Sleepwalking into disaster? Requirements engineering for digital cash (Position paper)*

Frank Stajano (✉)[0000−0001−9186−6798]

University of Cambridge (United Kingdom)
frank.stajano@cl.cam.ac.uk
stajano.com

Abstract. Digital cash seems inevitable. But it's not going to be bitcoin or the like, which will be regulated out of existence rather than being allowed to become mainstream currency. Central Bank Digital Currencies promise to eliminate crime but come with many of the problems that bitcoin set out to avoid. What do we actually *need* from digital cash? We had better figure it out before building and deploying unsuitable systems.

Keywords: Digital cash, CBDC, bitcoin

1 Introduction

Nowadays we use coins and banknotes less and less. It appears inevitable that physical cash will vanish into insignificance. For some of us, who no longer even carry a wallet, this seems to have largely happened already in everyday life. Are we heading towards digital cash? What do we even *mean* by digital cash, and how is it different from credit cards or bank transfers?

Imagine currency that, if you didn't spend it by a certain date, would self-destruct—like the glasses with the instructions for the secret agent in the opening credits of *Mission Impossible II*. And I am not just talking metaphorically about the value of currency getting eroded by inflation: I'm talking about currency that *completely* self-destructs. Currency that, like a carton of milk, has an expiry date, after which you just can't spend it any more. With payments becoming digital, with cash itself becoming digital, that's all possible. Digital currency can be programmed to disappear.

And of course it doesn't stop there. Digital currency can be traced, to stop tax evaders and to track down criminals through their illicit profits. It can in theory be programmed to pay any tax due as part of a purchase, instead of

* Author's preprint, revision 45b of 2023-05-31 23:12:20 +0100 (Wed, 31 May 2023). In *Proc. Security Protocols Workshop 2023*, Springer LNCS 14186.
BTW—I mumble to myself a lot. It's OK to skip all these footnotes! ☺

hoping that the relevant party will pay tax later. And it would not even need to be programmed uniformly: every individual dollar could be programmed differently, with your dollars working differently from my dollars. Currency could be programmed to make a rich person pay more taxes than a poor one[1]. It could be programmed so that a criminal's currency suddenly stops working altogether. All this is possible and some of it has already been implemented and deployed with e-CNY (China's digital yuan or digital renminbi) in 2020 and 2021, in trials involving tens of thousands of people [13,4].

In this position paper I'm trying to make sense of all this, of where we are heading and where we *should* be heading. I am not trying to sell you a solution: I am instead offering controversial questions that I hope will trigger fierce debate, and I am well aware that I don't have all the answers. Here are the points I am going to defend:

1. Digital cash is unstoppably happening, but it won't be bitcoin or one of its hundreds of imitators.
2. What will happen instead is government-issued digital cash (CBDCs), which has radically different properties.
3. Many of the claims made about the advantages of the various forms of digital currency are exaggerated and unfounded.
4. Digital cash, whatever its form, cannot eliminate crime: at most it will simply displace it. (If we were smart, we'd figure out where to in advance.)
5. There is no consensus yet on a subset of features of digital cash that would be desirable and fair for the honest citizens of the digital society, and some of the desirable features are mutually incompatible. We don't know how to build digital cash technically (although many partial solutions have been put forward) but, before that, we don't know what we *need*.
6. In a rush not to be overtaken by our nation-state competitors, we are on track to build and deploy a dangerously inappropriate technology infrastructure that will be very hard to remove later, both for reasons of lock-in and inertia and also for more sinister reasons of surveillance and repression. It is crucial that we get the requirements right before succumbing to the insidious disease of do-something-itis.

2 Setting the scene

An item of digital cash is a bit string. It can be conveniently moved around, like any bit string, but it can be spent anonymously, like cash. An apparent contradiction because a bit string can, by its nature, be duplicated (and thus spent) arbitrarily many times, making it useless as cash. Thus the main cleverness in digital cash research, since its inception, has been the invention of mechanisms for the prevention (or at least the reliable and timely *detection*) of multiple

[1] Or, a cynic might suggest, vice versa—since it's ultimately the rich people who determine how currency works.

spending, but without resorting to the trivial yet privacy-invasive countermeasure of keeping a log of who paid whom (as is commonly done by cheques, credit cards and bank transfers in general).

In 1983 David Chaum introduced the *blind signature* [8], a fundamental cryptographic building block towards anonymous digital cash. On top of that, he and others [10,5,9] constructed various ingenious online and offline digital cash schemes. But multiple attempts at commercialising these significant theoretical developments resulted in failure. Digital cash largely remained little more than an amusement for cryptographers until the advent of bitcoin.

In 2008, someone going by the pseudonym of Satoshi Nakamoto introduced bitcoin [16] and its so-called blockchain[2], an alternative solution to the double-spending problem. Through a combination of a working open source implementation and a libertarian ideology that appealed to hackers[3], bitcoin attracted a critical mass of technically competent and evangelically committed early adopters and grew virally, succeeding where its many predecessors had failed.

