrees from the University of Bonn and Vanderbilt University Law School. He has worked on three continents, speaks eight languages, cares deeply about freedom, and helps legislators with their efforts to protect it. Some of Maier's early legal work was related to what happened in East Germany, a country with an overbearing and invasive government and very little individual freedom, which spied on its own citizens and killed them when they tried to flee the country. This experience had a lasting impact and instilled a deep appreciation and concern for liberty in him. He has since advised corporate clients on IT security and data protection laws, worked as a prosecutor, conducted international litigation, and is a resource to legislators and government officials. He writes legislation to protect liberty, including firearms rights and financial transaction freedom. He also gives speeches about the importance of cash.



Organizations and People to Support

If you would like to support my work, the best way is to purchase physical copies of this book at preservecash.org and hand those out to people who might read them. This way you also spread the message at the same time. Aside from that, I specifically want to recommend the following two organizations: T.Rex Arms and the Solari Report.

If you are in the market for a holster or other tactical equipment, consider buying it from T.Rex Arms (trex-arms.com). They are great people, their products are excellent, and they have supported my work for years.

If you want to learn more about financial transaction freedom and ways to protect it, as well as about a variety of related issues that can help you lead a prosperous and conscientious life, you will find a wealth of information at solari.com. Beyond the publications and information available there, they also help fight for the protection of cash, including legislatively, and support others who do the same. This book would not exist without the help and support from Solari. If you would like to support them, consider a subscription to the Solari Report (it is worth it).

I don't know all the local businesses in your area, but supporting the ones who offer cash discounts and not frequenting the ones who refuse to accept cash (after telling them why), is always a good idea.

Finally, if you have children in your life, whether your own, or those of your friends and relatives, occasionally or regularly give them some cash. Pay them an allowance, or reward them for something by giving them a few bucks. You will help them naturally learn important financial skills and they will appreciate not just you but also physical cash, which they might otherwise not come in contact with.

Glossary

AI: Artificial Intelligence. Computer algorithms based on so-called "large language models", crawling data, identifying patterns, and creating an output resembling such patterns, based on the available data, in response to a user prompt. Different from conventional algorithms in that some AI algorithms can write their own code, change themselves and develop beyond what the programmer specifically coded, which includes performing actions neither the programmer nor the user intended nor specifically prompted.

AI-Slop: Content created with generative artificial intelligence, generally regarded as cheap and low-quality, especially due to its lack of effort and accuracy.

Algorithm: A sequence of computer code written to accomplish a specific task.

ATM: Automated Teller Machine. An electronic bank terminal that enables bank customers to access their account, withdraw cash, and, in some cases, perform other basic banking functions, such as transfers.

Audiojack: A round port for the direct physical analog connection of an audio device, such as a speaker, amplifier, microphone or headphone.

Bailout: Socialization of private debt, e.g. the the debt of a private company or bank, by transferring public taxpayer dollars to the private entity in order to cover that entity’s obligations, or by reassigning that debt to the public hand.

Bail-In: Utilizing creditor or depositor funds to cover liabilities of the debtor or custodian.

Barcode: A machine-readable sequence of vertical lines of varying width, which directly translates into characters (letters, numbers, and a limited

number of commonly used special characters). Very limited in how much information can be contained in it (impractical beyond a number of less than 20 digits or a word or two).

Blockchain: A distributed ledger, or growing chain of data entries, that serves as a permanent and unchangeable record of all entries ever made on it. Used for cryptocurrencies to permanently record all transactions.

Bot: A computer program or algorithm that automatically performs repetitive but voluminous tasks, such as writing and sending emails (often for marketing or spam purposes) or crawling databases or websites for indexing or analysis purposes. Shortened from "robot." By itself, bots are not categorically good or bad. They can be extremely helpful, but also disruptive and annoying, depending on how and what for they are used.

Captcha: Challenges, such as illegible text and images a user has to try to solve and click through in order to access a website or for a task to proceed. Very effective in blocking actual human beings and making the internet less and less accessible.

Cashstuffing: A simple method for budgeting by assigning envelopes or other containers to certain spending categories and then putting the allotted funds (in physical cash) into the respective envelopes (i.e. stuffing cash into them).

