Redesigning digital money:
What can we learn from a decade of cryptocurrencies?

Robleh Ali and Neha Narula
Digital Currency Initiative, MIT Media Lab

Introduction

In a 2019 speech, Bank of England governor Mark Carney said that “Technology has the potential to disrupt the network externalities that prevent the incumbent global reserve currency from being displaced.” Certainly one of the most interesting places where technology is disrupting payments and finance is in cryptocurrencies. Cryptocurrencies have emerged from open source development communities in large part because electronic transaction systems are too expensive and they have not evolved fast enough to keep pace with the demand for retail online digital payments and more sophisticated types of financial transactions. The wide variety of experimentation in cryptocurrencies is causing technologists and central bankers to rethink the interface to money and explore a digital form which can be held by users and companies directly. This could lead to a financial system with a simplified institutional structure, capable of serving the public at a much lower cost. Though there has been much discussion about the policy design for central bank-issued digital currency (CBDC), there are important technical points missing from the conversation: CBDC should not be a direct copy of existing cryptocurrencies with exactly the same design and features but there are things we can learn from their emergence - the usefulness of programmability in money and the importance of preserving user privacy.

Cryptocurrency technology, in some instances, can provide an important feature: Anyone can participate and build applications with financial transactions to a standard, which creates a free-entry market that enables competition. These rules are set and maintained by users of the system, not by a coalition of companies or other large market participants.[1] This is due in large part to the fact that many participate in observing, auditing, and validating the creation of money and the legitimacy of payments by observing a highly replicated audit trail of activities.

The cryptocurrency ecosystem should be viewed as a laboratory where developers are inventing different technologies, monetary policies, governance strategies, and reward systems which are competing. The space is still in its infancy, but make no mistake -- successful ideas from this area will eventually find their way into the more conservative world of fiat digital payments. Libra and other stablecoins are the latest prominent example of these ideas breaking through. There will be more.

[1] Harper, Colin. “Bitcoin Independence Day: How This Watershed Day Defines Community Consensus.” *Bitcoin Magazine*, August 1, 2019. https://bitcoinmagazine.com/articles/bitcoin-independence-day-how-this-watershed-day-defines-community-consensus

Thus it makes sense to review some of the technologies that have been developing in cryptocurrencies over the past ten years and to consider how they might address concerns around centralization,[2] competition, risk, surveillance, and privacy when designing a digital fiat currency (DFC), stablecoin, or a central bank digital currency (CBDC). To address these concerns we will give a brief explanation of pieces of technology which either first emerged with cryptocurrencies or were popularized and developed further through cryptocurrencies, and how they relate to the problems at hand. These technologies are:

- **Consensus protocols as used in decentralized blockchains**. We'll show how these protocols can empower users and enable competition through free entry, but might not be worth the cost in software complexity for government-backed currencies if one can achieve free entry in other ways.

- **Atomic cross chain transactions as an example of programmable money**. As an example of a specific use case of programmable money, we will discuss how atomic cross chain transactions reduce counterparty risk and thus can potentially lower transaction costs and improve financial stability.

- **Cryptographic techniques for preserving privacy in blockchain-based systems**. We'll show how these techniques might also be used to achieve regulatory enforcement without revealing the detailed contents of financial transactions. Beyond financial services, preserving privacy has become increasingly important as we see how far it has been eroded in recent years.

Whether the impetus comes from government or legislature, one central bank issuing CBDC or the private sector, central banks need to be prepared. Advocates of various software platforms and the cryptocurrencies that come attached are making claims that can only be assessed by understanding what the technology can do, and what it cannot. The broader purpose of analyzing these three technologies is to show how cryptocurrency can be broken down into its constituent parts to see which pieces fit the policy goals of central banks and regulators. Some will and others won't, and central banks should accept the pieces that advance their policy goals and reject those that don't. Central banks do not have to accept prepackaged solutions, they can tailor the technology to their needs.