As soon as bitcoin started to get some traction, it spawned legions of imitators, all eager to have *their* version of digital cash[4] become the standard. A few cryptocurrencies proposed significant innovations; several only offered minor incremental improvements; most were just fraudulent pump-and-dump schemes. The most noteworthy was perhaps Vitalik Buterin's Ethereum [7], whose significant distinguisher was smart contracts[5]. It rose to second place in market capitalisation compared to bitcoin.

In the intervening 14 years since its introduction, bitcoin has retained its dominant market position over other cryptocurrencies and its rather volatile exchange rate with the US dollar has spanned more than 6 orders of magnitude, from 10,000 bitcoins for two pizzas in 2010 to over 60,000 dollars per bitcoin in 2021. Bitcoin has been accepted as payment by Tesla (which then changed its mind a few months later), declared legal tender is El Salvador and Venezuela, used as the preferred mode of payment for ransomware, and outlawed in China and elsewhere. And we haven't even mentioned the wasted electricity. All along, its use as an actual medium of financial exchange has been insignificant compared to its hoarding for financial speculation.

But in this paper I won't be going into a history lesson or a taxonomy of digital cash proposals. I am rather more interested in the question of: *where should we go next* with digital cash? I want us to understand **what a free and fair digital society actually *needs*** rather than immediately rushing into inventing how to build it (which many have already done, but before answering the question satisfactorily—or at all).

[2] Interestingly, a term that was never actually used in the original bitcoin paper.
[3] With more faith in working code than in meddling governments and Central Banks.
[4] Of which they had conveniently stashed away the first few millions.
[5] The smart contract idea predates Ethereum: it was originally put forward by Nick Szabo [18] in 1997 , but Ethereum implemented it and made it popular.

First of all, just so that we are all on the same page, I'm going to briefly clarify what I mean by digital cash, distinguishing its various incarnations. After that, I'll revisit and justify each of the points I mentioned in section 1.

2.1 Digital cash—what do you actually mean?

Two friends, the canonical Alice and Bob of every security protocol, discuss digital cash. Alice is a neophiliac who enthusiastically embraces new technologies, whereas Bob is a grumpy cynical sceptic who alternatively thinks he's seen it all before or, alternatively, that it'll never work. Their banter may help us distinguish, at least informally, the various forms of digital cash.
Alice: Digital cash is coming! Most payments have become digital. I no longer even carry a wallet: I pay for everything with my smartwatch.
Bob: Paying with your smartwatch is digital, yes, but that's not like cash: I can give you some coins, but you cannot pay me with your smartwatch: you can only pay a merchant, someone who has the machine that you tap your smartwatch onto.
Alice: But I can make a digital payment to you by bank transfer if you give me your sort code and account number.
Bob: But that doesn't work well internationally, across countries and across currencies. Even with the IBAN, it's slow, cumbersome and expensive compared to a cash transaction.
Alice: If you need to do international payments between private individuals you could also use something like PayPal. Competition with the incumbents (banks) gives these challengers the incentive to be much easier, quicker and cheaper for end users.
Bob: But that still leaves a trail, unlike cash, and so do all the other methods you mentioned. And I don't like to leave that trail behind me, every time I pay, which is why I prefer cash.
Alice: Then use bitcoin! That was one of the motivating design principles of bitcoin. Even if you've never used it you must have heard of bitcoin, right? Decentralised, untraceable, payable to anyone in peer-to-peer fashion, inflation-proof. It's got hundreds of imitators but it's still the number one in market cap, of the order of a trillion dollars. Entire countries, like Venezuela, have adopted it as their currency. Even Tesla accepted it as payment for its cars. You can't ignore that. Bitcoin is here to stay. Digital cash is happening!
Bob: Of course I've heard of bitcoin. It's that ecological abomination that wastes more electricity than Denmark and Finland combined. It's that Ponzi scheme that made suckers buy into an extremely volatile asset whose exchange rate with the US dollar has spanned a factor of over a million. It was the currency of the Silk Road digital black market for drug dealers, and it's also the currency of choice for ransomware extortionists and other organised criminals. Surely that's not what you want as a cash replacement in a civilised society, right?
Alice: OK, then how about a Central Bank Digital Currency? The digital dollar, digital euro or digital pound? A CBDC will be government-backed, which ensures stability, and it will allow digital payments with minimal friction. It will promote

fintech innovation, will protect citizen privacy, will deter crime and all sorts of other wonderful benefits. Just as trustworthy and reliable and universally accepted as the dollar, but digital, working across the internet, without you having to carry a wallet. How about that?
Bob: How about the digital yuan, which is already years ahead and is probably what's putting the fire under the bottoms of those who are considering the digital dollar, euro and pound? How about your every purchase being monitored by an oppressive government? How about a dictatorship being granted the power of making the currency of criminals stop working, bearing in mind that the government is free to define as a criminal anyone who disagrees with it, even if peacefully?