CBDC: Central Bank Digital Currency. A digital token that only exists virtually, not physically, and is issued by a central bank. A CBDC is one form of programmable money. It gives the issuer (and potentially others) complete knowledge of, and control over, each individual transaction.

Cryptocurrency: A virtual digital asset, the transactions of which are permanently recorded on an encrypted public distributed ledger. Well-

known examples are Bitcoin and Ethereum. Cryptocurrencies are a form of programmable money.

Cybercrime: Crime committed via the use of computers and networks, including the internet, often exploiting security vulnerabilities in software or hardware, defrauding careless users or tricking them into revealing credentials, or gaining and misusing unauthorized access to networks, servers and devices by other means. Given the ability to potentially access anything on the internet from anywhere on the planet (hence the name World Wide Web, which is what www. in a url stands for), cybercrime is very often committed internationally from countries far away, making effective law enforcement extremely difficult.

Data Broker: A company collecting and combining data, including often deeply personal information about you from various sources and selling it to others.

Digital ID: A unique identifier for a human being, similar to a conventional ID (e.g. passport or driver's license), but existing in digital form, e.g. on a smartphone. Used by totalitarian governments to control access to the internet and allow for complete surveillance.

DMV: Department of Motor Vehicles. Common abbreviation in the U.S. for the government office where you get your driver's license or register a vehicle.

Dumbphone: The opposite of a smartphone. A classic cellphone (or mobile phone), usually with physical keys as opposed to a touchscreen, which allows for calls and texts, but has very limited functions beyond that and often no internet capabilities.

ECB: European Central Bank.

ECCB: Eastern Caribbean Central Bank.

ECCU: Eastern Caribbean Currency Union.
Enshittification: See part 12 of chapter X.
ESL: Electronic Shelf Label - Price tags in stores that can be remotely or automatically updated, e.g. to respond to smart devices detected nearby and allow surveillance pricing.
EU: European Union.
FBI: Federal Bureau of Investigation.
FDIC: Federal Deposit Insurance Corporation. A U.S. government corporation supplying deposit insurance for depositors in American commercial and savings banks.
Fiat Currency: A currency created "out of thin air" and not backed by tangible assets such as precious metals (from Latin *fiat* = it shall be).
Flip-phone: Usually currently used interchangeably with dumbphone, although the term flip-phone is less precise. All early cellphones were dumphones, but for the longest time, most didn't physically flip open or shut and were therefore technically not flip-phones. Recently, some smartphones were introduced that have two screens and, depending on the physical mechanism, could be understood as "flip-phones" by some, even though they are not dumbphones. As of the writing of this book, most people mean a non-smartphone when they use the term flip-phone.
Flock-Cameras: Surveillance devices from a company called Flock Safety that record audio, video, unique device identifiers of passing smart devices, facial recognition and other biometric data, as well as license plate and other identifying vehicle information, such as stickers and dents.
GENIUS Act: Guiding and Establishing National Innovation for U.S. Stablecoins Act. A 2025 federal law that governs payment stablecoins in the U.S.
Ghost Tapping: The unauthorized initiation of a tap-to-pay charge by reading out the contactless payment

information of an RFID enabled credit card or smartphone of a person in close proximity.

Headphone Jack: See audiojack.

HTML: Hypertext Markup Language. A programming language for websites.

IMF: International Monetary Fund. A global financial agency of the United Nations.

IOU: Phonetic abbreviation for "I owe you." Describes the concept of a certificate for a claim that can be traded with the promise of redemption.

IRS: Internal Revenue Service. The United States Department of Revenue's tax collecting agency.

JavaScript: A programming language for internet content.

KYC: Know Your Customer. Legal requirement for payment and financial service providers to verify the identity of their customers.

KYT: Know Your Transaction: KYC but additionally requiring the provider to know details about the individual transactions the customer or user attempts.

Malware: Software designed to compromise, destroy, or disrupt, gain unauthorized access to, or steal data from a computer system, including a smartphone, server, laptop, network, or smart device, or to gain control over such device or system.

Negative Interest Rates: Interest charged to an account, rather than credited to it, as a penalty, rather than reward, for having money in the account.

NGO: Non-Governmental Organization.

PBDC: Private Bank Digital Currency - A digital token that only exists virtually, not physically, and is issued by a private bank or issuer. A PBDC is one form of programmable money. It gives the issuer (and potentially others) complete knowledge of, and control over, each individual transaction.