A common mistake is to assume new technology always improves things; this is often not true. Introducing new technology into a complex system usually has effects that cannot be predicted, some positive and some negative. And whether things have improved depends on your perspective. Gains and losses are rarely uniformly distributed; the voices of winners are celebrated and amplified while those who have lost are derided, marginalized or ignored.

[2] Decentralised financial technologies Report on financial stability, regulatory and governance implications, FSB (2019) https://www.fsb.org/wp-content/uploads/P060619.pdf

Consensus protocols and decentralization

Consensus, quite simply, is the idea of how to reach agreement among a set of participants in the presence of failures. It's a fairly old problem in computer science, first published by Pease, Shostak, and Lamport in 1980.[3] Since then there have been dozens of proposed consensus protocols with different properties and guarantees. Given an abstract model in which one makes assumptions about the network and adversary, one can design efficient protocols which tolerate certain types of failure, though might require a minimum amount of communication.

Practical algorithms and systems have emerged -- companies like Google, Facebook and Microsoft use consensus protocols inside their datacenters to keep computers consistent. [4][5][6] Until Bitcoin, consensus protocols were only employed within a single organization. Now, developers are reaching back to protocols invented in 1999 to create ledgers run by multiple organizations. All pre-Bitcoin protocols are fundamentally based on *voting*, and thus require enumerating all the participants, or voters. We refer to these protocols as *permissioned consensus* protocols. Bitcoin was the first consensus system that did not require knowing *a priori* who would be participating in maintaining the ledger, and in fact was open to new participants as long as they were willing to demonstrate some cryptographic activity. This is what is known as Bitcoin "mining" or proof-of-work: computers race to find a random number that will will produce a cryptographic hash of a block of transactions with enough leading zeros; the first to do so receives the transactions fees and newly minted bitcoin from the block. Everyone participating in the system agrees that the valid blockchain with the most evidence of this work is the correct history of Bitcoin transactions. This was a novel method of gatekeeping in consensus, and is now known as *Nakamoto consensus*.

Unfortunately, this led to a market for faster and faster computers to find these random numbers effectively, and since the software increases the difficulty of the puzzle with more mining power, we have ended up with a system where thousands of computers around the world are using vast amounts of energy simply to complete this task. This has led to research in new consensus protocols that do not require the same energy usage.[7]

These new large scale consensus algorithms provide similar guarantees to the previous era of consensus algorithms, in that they are designed to operate around assumptions about the honesty of the participants and the types of malicious behavior they might exhibit. They also still require enumerating the set of participants in order to count votes. The difference from the past

[3] Pease, Marshall, Robert Shostak, and Leslie Lamport. "Reaching agreement in the presence of faults." *Journal of the ACM (JACM)* 27.2 (1980): 228-234.

[4] Chandra, Tushar D., Robert Griesemer, and Joshua Redstone. "Paxos made live: an engineering perspective." *Proceedings of the twenty-sixth annual ACM symposium on Principles of distributed computing*. ACM, 2007.

[5] https://cloud.netapp.com/blog/azure-storage-behind-the-scenes

[6] https://engineering.fb.com/data-infrastructure/location-aware-distribution-configuring-servers-at-scale/

[7] Note that this area is under active development; any summary given now will soon be out of date.

is that the new protocols are designed to work with a much larger set of participants than previous protocols -- thousands or millions instead of dozens -- and, inspired by recent blockchain protocols, they include validation and cope with an in-flux, frequently changing set of voters.

Another new line of work is *federated consensus*, which relaxes the requirement to know all of the participants in the system. In federated consensus systems, one does not need to register with everyone in order to participate; participants may have different trust domains and may accumulate votes differently. Note that this is not true in permissioned consensus.