3 The claims I am defending

3.1 Digital cash is unstoppably happening, but it won't be bitcoin

In 2011, when few non-geeks knew about bitcoin, a friend asked me what I thought of it "as a cryptography expert"[6]. I wish I had made my answer more public at the time, as I still stand by it. I told him that, regardless of any security considerations, I did not believe bitcoin could work as money because it is not backed by anything. There isn't a deposit of gold or any other asset that you can redeem bitcoin against. As Harry Browne [6] wisely explained in 1970:

> Money is a commodity that is accepted in exchange by an individual who intends to trade it for something else. [...]
> The commodity [to be used as money] must have accepted value. It must be usable and accepted for a non-money purpose before it can serve as money. Only then can the recipient be sure he isn't receiving a white elephant.

After sharing this viewpoint with others, many of them dismissed my objection to bitcoin by observing that the dollar isn't linked to gold either (since Nixon famously left the gold standard in 1971) and neither is any other major currency nowadays. But never mind what *I* said privately in 2011: listen instead to what the most successful investor of all times, Warren Buffett, publicly said at the Berkshire Hathaway shareholders meeting in April 2022 [15], when one bitcoin was worth over 40,000 USD:

> If you said... for a 1% interest in all the farmland in the United States, pay our group $25 billion, I'll write you a check this afternoon. [For] $25 billion I now own 1% of the farmland. [If] you offer me 1% of all the apartment houses in the country and you want another $25 billion, I'll write you a cheque, it's very simple. Now if you told me you own all of the bitcoin in the world and you offered it to me for $25, I wouldn't take

[6] Overestimating my competence, or flattering me, or both.

> it! Because... what would I do with it? I'd have to sell it back to you one way or another. It isn't going to do anything. The apartments are going to produce rent and the farms are going to produce food.

My point was, and I was glad to discover someone infinitely more qualified than me making it more dramatically: *bitcoin is not backed by anything.* Although its technical foundation is impressively ingenious (if irresponsibly wasteful), its financial value is built on expectation and hype, not on inherent utility. This has made it wildly volatile. It may have a capitalisation of half a trillion dollars as of 2023 but that's all speculation, not actual trade. These 0.5 trillions are not purchases in exchange of goods[7].

But the most powerful reason why bitcoin will never become currency has been articulated in 2021 by another one of the world's most savvy investors, Ray Dalio [14], the founder of Bridgewater, the world's most successful hedge fund:

> Every country treasures its monopoly on controlling the supply and demand [of currency]. They don't want other monies to be operating or competing, because things can get out of control. So I think that it would be very likely that you will have [bitcoin], under a certain set of circumstances, outlawed—the way gold was outlawed.

So there you have it. Either bitcoin will fail, and then it will be irrelevant; or it will succeed, and then it will be banned.

3.2 CBDC will happen, but it's rather different

Chaum's digital dollar was, in essence, a bank-signed bitstring where the bank said "I promise to pay the bearer on demand the sum of 1 $". It was given to you by the bank in exchange for a deposit of a dollar, and it was redeemable for that dollar, so it was anchored to some value[8]. It was signed by the bank, so nobody could produce a counterfeit string. It had a serial number, so nobody could redeem it from the bank a second time. And it was signed with a blind signature, crucial innovation, so the bank didn't know to whom it had issued a certain serial number. Offline double-spending prevention was achieved with a cut-and-choose protocol such that if the currency was spent once, the spender remained anonymous, but if it was spent more than once then the double-spender's identity would be revealed, which was supposed to be a deterrent (although the recipient of the doubly-spent currency still lost out).

Bitcoin deals with double-spending differently: it maintains a public, distributed, peer-to-peer, tamperproof, append-only ledger of all transactions—the famous blockchain. Anyone who is offered a bitcoin can look it up on the

[7] If we ignore the drug sales that my fictional Bob mentioned earlier and that actually happened on Silk Road, but which were still a tiny fraction of the overall bitcoin economy.

[8] Insofar as you believe that a fiat currency like the dollar has any intrinsic value, which is in itself debatable—but that's a separate story. Let's suspend disbelief for the time being.

blockchain and check whether it has already been spent. This approach inherently introduces latency issues, as well as being very wasteful computationally[9]. In a Central Bank Digital Currency (CBDC), instead, the ledger is not a distributed peer-to-peer data structure: it is kept at the Central Bank. The logic is: assuming you trust dollars, you trust the Central Bank that issues them, and therefore you might as well trust the Central Bank to hold the ledger. Now, this argument is far from watertight; firstly, not everyone agrees with the baseline assumption that the Central Bank is trustworthy, which was one of the reasons why bitcoin was created[10]; secondly, believing that the Central Bank will protect the value of the currency is not the same as trusting the Central Bank with the power to observe all your financial transactions, much less trusting it with the power to change at will[11] the value of *your* individual pieces of digital cash.

Keeping the ledger at the Central Bank has two main consequences: one, the centralised ledger is much simpler and much more computationally efficient to implement than the peer-to-peer distributed ledger; two, it allows the Central Bank to retain control of the currency—in particular, of how much currency is in circulation. Arguably the main driver for the creation of bitcoin was precisely to *remove* that control from the Central Bank so that they could no longer print currency arbitrarily[12]. Printing currency is a stealth tax on anyone who saved any of the currency; it distorts the reference[13], fooling people into evaluating prices incorrectly; and is one of the root causes of inflation. But governments want to be able to pull those levers to fix big problems that require big infusions of cash they don't have, like the COVID-19 pandemic or the invasion of Ukraine, and changing the value of currency is much quicker and easier than the politically impopular alternative of imposing a new tax (which would be more explicit and honest), so they definitely won't want to lose the ability to do that.

