Open problems about the forthcoming financial infrastructure of the digital society

Frank Stajano[0000-0001-9186-6798]

University of Cambridge
frank.stajano@cl.cam.ac.uk

Abstract. The migration towards digital currency appears inevitable. Technical designs for digital cash have been put forward since the 1980s. For every technical problem, from prevention of double spending to divisibility of coins to privacy protection, creative cryptographers have offered some technical solution. But no design solved all problems simultaneously, because some of the requirements are inherently contradictory.
Society is at a crossroads. A new version of the financial infrastructure of the digital society is being built under our feet, from cryptocurrencies and CBDCs to DeFi, but without a clear architectural design and without any explicit agreement about the necessary trade-offs. We must be creative in envisaging new solutions but also vigilant in anticipating the long-term consequences, for all parties, of any proposed approach: it will be hard to displace any technology that is widely deployed.
In this position paper we offer a bird's eye overview of important unresolved problems for digital currencies and decentralised finance, highlighting the societal, financial and political problems where a trade-off between conflicting requirements must be struck.
We believe it is imperative that we carry out this analysis ahead of deployment and that we make explicit choices about the properties that the financial infrastructure of the digital society must guarantee. Failure to do so risks locking us into an architecture that will unfairly benefit a few early movers with vested interests, to everyone else's detriment.

1 Introduction

Perhaps the best way for me to honour my brilliant PhD supervisor Ross Anderson is to attempt to follow his lead and venture beyond the narrow technical boundaries of security, so as to address a forthcoming societal problem that requires a long-term vision and an interdisciplinary approach. In this position paper I won't offer any solutions. We need to start with the questions.

The days of cash are numbered. It seems inevitable that cash will eventually become digital. We are not talking merely of payment methods becoming digital (tap watch to pay for coffee) but actually of currency itself becoming digital and, crucially, programmable, with banknotes and coins eventually disappearing, despite assurances to the contrary to avoid a public backlash.

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.

The core technical problem of using a string of bits as cash[1] has been extensively studied by cryptographers since the early 1980s, starting with Chaum's pioneering inventions [8,6,7]; but only with the emergence of Bitcoin [15] has digital cash reached public awareness. Although today's highly volatile cryptocurrencies are unsuitable as either a medium of exchange or a store of value, they have still become a three-trillion-dollar asset class. Meanwhile, the world's major economies have been planning for Central Bank Digital Currencies (CBDCs)—despite considerable scepticism from both within [21,10] and outside [13,18].

Triggered by the Bitcoin revolution [3,16], various innovations have flourished around "blockchain" (a distributed tamper-proof ledger that no single party could manipulate), made programmable by the Smart Contracts originally proposed by Szabo [19] and then first implemented by Ethereum [5]. Under the paradigm of Decentralised Finance (DeFi) [22], financial actors may interact with each other through programmed contracts that are automatically enforced and executed without having to trust an intermediary such as a bank or a broker.

On this technology, platforms have emerged that enable peer-to-peer lending, trading, currency exchange, arbitrage, speculation, options, futures and so forth, importing the ideas and mechanisms of traditional finance into a disintermediated (and, so far, largely unregulated) parallel universe [17].

Many more original ideas are being explored in this financial Wild West, which still moves more quickly than the regulators.

2 The problem

The shift to digital currency and DeFi will cause radical transformations in the digital society. We are living this process moment by moment and we have difficulty seeing the big picture of what is happening; but it is imperative that we do. We might list various desirable properties for digital currency (unforgeability, privacy, divisibility, offline operation, trustworthiness, usability, robustness, recoverability, traceability and so forth)—and indeed clever techies have invented cryptographic methods to implement each of them—but it is impossible to build a version of digital currency with all of these good properties simultaneously, because some of them are inherently in conflict with each other.[2]

We need a long-term, big-picture vision. I believe we must first understand where we are, understand what the technology plausibly allows us to do, understand the constraints of the design space and understand the benefits and pitfalls of a hypothetical global deployment of each of the plausible variants and innovations. Then, systematise these future scenarios to inform the general public and the key decision makers before committing to any particular implementation that will exclude the alternatives and will be hard to change, once entrenched, because of backwards compatibility shackles.