Confusingly, sometimes voting power is proven by demonstrating ownership of a coin. We distinguish permissioned protocols where participation is determined by coin ownership from proof-of-stake protocols by the honesty assumptions of the participants; permissioned consensus and federated consensus protocols assume participants are either honest or malicious, whereas proof of stake protocols assume participants are honest, malicious, or rational (in the hope of coping with scenarios with few altruistic participants) and incorporate a punishment mechanism, requiring users to "stake" their coins. These bonded coins are then taken, or *slashed*, within the blockchain protocol if anyone can submit computer-readable evidence of misbehavior on the part of the bonder, such as voting for two different blockchains at the same time. Oftentimes these protocols have a permissioned consensus protocol at their core (for example, Tendermint and Cosmos). Table 1 summarizes all the protocols.

What might this have to do with CBDC? One connection is that many developers are implementing so-called "stablecoins" on top of permissionless architectures like Bitcoin and Ethereum, and these stablecoins might eventually compete with CBDC. It's worth stepping back to examine why these types of consensus protocols are interesting, and also to note where they encounter challenges. Note that we are not addressing risks introduced by the way the assets backing the stablecoin are managed.[8]

[8] Wall, Eric. "Privacy and Cryptocurrency, Part IV: Stablecoins— Blacklists and Traceability." Accessed January 15, 2020. https://medium.com/human-rights-foundation-hrf/privacy-and-cryptocurrency-part-iv-stablecoins-for-human-rights-blacklists-and-traceability-6d74ee17c25d

Category	**Description**	**Examples**	**Admission Control**
Permissioned consensus	Selected set of *n* participants (*n* might be very large) run an agreement protocol	PBFT, TendermintBFT, Hotstuff, Algorand	Obtain voting power[9]
Nakamoto consensus	Proof-of-work and longest chain	Bitcoin, Ethereum, Litecoin	Obtain hashrate
Federated consensus	Nodes choose which other nodes to trust by forming *quorums* with which they run an agreement protocol	Stellar, Ripple	Obtain voting power
Proof of Stake	Participants determined by who stakes coins; includes punishment for bad behavior	Ethereum 2.0, Tezos, Cosmos	Obtain coins in the blockchain and lock them

Table 1. Categorization of consensus protocols with a short description of what it takes to participate in the “write” part of the protocol. There are protocols that support multiple different admission mechanisms (for example, proof-of-work and voting) which are not covered here. In permissioned systems where *n* is very large, some protocols first elect a log(*n*)-sized committee to run the agreement.

Two important features underlie these systems: First, they are designed so that many people can join and participate. This results in promoting competition and preventing capture. Second, participants can validate and verify the system’s operation, and thus, users can detect and threaten to leave a system that is not operating to their standards by forking the protocol. This reduces dependence on any actor or small number of actors, and enables the system to keep running even if many of the existing maintainers disappear. Combined, this is what is often referred to as “decentralization”.

In practice, this does not always happen as intended. The newer protocols have not been around long enough to form a judgement, but let’s take a look at proof of work. Mining power in Bitcoin has concentrated among a few mining pools; mining and energy contracts have economies of scale that act as an underlying force pushing miners to grow larger to capture

[9] Obtaining voting power is done by by convincing all current participants to admit you to the system and recognize you as a participant, with a vote. Some protocols use proof of ownership of a coin.

more profit, or for individual miners to join pools to reduce variance in returns. Initial research indicates that coin ownership, or stake, might have similar concentration issues.[10]

However, what might appear concentrated in one light could be revealed to be effective in another if free entry is preserved. Though more than 50% of the Bitcoin hashrate is controlled by just four mining pools,[11] they do not have as much control over the protocol as it might seem. Miners receive rewards in Bitcoin; if they were to misbehave or fork the protocol in a way that upset users, users could sell their coins and render the miners' equipment worthless. Users depend on the miners and developers for security and reasonable operation of the system. Developers rely on miners and users to voluntarily upgrade and run the code that they write. There is an interesting balance of power between miners, developers, and users in proof-of-work based systems. Something like this probably applies to proof-of-stake systems as well.

Decentralization has different dimensions; in addition to technical, there are legal, social, and economic aspects. While a consensus protocol can help decentralize a system, the last decade of innovation in cryptocurrency shows that technology alone cannot guarantee decentralization or even a different economic structure.