The role of the Central Bank, as opposed to the commercial banks, is that it manufactures the currency that circulates in the economy and that other participants exchange. The bank account I have at a commercial bank is a claim I have on that bank that, if I go there, they'll give me back that amount of Central Bank currency. At the base level, the commercial banks *just move around* the currency created by the Central Bank, whereas the Central Bank is the only entity that can *create* more currency. At the next level of sophistication there is the fractional reserve system, where the commercial banks lend out the currency that customers have deposited (within limits set by the Central Bank), which

[9] But bitcoin's first mover advantage has prevented more efficient proposals, no longer based on proof-of-work, from overtaking it.

[10] Although, after all, most of the speculators who buy bitcoin for dollars today do so in the hope of exchanging it for more dollars later, so they do still rely on the dollar being worth something to them.

[11] Or: under coercion from the evil government that is after you as a political dissident.

[12] The practice euphemistically referred to as "quantitative easing".

[13] The "reference" being the value of one unit of currency, which decreases if more units are introduced. Distorting the reference that is used for pricing goods is as destabilising and perverse as surreptitiously changing the length of the standard metre or the duration of the standard second.

creates additional liquidity and in turn further devalues the currency (albeit to an extent still controlled by the Central Bank).

The Central Bank would lose this pivotal role, and this crucial ability to exert an influence on the economy, if the digital currency that people used for payments were created by some other entity. This is in essence the Ray Dalio objection I cited in section 3.1 on page 6.

3.3 Claims about digital cash are exaggerated and unfounded

Proponents of digital cash make various claims about its benefits but, although as a pro-privacy person I'd love to be a believer, I remain unconvinced.

Convenience. Is there any structural reason why digital cash should be more convenient than what we can already do with non-anonymous bank transfers, credit card transactions and so forth, given the right commercial incentives? Maybe a bank transfer is cumbersome but compare with Apple Pay[14]. That's also, ultimately, a hidden chain of bank transfers and credit card payments, and yet it's smooth and seamless for the end user: essentially a credit card payment with a better user experience. There is no intrinsic reason why "convenience" should require digital cash.

Transaction costs. Is it sometimes claimed that digital currency will lower the transaction costs. Why? Bitcoin miners will increasingly be paid primarily by transaction costs rather than lock rewards, hence in that ecosystem transaction costs are, by design, only going to increase. Relatively high transaction costs don't seem to have stopped the credit card industry for the past several decades. And, even if raw transaction costs are lowered, there is no guarantee that this will translate in lower fees to end users. Maybe it will be the fintech innovators or the payment infrastructure providers who will pocket the difference.

Untraceability. Bitcoin claims to be anonymous. That is clearly not the case: at best pseudonymous, since you can follow the bitcoins through the blockchain. But, even then, that pseudonymity is only for those individuals who mine their own bitcoins in the privacy of their bedroom, which a few people used to do in the early 2010s. Nowadays, ordinary people can no longer afford to do that any more: given that the difficulty of mining keeps increasing (by design) as time goes by, bitcoin is only mined with dedicated hardware, in large farms federated into mining pools. Individuals who own any bitcoin (unless they got it through ransomware) generally buy it off someone else on a cryptocurrency exchange. And the exchange, in most jurisdictions, is regulated by Know Your Customer and Anti Money Laundering rules, so it requires a scan of your passport and it definitely associates your bitcoins with you in a totally non-anonymous way.
The anonymity claims from CDBCs are also dubious at best. "Rigorous standards of privacy and data protection", says the Bank of England's Consultation

[14] Which, as a challenger to traditional banks and credit card companies, has a strong commercial incentive to be more convenient to the end user than the payment methods offered by the incumbents.

Paper [2] about the digital pound: "the digital pound would be at least as private as current forms of digital money, such as bank accounts" (meaning not at all...) and "the identity of users would only be known to their Payment Interface Provider, and neither the Government nor the Bank would have access to digital pound users' personal data, except for law enforcement agencies under limited circumstances prescribed in law and on the same basis as currently with other digital payments and bank accounts more generally." This is a regulatory promise not to snoop, rather than an architectural guarantee that would make snooping technically impossible. These are two radically different concepts. Ultimately, full and unconditional anonymity is fundamentally incompatible with regulatory oversight and it is therefore never going to be provided by a CBDC.