[1] A seeming impossibility: bits are inherently copiable, which opens the door to multiple spending [7].

[2] Cfr. questions 2, 3 and 4 in the next section.

3 Open questions

Research questions that need exploring include the following. Although some of them may have already attracted substantial attention, we are still far from a holistic perspective.

1. What desirable properties should digital currencies and DeFi possess, for the greater good of the citizens of the digital society?
2. Where is the correct trade-off between ensuring that digital money retains its purchasing power[3] versus allowing governments and central banks to respond promptly with cash injections to potentially catastrophic emergencies such as COVID-19, the invasion of Ukraine or the inevitable recessions caused by economic cycles? On the macroeconomic front, central banks will obviously want to retain control of the levers that allow them to steer their country's economy, including the ability to print more money. Are cryptocurrencies so destabilizing to traditional monetary policies that they will be banned, as argued by Dalio [14]?
3. Where is the correct trade-off between the privacy afforded by cryptocurrency transactions [1] and the traceability required to prevent large-scale criminal abuse such as ransomware and tax evasion? While it is clearly undesirable to allow the bad guys to operate undetected, it would be just as bad to deploy a financial infrastructure that allowed pervasive surveillance by the State: evil governments would readily use such powers to crush their opposition. This trade-off has been discussed extensively but perhaps a new taxonomy might help, and it would be interesting to study how much anonymity and unlinkability the regulators of a non-evil government would still tolerate.
4. What other pairs of desirable properties of digital currencies and DeFi result in irreconcilable tensions where we can't have both and a trade-off must be sought? It would be a useful contribution to identify as many of these constraints as possible.
5. At the "meta" level, for such tussles that involve the fabric of the digital economy and thus affect all its citizens, what decision method would ensure the fairest outcome? One-head, one-vote? Centralised decision by elected representatives? Decentralised democratic decision making? Across national boundaries (cfr. question 6)? One-country, one-vote? GDP-weighted? Strong vested interests as to what "fairness" even means... Quite political!
6. Digital currencies and DeFi, as a common good, must be trans-national. Clearly each central bank will want to impose its own constraints and retain control of the money supply, yet international interoperability remains key. Is it possible to build a technological foundation that, like the Internet, works interoperably despite the local pieces being built and managed by mutually mistrustful principals? On a related note, is it possible to build a

[3] As Bitcoin originally set out to do in the wake of the 2008 financial crisis and subsequent quantitative easing.

trans-national technological foundation (the "laws of physics" of the digital universe) that a rogue evil government would not be able to subvert just by defining new national laws?

7. How to guarantee the redeemability of our digital assets against actual buying power when the digital trading platform is not under our own jurisdiction?
8. Though fintech startups have shorter time horizons, from a perspective that spans centuries (such as Dalio's [12]) we must envisage major disruptions such as the demise of the US dollar as the world's reserve currency—or even World War 3. The first two World Wars caused major resets of the world's monetary systems.[4] How should such big-picture awareness inform the design of the world's digital money infrastructure from a macroeconomic viewpoint? Will anything, besides gold, remain a reliable store of value and retain international trust? Will CBDCs only ever be fiat money?[5] What will make the CBDC of another country trustworthy? Technologically and economically, these are ultimately architectural questions about the limits of what is feasible. But the political power issues around control of the world's reserve currency are even more significant; in imagining the future we cannot pretend to ignore that such dramatic power shifts will be accompanied by large-scale military conflicts.
9. Boiling things down to the essentials, what are the substantial points of agreement and disagreement between the properties of the CBDCs (e-dollar, e-yuan, e-euro and so forth) that have been put forward in the white papers of the world's major central banks? Which of the disagreements would make these currencies incompatible, to what extent and with what consequences? Which of the incompatible alternatives is most "fair" to the various classes of citizens of the digital society? What can we learn from the small-scale trials that have already been carried out, for example in China with expiring digital yuan [4]?
10. Similarly, what are the key common points and key distinguishers of the major decentralised cryptocurrencies? Can we articulate their original visions and how they compare to what those cryptocurrencies have morphed into today?[6] Are there any invariants? What can we learn from *these* experiments? What happened that had not been expected at design time?