Wealth in cryptocurrencies is often more concentrated than in other assets.[12] There are many claims of revolutionary new systems in which power is practically far more concentrated than the existing financial system with a consensus protocol thrown in to add a veneer of technical decentralization. For example, investors in the spate of Initial Coin Offerings (ICOs) in 2017 and 2018 hoped that token holders would be rewarded if the ICO platform was able to eventually achieve massive scale. Token issuers touted the decentralization of their system to regulators, but promised their ability to capture rent and make a profit to investors.[13] Policymakers need to be extremely cautious about these incentives and understand the economic interests which lie behind each platform, Bitcoin included.

Given the complexity of decentralized consensus protocols in both their technical implementation and their governance, an open question is whether a decentralized protocol is *required* to achieve free entry in practice, or if such a thing could effectively be achieved by a diverse coalition of organizations or even by a non-profit or government entity with a legal contract to govern the system and provide open access. History has shown that these coalitions can be co-opted by incumbents; this could happen with permissioned blockchains with tens or

[10] Fanti, Giulia, Leonid Kogan, Sewoong Oh, Kathleen Ruan, Pramod Viswanath, and Gerui Wang. "Compounding of wealth in proof-of-stake cryptocurrencies." In *International Conference on Financial Cryptography and Data Security*, pp. 42-61. Springer, Cham, 2019.

[11] BTC.com Pool Distribution. https://btc.com/stats/pool. Accessed January 15, 2020.

[12] Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network, Kondor et al (2014) https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0086197

[13] https://www.sec.gov/litigation/complaints/2019/comp-pr2019-87.pdf

even hundreds of participants. Is there a number or composition of participants that could make this too difficult to happen?

Nor should we discount, or lightly cast aside, the democratic accountability which exists in the current monetary system. While not perfect, independent central banks are answerable to their legislatures and this is a real check on power. These democratic credentials stack up well against arbitrary foundations, startups, and large technology companies over which the public has no control. Monetary policy should never be determined by a self-appointed group of private corporations.

Given this, one must ask whether or not it makes sense to implement CBDC using blockchain technology. The phrase "blockchain technology" covers a multitude of platforms with varying levels of complexity. Central banks have already been prototyping and experimenting to become more familiar with this technology. For example, the Bank of Canada and the Monetary Authority of Singapore used a combination of Corda and Quorum to settle cross-border payments.[14] Another type of fiat implementation has come through the development of stablecoins, where the digitized token represents either a claim on a unit of fiat currency held in a bank account (Tether, TrueUSD, USD-C, Paxos) or a cryptocurrency-backed, algorithmically pegged token (Dai).

These platforms are useful for experimentation and prototyping because of their flexibility and features, and because of the enthusiasm of the companies promoting the technology. However, what is helpful for prototyping might not be good for practice; these complex platforms make trade-offs when it comes to security, stability, and scale. In practice, we've seen that technical complexity breeds a larger attack surface. Tools from distributed systems and cryptography can be used to increase public verifiability, but current blockchain technology and the incentives within existing public blockchain systems do not seem like a good replacement for our current systems for democratic accountability in money.

This has been a grand experiment in a new way to structure secure distributed systems. Technology, when properly used, can make systems more secure by making tampering with the ledger easy to detect, even if a fully decentralized consensus protocol is not required. We should also learn from the open access and programmable nature of cryptocurrencies. This is an example of how cryptocurrencies can be seen of a set of constituent parts, some of which are more relevant to fiat currencies than others.

Programmable Money

The phrase "smart contracts" is used to describe a way of running generalized programs on a public blockchain where the primary purpose of the contract may be more than the simple

[14] Jasper – Ubin Design PaperEnabling Cross-Border High Value Transfer Using Distributed Ledger Technologies, Bank of Canada and Monetary Authority of Singapore (2019) https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf

transfer of money. We distinguish support of smart contracts from programmable money, which is more about supporting a limited set of operations which aim to facilitate the transfer of value according to carefully vetted conditions, scripts, and rules. We make this distinction because introducing the full generalizability of smart contracts can come with a cost of complexity and can lead to a larger attack surface, undermining the security of the system. As an example of what useful features programmability can enable in a monetary system, we will discuss atomic cross-chain swaps.