Accessibility. Using digital cash will require a digital device: a computer, a dedicated banking token, a smartphone, a smartwatch, or at least some kind of smart card. It is unclear how much can be done securely on a smartcard without a user interface, hence it is unclear that this approach compares favourably, in accessibility terms, to plain physical cash for people who can't afford a computer or smartphone, or who find it too difficult to operate one. What about pocket money for children? A parent might want to use cash in order to give pocket money to a child too young to have a bank account. Would a holder of digital cash not need to have some form of digital cash account? If not, at least they would need to have a digital device storing a secret. Which is more plausible: a child having such a digital device, or a child having a bank account? In either case, from what age, and how would that compare with the age from which they could reasonably be entrusted with a few coins in a piggy bank? What if the child lost the digital device[15] or the credentials needed to operate it? Would the child then lose all their digital cash in one go? Similar questions could be asked at the other end of the age spectrum, for technologically illiterate (or even technophobic) elderly people.

Peer-to-peer transactions. Can't we already do that with bank transfers or PayPal and the like? Sure, the transaction is intermediated and is not anonymous[16], but we do already have other means of paying non-merchants digitally.

Financially risk-free. As an example of the claims for CBDC, the still hypothetical digital pound is claimed to be "financially risk-free in the sense that there is no credit, market or liquidity risk" [2]. The Bank of England white paper acknowledges operational risks "including those related to the security and resilience of CBDC infrastructure" but does not mention devaluation due to quantitative easing, which was one of the most significant consequences of[17] mainstream currencies abandoning the gold standard and one of the main drivers for the creation of bitcoin. The ability of a bank to print more CBDC reduces the trustworthiness of CBDC as a store of value. But then bitcoin itself, on the

[15] How likely is it that the child regularly took backups of the device? How frequently do adults back up their smartphone?

[16] But we already said what we think about claims of anonymity of digital cash, whether decentralised or CBDC.

[17] Or *reasons* for...

other hand, fails even more spectacularly on this "financially risk-free" criterion because of its extreme volatility, given that it is not anchored to any real-world value, as we noted in section 3.1.

Note in passing that saying "*financially* risk-free" elegantly glosses over the additional risks introduced by digital cash over physical cash through the unavoidable cybersecurity vulnerabilities.

A CYNIC'S VIEW None of the above claims is fully convincing. People rather more knowledgeable than me on monetary theory, such as Christopher Waller [19] from the US Federal Reserve, also express scepticism about there being a compelling need to introduce a CBDC.

To me, the most believable justification for introducing CBDC, though not one often offered by its proponents, is that governments and Central Banks don't want to be left out. If everyone started trading using bottle caps instead of dollars, the company making bottle caps would become influential, to the detriment of the Central Bank (the Federal Reserve in the specific case of US dollars). Thus, to a cynic, the most sincere reason for Central Banks wanting to introduce the digital dollar, or the digital euro, or the digital pound, is their wish to remain relevant, both in the face of competition from PayPal, Apple Pay and other commercial entities[18], and in the face of competition from the digital yuan, which is already a few steps ahead of its Western counterparts.

On the other hand, the most plausible justification for the introduction of most of bitcoin's successors[19] is that the creator of the coin is in a privileged position to create and stash away an initial pile of coins for herself—literally "making a mint" if the coin later takes off. And that's not even mentioning the all too numerous "initial coin offerings" that are no more than pump-and-dump schemes, where the business plan is not even to hold a stash of coins that will become valuable once the cryptocurrency becomes valuable but, rather more blatantly and efficiently, to collect the money of gullible suckers and then promptly disappear. We should be wary of *who would profit* from the introduction of any specific instance of digital currency, especially (but not only) unregulated ones.

3.4 Digital cash won't eliminate crime: it will simply displace it

Tax evasion is a major burden on honest citizens. In theory, if everyone paid their dues, taxes could be lower for everyone. Some honest people who are fed up with tax evaders might be willing to give up their financial privacy, and agree to the government monitoring their every transaction, in exchange for the elimination of tax evasion. At a higher level, a similar argument could be made for almost all crime: those honest people, and others, might be *even more* willing to give up their financial privacy if this meant that all illicit profits could be traced and

[18] Or, in China, AliPay and WeChat Pay—witness how Beijing dealt with *that* commercial competition [21].

[19] If not (and, after all, why not?) of bitcoin itself!

their recipients prosecuted. Those righteous citizens would happily trade their privacy in exchange for the elimination of crime.

But would they actually get the promised deal in this Faustian pact? I am very sceptical that the goal of eliminating crime could ever be achieved by moving to CBDC and universal observability of financial transactions. The only part of the deal that would happen for sure is the one whereby the law-abiding citizens would lose their privacy[20]. But criminals would not disappear: they would simply pivot towards different operating procedures. They would find ways of extracting their profits from the system through other means: in kind, in favours, through more layers of intermediaries or through other jurisdictions. Instead of basking in the comfortable but naïve feeling that CBDC would allow law enforcement to monitor and intercept all of the criminals' financial transactions, we should try to anticipate what else the crooks would be doing instead. Digital cash won't eliminate crime: it will merely displace it. We should figure out where to.

3.5 We don't know what we need

Some of the conceivable features of digital cash are necessary, some are desirable, some are very difficult to implement, particularly in combination. Among them:

- preventing double spending
- preserving anonymity of transactions
- making coins divisible
- allowing offline transactions
- allowing re-spending of a received coin without first having to return it to the issuer

I doubt it is possible to offer all of the above simultaneously without relying on axiomatically tamper-proof hardware[21].