[4] Cfr. hyperinflation and ultimately the demise of German Mark after WW1; and Bretton Woods after WW2.

[5] Note how being tethered to the US dollar, or even to a basket of fiat currencies, as some stablecoins [9] do, is still rather different from being redeemable for gold. And what would "redeemable for gold" even mean in a decentralised transnational context? Which principal would be making the underlying promise to pay out in gold, and why should anyone trust them to uphold it? Recall how Russia never returned the 90+ tonnes of gold that Romania sent there for safeguarding in 1916.

[6] Bitcoin, for one, is now radically different in many important dimensions from what its 2008 white paper envisaged—it is only used for speculation rather than as a medium of exchange and mining is now concentrated in the hands of a few large consortia rather than distributed among all participants, to cite but two.

11. What are the incentives and interests of the incumbent players that DeFi and digital cash might displace, such as retail banks, credit card companies, stock brokers and so forth? How might such incentives influence and possibly distort the transition? What new roles could these actors take on, if any, that might leverage and exploit their existing infrastructure?
12. How to prevent digital exclusion? How will the elderly and the digitally illiterate deal with digital currency? (We see the teething problems already with digital payments, even if still based on traditional currency.) How to cater for those who, mistrusting computers, will never agree to give up physical cash? How to make the new digital systems reliable and recoverable in the face of both accidental errors and fraud? How to ensure that ordinary people won't lose their life savings just because a digital wallet or a crypto key or some other geeky gobbledygook was not backed up [20]?
13. DeFi substantially increased the attack surface for both technical attacks [23] and (given its novelty, opacity and lack of regulation) for traditional frauds at scale. While Mt. Gox's 2014 collapse started with hacking incidents (but then also involved accounting fraud from CEO Mark Karpelès), the FTX collapse of 2022, in which CEO Sam Bankman-Fried was convicted of fraud, conspiracy and money laundering in excess of 10 billion USD, was substantially a "traditional fraud" as opposed to a technical attack on the cryptocurrency protocols. Unregulated business practices have been exploited (cfr. the 2023 Peraire-Bueno brothers' MEV attack [11] on Ethereum). Could any architectural safeguards, such as formal verification, prevent such attacks, or will attacker ingenuity always find something new [2]?

4 Conclusions

I strongly believe it would be unwise to leave it to a few enterprising technical innovators (or incumbent trillion-dollar internet giants), each with their own vested interests, to define the specific subset of properties of the financial infrastructure of our future digital society, and for everyone else to have to accept them as a *fait accompli*. We have a duty to foresee where the various alternatives could lead us and anticipate the potential upsides and downsides rather than being surprised and upset by them after the fact, once it is too late to move away from the already-deployed technology.

We are at the stage where a new universe is being created and its laws of physics are being written. This new universe, the financial infrastructure of the digital society, will become a digital commons of fundamental importance and we must carefully ensure we end up with desirable properties for it. Desirable and fair, that is, for *all* the citizens who will have to live in it, including the digitally illiterate and those struggling in the bottom portion of the wealth curve.