Phishing: A scam method that tricks users into voluntarily providing their access credentials, such as user

names and passwords, or other sensitive information, such as social security numbers or payment information, by sending them emails with malicious links, but that look like they come from a legitimate source, or by sending them to fake websites that look like the ones the user expects to see (such as a bank or payment portal).

Piggybank: A savings box, often in the form of a toy, such as a porcelain or plastic pig with a slot at the top that allows for the insertion of coins (or folded notes). Some piggybanks have a lid at the bottom that allows for the opening and emptying of the container, some (less common, usually made from porcelain) require the destruction of the object to retrieve its content.

POS: Point of Sale.

Programmable Money: See chapter V.

Pyrrhic Victory: Means a hollow or temporary, and ultimately meaningless victory. Often used interchangeably with winning the battle but losing the war. Named after the Greek king Pyrrhus of Epirus, who between 280 BC and 275 BC fought several victorious battles against Rome, but lost most of his soldiers and commanders in the process, which rendered his victories meaningless and Pyrrhus ultimately unable to permanently defeat Rome.

Quishing: Phishing via the use of QR codes.

QR code: Short for "Quick Response Code" - A square with a huge number of little dots or squares which translate into computer code. Unlike barcodes, QR codes contain trackers and can contain enormous amounts of code, which can instruct a scanning device to perform a variety of functions beyond just taking the user to a certain webpage. Given the obscurity and volume of the code in a QR code, malware and other

unwanted code can be embedded in a QR code without being apparent.

Real ID: A state issued identification card (ID), such as a driver's license, which meets the requirements of the federal Real ID Act and is recognizable by a star printed on it (which conventional state IDs don't have). Can be used for domestic U.S. air travel in lieu of a federal ID (such as a passport book or passport card).

RFID: Radio Frequency Identification: a technology with which digital data can be encoded in a smart tag, label, or other object, such as a credit card. The technology allows for contactless reading of the digital information, thus enabling contactless payments, among other uses.

Shadow Profile: A dossier built about a person from data that person never directly shared with the party compiling the dossier. Often assembled by data brokers or parties in the data collection business such as social media platforms.

SIM card: A small physical integrated circuit board card with contacts that look like the chip-contacts on some credit or debit cards, and which gets inserted into a cellphone to identify the device as the one associated with a certain phone number. SIM stands for Subscriber Identity Module. A removable physical SIM card ensures that your phone number is not tied to a specific device. If your device dies, becomes inoperable or gets hijacked by ransomware, you can take out the SIM card, insert it into another phone and continue to send and receive texts and make and receive calls with your phone number. This is not possible for so called “eSIMs” which are virtual. If you are dependent on an eSIM and your phone dies, you are out of luck. Only your phone carrier can reassign your number to a different device with an eSIM and you may be

required to install a special app and download a unique key file or code from your carrier.

Smart Contract: A dynamic contract that can be embedded in programmable money and cause the money to automatically perform certain transactions without the user specifically initiating each transaction.

Spam: Unwanted and usually mass-generated communication, often for marketing purposes. Most notorious in the form of mass emails or random marketing phone calls.

Stablecoin: A digital token, such as a cryptocurrency, which is pegged in value to the value of a specific other denominator of value; e.g. a payment stablecoin in the U.S. is always worth exactly one dollar. Stablecoins are a form of programmable money.

Third Lock: Metaphor for the dependency on the consent of third parties in the case of electronic transactions. In a two-lock situation (such as for transactions conducted with physical cash, barter, or physical gold and/or silver coins) only the payer and the payee (e.g. seller and buyer) have a "lock", i.e. the ability to say yes or no to the transaction. With electronic payments, third parties (such as the payment provider, governments, etc.) have a lock as well and can approve or deny the transaction.

Trudeauing: Freezing bank accounts for political reasons.

URL: Uniform Resource Locator; colloquially referred to as a web address. You find it in the address bar of a browser (for example www.preservecash.org, www.congress.gov, or https://faq.usps.com/).

WEF: World Economic Forum.

Working Poor: People who are employed and working but whose household income falls below the poverty line, often not allowing them to cover necessary expenses, despite being employed.