Crypto geeks obsess about inventing clever ways of making the desirable features technically feasible and computationally efficient. The point is, some of the desirable properties of digital cash are inherently incompatible with each other, so we can't have them all, even if we manage to invent constructions that make each of them individually feasible.

The two main axes along which I see irreconcilable tensions are the one about anonymity of transactions and the one about control over the money supply. For each of these axes there are desirable features at either end, but they are mutually exclusive. The technical problems favoured by the crypto geeks (for

[20] Those of us who believe in privacy will strongly resist attempts to create a society in which every payment is traceable: total and absolute transparency, especially if asymmetric, makes social interactions awkward. In small doses, plausible deniability and merciful white lies are necessary social lubricants, without which we lose freedom and control.

[21] Which would probably not be a sound idea if the security of an entire currency system had to depend on that dubious axiom—bearing in mind the 1996 "cautionary note" of my colleagues Anderson and Kuhn [1], which hasn't lost its value today.

example, "how to implement fully anonymous digital cash", which lies at one extreme of the anonymity vs traceability axis), although objectively challenging, are *easy* in comparison to the real-world problems of choosing what will make a solid foundation for a fair digital society.

Will we be better off allowing traceability in order to prevent crime, or allowing strong anonymity and unlinkability in order to protect civil liberties? Anonymity of payments makes criminals hard to track down, as demonstrated by the various strains of ransomware that emerged in the 2010s (Cryptolocker, Wannacry, Petya, Notpetya etc) and contravenes the anti-money-laundering regulations that are nowadays commonplace in many jurisdictions[22]. On the other hand, making all financial transactions observable[23] violates the citizens' right to privacy[24] and allows an evil government to conduct mass surveillance and oppression of dissidents to an unprecedented extent[25].

Will we be better off allowing Central Banks to print currency (whether typographically or electronically) in order to respond promptly to exceptional crises such as COVID-19, or should we prevent currency manipulation in order to preserve the value of already-issued currency and avoid inflation? White [20], writing over a century ago, offers a wealth of compelling historical evidence for his statement that

> ... of all contrivances for defrauding the working people of a country, arbitrary issues of paper money are the most effective.

In each of these trade-offs, we can't have it both ways, and both extremes (libertarian bitcoin-style or centralised CBDC-style) have undesirable consequences. Is a halfway-house technically possible? Could we, for example, give citizens some white-lie leeway[26] for amounts up to a threshold[27] but enforce transparency above that, in order to prevent serious crime?

The cited Bank of England's consultation paper [2] claims that we need to engage in the design of a digital pound, essentially so as to develop local expertise and not to be left behind by the Chinese[28]. That's all very well, and it's better than doing nothing, but I would argue that we have not yet converged on a set of features that is desirable, fair to all members of society, and (as a secondary concern) also technically feasible.

[22] Although Sharman [17] claims that anti-money-laundering policies have high costs but few practical benefits.

[23] Something that physical cash disallows for reasons of scale, but that non-anonymous digital cash could make commonplace.

[24] With the complicity of the fallacious "nothing to hide" argument, to which peaceful and unconcerned citizens subscribe until it's too late.

[25] Particularly when coupled with the ability to redefine or reset the value of individual items of currency.

[26] See footnote 20.

[27] And what would be a good compromise for this threshold? The value of a house? Of a car? Of a bycicle? How much should be allowed to sneak under the radar?

[28] Though they don't quite say it in these words.

Although it is encouraging and desirable to see the Central Banks of the world's major currencies (USD [12], EUR [11], JPY [3], GBP [2]) running consultations, market research and pilot programs on CBDCs, I do not believe we are close to reaching a genuine consensus on the right balance to be struck in the above tussles, nor that we will before moving from pilot to deployment. It seems to me that we are rushing towards design and deployment of some form of digital cash without having completed a solid requirements analysis, without much awareness from ordinary citizens, and without having agreed collectively on the long-term irreversible implications of this significant societal change.

3.6 Deploying the wrong infrastructure could be disastrous

The People's Bank of China have already been running trials with tens of thousands of people in several cities in 2020, with amounts exceeding 100 M$. They have issued digital yuan that would expire after a certain date [4]. The scenarios from section 1 are not science fiction: they have happened, and they are just an appetiser for even more disruptive future developments.

But, if we deploy the wrong kind of technological infrastructure, it may be very difficult to get rid of it later, even if we then discover it was inappropriate. First, because of cost, inertia and technological lock-in. Second, and more sinister, because by the time we realise it can be used as an oppressive technology, it may already be used to oppress and suppress those who think so and try to change it. This is not science fiction either, as the *Financial Times* reported in 2021 [13]:

> [The e-yuan's] digital format enables the central bank to track all transactions at the individual level in real time. Beijing aims to use this feature to combat money laundering, corruption and the financing of "terrorism" at home by strengthening the already formidable surveillance powers of the ruling Communist party. [...]
> Beijing's ambitions for the digital renminbi derive from a deep-seated impulse towards social control, analysts say. [...]
> "The digital renminbi is likely to be a boon for CCP surveillance in the economy and for government interference in the lives of Chinese citizens," wrote Yaya Fanusie and Emily Jin in a report last month for the Centre for a New American Security, a Washington- based think-tank. [...]
> "If the Communist party will get insight into every trade we do through the digital renminbi, then I think a lot of people outside China will prefer not to use it," says one businessperson in Hong Kong, who declined to be named.