When swapping digital assets a risk arises because one side has to go first. To reduce counterparty risk and ultimately transaction costs, it's desirable to ensure that the exchange happens *atomically* -- either both assets change hands, or neither do. This is traditionally achieved with a trusted third party to hold the assets and facilitate the exchange, like a central securities depository.

We call this the institutional method for eliminating risk. One creates an institution like CLS Bank or DTCC, and ensures participants in the system deal with the central institution rather than each other directly. This does not totally eliminate counterparty risk in the system but transfers it to the intermediating institution.

This structure raises barriers to entry in two ways: First, it is more efficient for everyone in a given market to deal with the same intermediary; if not, counterparty risk is reintroduced between the different intermediating institutions. Second, because of its systemic importance, the central entity needs to be strongly regulated. For example, many central banks sit on the CLS oversight committee[15]--such is its importance.

The interface of cryptocurrencies provides a very different way of addressing this problem: an atomic cross-chain swap. The problem of an atomic cross-chain swap is that Alice and Bob each have different cryptocurrencies, and they would like to exchange them without using a trusted third party such as a cryptocurrency exchange. As described, without a trusted third party to escrow the coins, whoever goes first in this exchange is at risk -- if Alice sends her coins first, in the intervening timespan Bob might renege on his commitment or even disappear, leaving Alice with nothing and Bob with both coins.

Programmable cryptocurrencies solve this problem by using scripts on each chain to escrow the coins. The scripts are programmed in such a way that if one executes a transfer, so must the other. Though the funds are escrowed in contracts, they cannot be redeemed by anyone other than Alice or Bob.

[15] https://www.cls-group.com/about-us/regulation/regulatory-affairs/oversight-committee

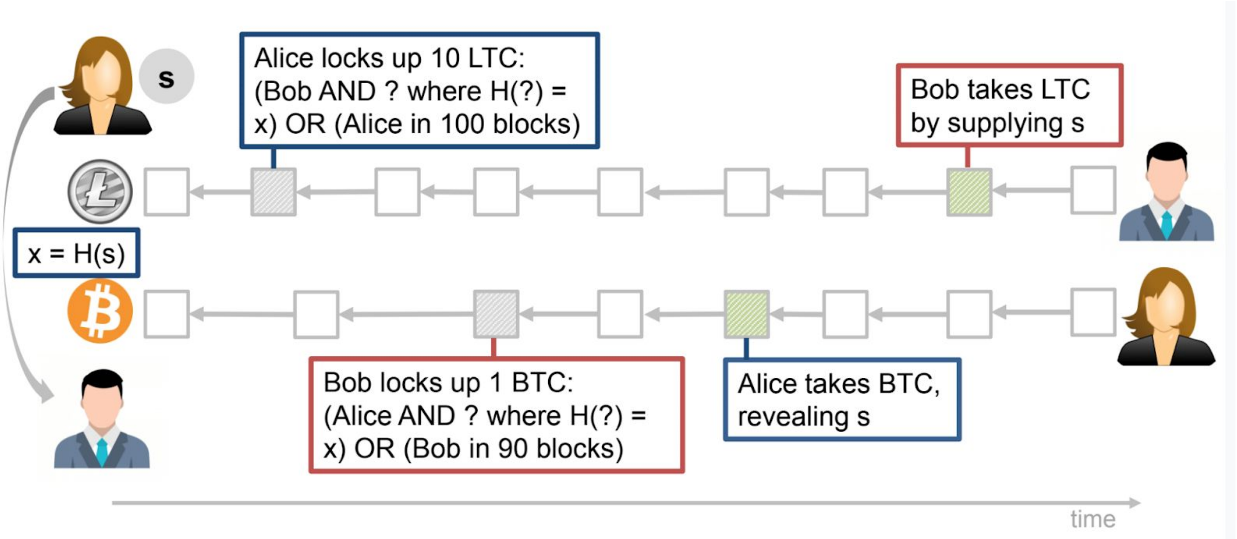
s
Alice locks up 10 LTC: (Bob AND ? where H(?) = x) OR (Alice in 100 blocks)
Bob takes LTC by supplying s
x = H(s)
Bob locks up 1 BTC: (Alice AND ? where H(?) = x) OR (Bob in 90 blocks)
Alice takes BTC, revealing s
time