References

1. Ghada Almashaqbeh and Ravital Solomon. "SoK: Privacy-Preserving Computing in the Blockchain Era". 2021. URL https://eprint.iacr.org/2021/727.
2. Ross Anderson and Nicholas Boucher. "If It's Provably Secure, It Probably Isn't: Why Learning from Proof Failure Is Hard". In *Proc. Security Protocols Workshop*, pages 199–204. Springer-Verlag, 2023. ISBN 978-3-031-43032-9. https://doi.org/10.1007/978-3-031-43033-6_19. URL https://arxiv.org/pdf/2305.04755.
3. Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll and Edward W. Felten. "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies". In *IEEE Symposium on Security and Privacy*. 2015. URL https://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf.
4. Biagio Bossone and Ahmed Faraghallah. "Expiring money (Part I)", November 2022. URL https://blogs.worldbank.org/allaboutfinance/expiring-money-part-i.
5. Vitalik Buterin. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform", 2014. URL https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf.
6. 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. URL http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF.
7. 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. URL https://chaum.com/wp-content/uploads/2021/12/Untraceable_Electronic_Cash.pdf.
8. David L. Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms". *Commun. ACM*, **24**(2):84–88, February 1981. ISSN 0001-0782. https://doi.org/http://doi.acm.org/10.1145/358549.358563. URL https://dl.acm.org/doi/pdf/10.1145/358549.358563.
9. Jeremy Clark, Didem Demirag and Seyedehmahsa Moosavi. "Demystifying stablecoins". *Communications of the ACM*, **63**(7), July 2020. URL https://dl.acm.org/doi/pdf/10.1145/3386275.
10. Economic Affairs Committee. "Central bank digital currencies: a solution in search of a problem?" HL Paper 131, House of Lords, January 2022. URL https://publications.parliament.uk/pa/ld5802/ldselect/ldeconaf/131/131.pdf.
11. Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach and Ari Juels. "Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability". In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 910–927. 2020. https://doi.org/10.1109/SP40000.2020.00040. URL https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9152675.
12. Ray Dalio. *Principles for Dealing with THE CHANGING WORLD ORDER — Why Nations Succeed and Fail*. Simon & Schuster, 2021. ISBN 978-1-4711-9669-0. URL https://www.economicprinciples.org.
13. David T. Llewellyn. "Is Retail Central Bank Digital Currency A Solution Searching For A Problem?", 2024.

14. Taylor Locke. "Ray Dalio: The government 'outlawing bitcoin is a good probability"', 2021. URL https://www.cnbc.com/2021/03/26/bridgewaters-ray-dalio-good-probability-government-outlaws-bitcoin.html.
15. Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system", October 2008. URL https://web.archive.org/web/20140320135003/https://bitcoin.org/bitcoin.pdf.
16. Arvind Narayanan, Joseph Bonneau, Edward W. Felten, Andrew Miller and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies*. Princeton University Press, 2016. URL https://bitcoinbook.cs.princeton.edu/.
17. Abrar Rahman, Victor Shi, Matthew Ding and Elliot Choi. "Systematization of Knowledge: Synthetic Assets, Derivatives, and On-Chain Portfolio Management". *arXiv preprint arXiv:2209.09958*, 2022. URL https://arxiv.org/pdf/2209.09958.
18. Frank Stajano. "Sleepwalking into disaster? Requirements engineering for digital cash (Position paper)". In *Proceedings of 28th Security Protocols Workshop (SPW 2023)*, page 3–19. Springer-Verlag, Berlin, Heidelberg, 2023. ISBN 978-3-031-43032-9. https://doi.org/10.1007/978-3-031-43033-6_1. URL https://www.cl.cam.ac.uk/~fms27/papers/2023-stajano-currencies.pdf.
19. Nick Szabo. "Formalizing and Securing Relationships on Public Networks". *First Monday*, **2**(9), Sep. 1997. https://doi.org/10.5210/fm.v2i9.548. URL https://firstmonday.org/ojs/index.php/fm/article/view/548.
20. Huw Thomas. "Man told he can't recover £598m of Bitcoin from tip". BBC News Online, January 2025. URL https://www.bbc.co.uk/news/articles/cj0r0dvgpy0o.
21. Christopher J Waller. "CBDC: A Solution in Search of a Problem?", August 2021. URL https://www.bis.org/review/r210806a.pdf.
22. Sam Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz and William Knottenbelt. "SoK: Decentralized Finance (DeFi)". In *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, pages 30–46. 2022. URL https://dl.acm.org/doi/pdf/10.1145/3558535.3559780.
23. Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song and Arthur Gervais. "SoK: Decentralized finance (DeFi) attacks". In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 2444–2461. IEEE, 2023. URL https://csdl-downloads.ieeecomputer.org/proceedings/sp/2023/9336/00/933600c444.pdf.