It may seem a great idea to make sure that the currency of the criminals vanishes, but it's the government of the day who decides who is a criminal. In Russia in 2023, saying that invading Ukraine was a bad idea makes you a criminal. As PGP creator Phil Zimmermann famously observed in 1996 in his poignant testimony to the US congress [22]:

> ... in a democracy, it is possible for bad people to occasionally get elected—sometimes very bad people. Normally, a well-functioning democracy has ways to remove these people from power. But the wrong technology infrastructure could allow such a future government to watch every move anyone makes to oppose it. It could very well be the last government we ever elect.
> When making public policy decisions about new technologies for the government, I think one should ask oneself which technologies would best strengthen the hand of a police state. Then, do not allow the government to deploy those technologies. This is simply a matter of good civic hygiene.

4 Conclusion

What should we do about digital cash? I definitely don't have all the answers. But I am convinced we should think harder about what we need, why, and for whose benefit, before putting effort into how to build it. "For whose benefit" means various things here:

- Are the digitally illiterate going to get a raw deal?
- Are criminals being given a free pass?
- Are the civil liberties of honest citizens being preserved?
- Would such technology allow a few individuals to profit at everyone else's expense?
- Would such technology allow a government to defraud the working people of a country? (White [20])
- Would such technology strengthen the hand of a police state? (Zimmermann [22])

As geeks with the ability to program computers, we have the incredible power that we can basically write the laws of physics of the digital society. And every year I remind my first year undergraduates of what a young Spiderman learnt from his uncle: "With great power comes great responsibility". We geeks have a duty to use our superpower to make digital cash work in a way that is fair for every member of society, especially the weaker ones who not only can't program computers but can't even *use* them.

We must write the laws of physics of the digital society so that the people who run, or would like to run, an oppressive government will find that the way digital cash works just *does not allow them* to do certain evil things. They must not be able to change those constraints by decree, in the same way that they will never be able to rewrite the law of gravity to make objects fall upwards instead of downwards.

In a sense, that's just the kind of thing that bitcoin idealistically set out to achieve. It was designed so that, no matter how powerful you were, you would not be able to print more currency arbitrarily and dilute the value of previously minted bitcoins. And thus bitcoin is a very important socio-technical

experiment in that sense. Now, bitcoin ended up being very different than how it had been originally conceived[29]. It never became currency. It never became a mainstream medium of exchange. It ended up being just a speculative asset. There are structural reasons for that, which we discussed in section 3.1, but there is also the fact that it ignited greed and FOMO[30]: bitcoin (and cryptocurrencies in general) became a speculative bubble that fed on itself, and the primary use of bitcoin has been this vacuously recursive "wanting bitcoin because it will go to the moon", rather than using it to buy anything concrete as in that famous 2010 pizza transaction. And then, as Dalio said, if bitcoin ever became too successful, it would be regulated out of existence, as it already has been in China and a few other countries.

But the spirit of geeks taking responsibility for writing the laws of physics of the digital society, which bitcoin (and PGP!) tried to do, is worth revisiting. Designing digital cash in a way that makes it not possible for a government to do evil things with it. The immutable laws of physics of the digital society must enforce fairness for everyone, unlike the human laws that a bad government could rewrite, arbitrarily redefining what is legal and turning a peaceful dissident into a criminal.

Of course this viewpoint of mine should be, in itself, rather controversial—as intended for a position paper at a workshop that thrives on debate. The definition of "what is fair" is not universally shared: what seems fair to me may not be what seems fair to you and everyone else. Some will argue that the only way to decide what is fair is through a political process, whereby elected representatives form a legislature that defines laws, and that it is *they* who should define how the digital society behaves, and that the geeks should not be entitled to special powers or extra votes just because they happen to be able to program.

So there we go: on one hand, public-spirited geeks righteously trying to build technology that cannot be used for evil, no matter who is in charge. On the other hand, non-geeks arguing that it's not up to the geeks to make the rules. I hope I have been sufficiently controversial. For my part, I continue to defend the position so eloquently expressed in that Zimmermann quote [22]:

> ... ask which technologies would best strengthen the hand of a police state; then, do not allow the government to deploy those technologies.

Let's do just that—whether by writing code or by engaging in public debate.

[29] Its consensus mechanism, designed for grass-roots operation whereby individuals would run their own nodes and anyone could devote spare cycles to mining bitcoin, has evolved into something unrecognisably different. The system, designed to avoid a central authority, is now much more centralised than originally intended: mining has become a specialist activity that only a handful of powerful "mining pools" have the resources to engage in. Individuals have no chance of competing against such pools and don't even try. Regular people don't run their own nodes and don't check the validity of the blockchain, delegating the management of their wallets to intermediaries (the exchanges) who host them on their behalf. The customers of these intermediaries rarely (if ever) bother to check the consistency of a block.