Figure 1. Alice and Bob wish to trade Litecoin for Bitcoin. Alice chooses a secret s and sends Bob the hash of s, x. Then Alice publishes a transaction on the Litecoin blockchain with a script that indicates that Bob can spend this the 10 LTC in this transaction immediately if he can reveal the preimage of x. In 100 Litecoin blocks, Alice can take her coins back. Bob then publishes a similar transaction on the Bitcoin blockchain spending one BTC. Alice has to show s on the Bitcoin blockchain in order to take the Bitcoin, which Bob then uses on the Litecoin blockchain to take the 10 LTC.

We call this the software method of eliminating risk. The first concrete algorithm to conduct an atomic swap was described in 2013 by Tier Nolan.[16] Since then, there has been much development: Users today can conduct atomic cross-chain swaps between different cryptocurrencies and several projects offer atomic swap services.[17][18] Almost all protocols for conducting these swaps rely on a cryptographic technique of committing to and then revealing a secret in order to claim coins on either chain. Due to the programmable nature of cryptocurrencies, Alice can make her payment to Bob *contingent* on revealing a secret, which is the same secret she must first reveal in order to claim her coins from Bob. Once Alice shows the secret, Bob can then proceed and take his coins. We show a cross-chain atomic swap in Figure 1 where Alice is trading Litecoin to Bob for Bitcoin.

Given the right programmability support, or application program interface (API), these swaps can apply outside of cryptocurrency systems, to many types of digital assets. For example, a CBDC might have the features required to implement cross-chain swaps with cryptocurrencies or future digital asset systems; this would support many use cases, from retail payments to

[16] Tier Nolan. Re: Alt chains and atomic transfers. https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949, May 21, 2013. Accessed January 15, 2020.
[17] Arwen. https://arwen.io. Accessed January 15, 2020.
[18] Summa. https://summa.one. Accessed January 15, 2020.

securities settlement. It is important to note that the guarantees provided are slightly different than if the exchange occurs between two decentralized blockchains: In a blockchain like Bitcoin, no party can unilaterally reverse transactions, so the terms of the swap will not be reversed. And ownership on the blockchain *is* ownership of the asset, so the swap's outcome must apply. If a central bank were providing an atomic swap interface, users would have to trust the bank not to reverse the swap transaction and honor the transfer. If the asset was not blockchain-native, users would have to trust the custodian to honor the chain state. However, this would still reduce risk on the part of the person on the side of the swap collecting cryptocurrency and it provides a useful interface.

Note that atomic cross-chain swaps are a settlement technique -- Alice and Bob still must somehow find each other and agree on the terms of the exchange. As such, they do not eliminate all types of intermediation but they potentially make a market more competitive by reducing barriers to entry for intermediation because counterparty risk is eliminated by the software rather than mitigated by the legal arrangements of a default fund. By reducing the need for centralized intermediaries, they can also reduce concentration risk.

Also note that in existing implementations, atomic swaps actually include an American-style call option. Though the trade is still guaranteed to happen atomically, one party usually has a time option to decide whether they would like the exchange to proceed or not. This technology speaks to the inadequacy of existing regulation to keep up with changing technology. Two users can conduct a bilateral, trustless swap of two cryptocurrencies without involving an intermediary in a way that is difficult to detect or prevent.

Several new blockchain platforms offer developers more expressible, Turing complete programmability in the form of smart contracts. However, this generalizability comes at the expense of increased complexity in the blockchain system itself which has implications for both scalability and security.[19] Any CBDC has to have security as a primary consideration and it may be that CBDCs of the future opt for greater simplicity over ever increasing functionality and complexity. An alternative vision of the future financial system is a very simple base CBDC layer with any added functionality added in the layers above.

But new technology can also provide ways to better implement policy goals. Swaps can assist with systemic risk reduction by enabling a different market structure that relies less on centralized intermediaries. Other cryptographic tools can be useful to support policy goals, such as auditing while preserving privacy.

[19] Atzei, Nicola, Massimo Bartoletti, and Tiziana Cimoli. "A survey of attacks on ethereum smart contracts (sok)." In *International Conference on Principles of Security and Trust*, pp. 164-186. Springer, Berlin, Heidelberg, 2017.

Privacy-preserving auditing

The profitability of advertising and data mining has led to a severe loss of privacy for users. People today are tracked as they browse the web, buy things online, and even as they move around their cities and homes. Most of this data is concentrated in the hands of large corporations, and it is being aggregated and used in surprising and uncomfortable new ways. These corporations have frequently failed to uphold the public's expectations when guarding that data and determining how it can be used.[20]

Turning to the issue of CBDC, it's clear that given the risks associated with surveillance, great care should be taken in preserving the privacy of users' financial transactions. Even if a central bank issues a digital currency, it should never become a panopticon. Legitimate public policy goals relating to combating criminal activity can be fulfilled while preserving the privacy of the public and preventing a central bank being drawn into the commercial surveillance models which are now prevalent in the private sector.

It is important to embed privacy into the technology itself, instead of relying on providers to provide it at the edges, so that it can assist the functioning of other checks and balances in the system. Embedding privacy directly into the technology means that institutions (public or private) will need to appeal to the legal process or gain the consent of the user before getting access to data; this gives the user the ability to get legal redress in the event that data is abused.

An example of this is the recent rise in end-to-end encrypted messaging. In an end-to-end encrypted payment system the central operator cannot automatically observe the payments made by citizens because they are private by default. An example of a practical design is that if there is a suspicion of illicit activity, law enforcement would need to go through the appropriate legal channels to access data on the user's device or at the user's wallet provider. There might be a variety of wallet providers with differing levels of guaranteed user privacy so protecting user privacy will require additional privacy regulation and enforcement. Though payments are by default protected and private, there are ways to embed metadata to help regulate the system and detect illicit behavior.

This is how the technology can enable the rest of the societal architecture (e.g. laws) to properly function as a check on public and private power. We went through a similar debate around HTTPS, the protocol used to secure today's web. At the time, it seemed inconceivable to allow user web activity to be encrypted, and outside the surveillance apparatus. Now over 81% of US government websites use HTTPS.[21] We have learned from decades of experience with and without strong encryption that privacy is critical to security.

[20] Cadwalladr, Carole, and Emma Graham-Harrison. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach." The guardian 17 (2018): 22.
[21] https://https.cio.gov

Initially, this seems at odds with the policy goals to guard against illicit activity, confirm market integrity, and maintain financial stability -- how can a regulator confirm that actors are comporting to the rules if she cannot see what is happening?

This underlying tension between privacy and enforcing public policy can be addressed using cryptographic techniques. We can turn to the example of public verifiability in cryptocurrencies as a starting example: Zcash and Monero aim to keep users' transactions secret while still maintaining public verifiability; *any* user can download either cryptocurrency's blockchain and verify that financial invariants like consent to transfer and the monetary creation schedule are preserved, even though the user cannot see the amounts, participants, or in some cases even the history of the transactions. Research we have done at MIT shows how on a distributed ledger, one can engage a third-party auditor who can get provably correct information about reserves, transaction size, market concentration, and more without revealing the contents of individual transactions.[22]

These systems rely on a primitive in cryptography known as a (non-interactive) zero-knowledge proof. In brief, zero-knowledge proofs concern two parties: the prover, who holds some private data, and the verifier, who wishes to be convinced of some property about this private data. For example, I might want to convince you I possess a government-issued ID indicating I am over the age of 18 without revealing my exact birthdate. I might also want to do this without revealing the establishment I am entering to the government. Or, a user might know a password used to encrypt a file, and wishes to convince the verifier that the password is non-trivial (e.g. has numbers, letters, characters, and mixed case) without revealing the password itself.