[30] Fear Of Missing Out.

Acknowledgements

I am grateful to the workshop attendees who engaged in the discussion during my presentation and whose comments appear in the transcript that follows this paper in the post-proceedings volume, as well as to Virgil Gligor, Harry Halpin, Adrian Perrig and Andrei Serjantov for further offline comments and references that allowed me to improve the paper. Nonetheless, all the opinions herein expressed, as well as any mistakes or omissions, remain my sole responsibility.

References

1. Ross Anderson and Markus Kuhn. "Tamper Resistance—A Cautionary Note". In "Proc. 2^{nd} USENIX Workshop on Electronic Commerce", 1996. ISBN 1-880446-83-9. URL `http://www.cl.cam.ac.uk/~mgk25/tamper.pdf`.
2. Bank of England and HM Treasury. "The digital pound: a new form of money for households and businesses? (Consultation Paper)", February 2023. URL `https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf`.
3. Bank of Japan. "The Bank of Japan's Approach to Central Bank Digital Currency", October 2020. URL `https://www.boj.or.jp/en/about/release_2020/data/rel201009e1.pdf`.
4. Biagio Bossone and Ahmed Faraghallah. "Expiring money (Part I)", November 2022. URL `https://blogs.worldbank.org/allaboutfinance/expiring-money-part-i`.
5. Stefan Brands. "An Efficient Off-line Electronic Cash System Based On The Representation Problem". Technical Report CS-R9323, Centrum voor Wiskunde en Informatica (CWI), 1993. URL `https://ir.cwi.nl/pub/5303/05303D.pdf`.
6. Harry Browne. *How you can profit from the coming devaluation.* Arlington House, 1970.
7. Vitalik Buterin. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform", 2014. URL `https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf`.
8. David Chaum. "Blind Signatures for Untraceable Payments". In David Chaum, Ronald L. Rivest and Alan T. Sherman (Editors), "Advances in Cryptology", pages 199–203. Springer US, Boston, MA, 1983. ISBN 978-1-4757-0602-4. `https://doi.org/10.1007/978-1-4757-0602-4_18`.
9. David Chaum and Stefan Brands. ""Minting" Electronic Cash". *IEEE Spectr.*, **34**(2):30–34, feb 1997. ISSN 0018-9235. `https://doi.org/10.1109/6.570825`.
10. David Chaum, Amos Fiat and Moni Naor. "Untraceable Electronic Cash". In Shafi Goldwasser (Editor), "Advances in Cryptology—CRYPTO '88", volume 403 of *LNCS*, pages 319–327. Springer-Verlag, 1990, 21–25 August 1988. ISBN 978-0-387-34799-8. `https://doi.org/10.1007/0-387-34799-2_25`.
11. European Central Bank. "Annex 1: Functional and non-functional requirements linked to the market research for a potential digital euro implementation", January 2023. URL `https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs230113_Annex_1_Digital_euro_market_research.en.pdf`.

12. Federal Reserve. "Money and Payments: The U.S. Dollar in the Age of Digital Transformation", January 2022. URL https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf.
13. James Kynge and Sun Yu. "Virtual control: the agenda behind China's new digital currency". *Financial Times*, February 2021. URL https://www.ft.com/content/7511809e-827e-4526-81ad-ae83f405f623.
14. Taylor Locke. "Ray Dalio: The government 'outlawing bitcoin is a good probability"', March 2021. URL https://www.cnbc.com/2021/03/26/bridgewaters-ray-dalio-good-probability-government-outlaws-bitcoin.html.
15. Tanaya Macheel. "Berkshire Annual Meetings: Warren Buffett gives his most expansive explanation for why he doesn't believe in bitcoin", April 2022. URL https://www.cnbc.com/2022/04/30/warren-buffett-gives-his-most-expansive-explanation-for-why-he-doesnt-believe-in-bitcoin.html.
16. Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system", October 2008. URL https://web.archive.org/web/20140320135003/https://bitcoin.org/bitcoin.pdf.
17. Jason Sharman. *The Money Laundry: Regulating Criminal Finance in the Global Economy*. Cornell University Press, 2011. ISBN 978-0801450181.
18. Nick Szabo. "Formalizing and Securing Relationships on Public Networks". *First Monday*, **2**(9), Sep. 1997. https://doi.org/10.5210/fm.v2i9.548.
19. Christopher J Waller. "CBDC: A Solution in Search of a Problem?", August 2021. URL https://www.bis.org/review/r210806a.pdf.
20. Andrew Dickson White. *Fiat money inflation in France: how it came, what it brought, and how it ended*. 1912. ISBN 978-1484834268. Reprinted 2013 in Burk Classics.
21. Raymond Zhong. "China's Halt of Ant's IPO Is a Warning". *The New York Times*, November 2020. URL https://www.nytimes.com/2020/11/06/technology/china-ant-group-ipo.html.
22. Philip R. Zimmermann. "Testimony of Philip R. Zimmermann to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation", 26 June 1996. URL https://philzimmermann.com/EN/testimony/index.html.