Using zero-knowledge proofs, the prover can produce a piece of data, the proof, that simultaneously persuades the verifier, yet does not reveal anything else about the password. Verifying the proof does not require any interaction between the prover and the verifier, and in the case of non-interactive zero-knowledge proofs, the prover can append this proof to the ledger, where it can be verified by any party of the system.[23]

Unfortunately the creators of Libra, one of the most well-known digital currency proposals, have not yet presented a solution reconciling the importance of privacy and regulation.[24] Their solution is the worst of both worlds: all transactions are public[25] and regulators are still

[22] Narula, Neha, Willy Vasquez, and Madars Virza. "zkLedger: Privacy-preserving auditing for distributed ledgers." *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*. 2018.

[23] See here for a visual explanation of zero-knowledge proofs: https://medium.com/swlh/a-zero-knowledge-proof-for-wheres-wally-930c21e55399

[24] https://libra.org/en-US/security-privacy. Accessed January 15, 2020. "The Libra Association will ... continue to evaluate new techniques that enhance privacy in the blockchain while considering concerns of practicality, scalability, and regulatory impact."

[25] https://libra.org/en-US/security-privacy. Accessed January 15, 2020. "Libra is designed to be transparent by default.The operation of all validators can be audited by any participant, and all transaction processing is available to be confirmed by anyone."

concerned about criminals using Libra for illicit activity.[26] Libra has chosen to adopt Bitcoin's model of privacy--pseudononymous identifiers--while relying on wallets and validators in the system to take responsibility for vetting transactions and users. We would argue that a digital currency aspiring to serve billions of users (including some of the most disenfranchised) cannot launch until it has a well-designed and tested solution for privacy.

Zero-knowledge proof technology is still nascent and is developing every day. It is unclear if it can be deployed effectively at the scale of a CBDC, and even if it can, there is no complete solution for CBDC yet. But it is a tool in the toolbox and important to watch. We are optimistic that with enough research and development, we can arrive on a useful architecture that will balance deterring illicit activity with preventing mass surveillance either by the state or private corporations, and one that ensures there are legal safeguards surrounding when data should be released.

Conclusion

A streamlined, cheaper, faster global payment system seems inevitable. The questions are 1) what will it look like? And 2) who will develop it?

We have described three technologies whose applicability to CBDC varies. Though we currently think a decentralized consensus protocol is overkill, programmability seems like a promising avenue. Enabling privacy and auditability through cryptographic techniques will be necessary to reduce the risk of financial surveillance and misuse of data. The second question is who will develop this system? Will it be an upstart cryptocurrency-based stable coin, or a coalition led by a large company like Facebook which already connects with billions of users globally? The motto "move fast and break things" is probably not a good one for a global monetary system.

It might be preferable to have such development done in partnership with democratically accountable institutions that already govern currency and who will carefully evaluate new technology and apply it to payments. Regulators and central bankers are right to be cautious. In this case, exercising caution means understanding what the technology can and cannot do, whether by staffing up internally or partnering with technical organizations, and preparing for an uncertain future. The industry is moving fast; the most perilous path of all is inaction.

These remarks are based on a speech October 17, 2019 at the Conference on the Economics of Central Bank Digital Currency at the Bank of Canada.

Contact

Neha Narula	Robleh Ali
narula@mit.edu	robleh@mit.edu

[26] https://ico.org.uk/media/about-the-ico/documents/2615521/libra-network-joint-statement-20190802.pdf