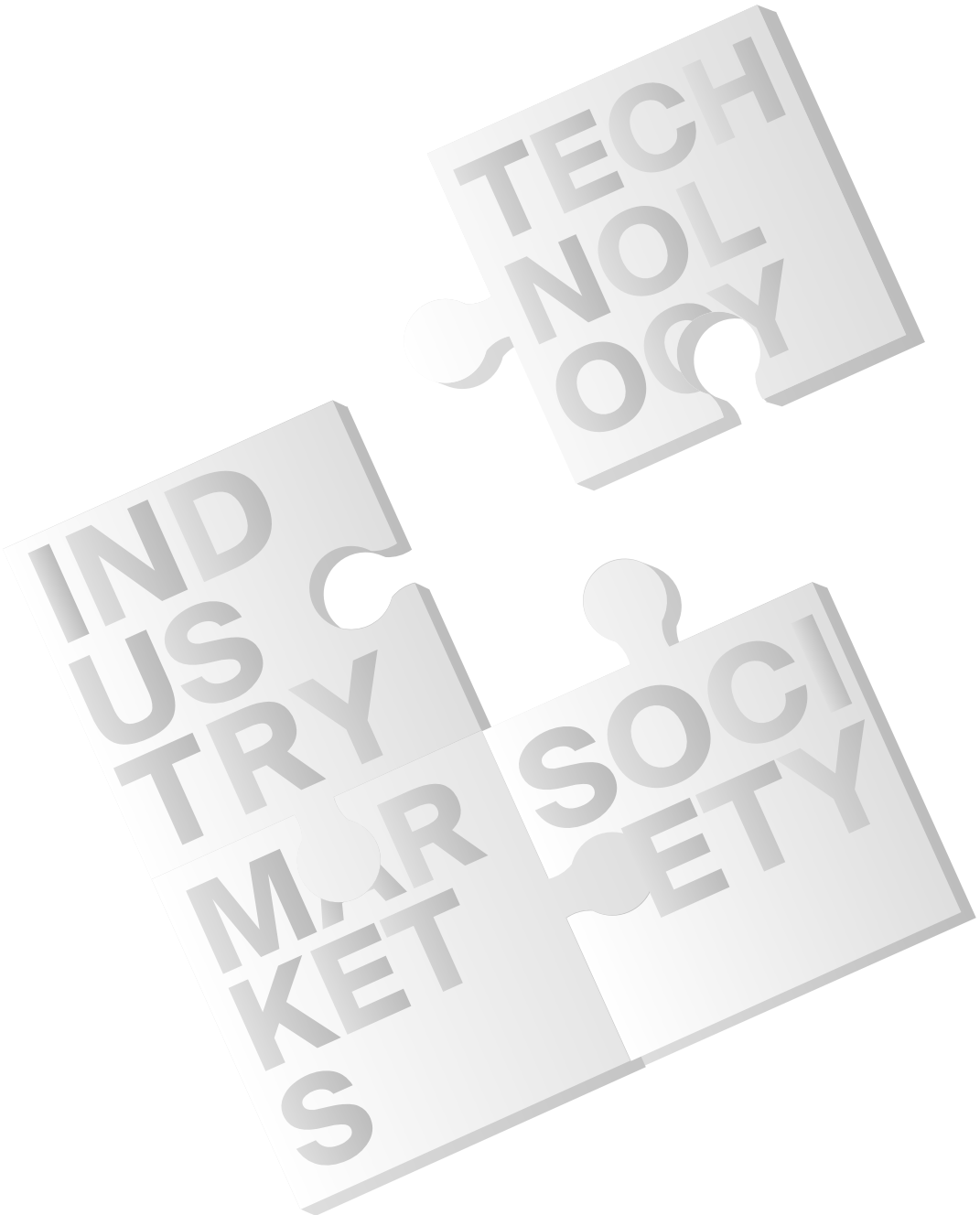
Bitcoin Suisse Themes - Technology

Privacy in the era of cryptocurrencies



Bitcoin Suisse

Contents

Key takeaways	**4**
Introduction: Money, privacy and society	**5**
Traditional cryptocurrencies and privacy	**7**
Privacy coins	**11**
Corporate currencies and privacy	**14**
Central bank digital currencies and privacy	**17**
Conclusion: Privacy and the individual crypto user	**21**

Digital Currencies Privacy Matrix

How various digital currencies compare in terms of key privacy considerations.

	Traditional Cryptocurrencies	Privacy Coins	Corporate and Private Money	CBDCs
Provide full anonymity and robust privacy?	No	Yes	No	Depends on the coin design
Can be used without revealing personal information?	In theory yes, in practice PI can often be revealed	Yes	No	Depends on the coin design
Are decentralised and not under the control of any entity?	Yes	Some, not all	No	No
Are legal to use?	Generally, yes.	Not everywhere, great deal of regulatory uncertainty	Yes, if approved	Yes
Are easy to use?	Generally yes, but some require technical savvy	Generally less so than traditional cryptocurrencies	Would likely be very user-friendly	Would likely be user-friendly

Key Takeaways

- **Money and privacy are intimately connected.** Financial privacy is an important individual right, yet the traditional financial system is increasingly unable to protect our data.

- **Cryptocurrencies are generally not private.** While cryptocurrencies like Bitcoin were invented in part to protect individual financial privacy, in practice they are highly transparent payment systems.

- **Privacy coins can help to a degree.** Privacy coins can indeed shield an individual's transactions, though not always as completely as many assume.

- **Government and corporate digital currencies will be coming soon.** CBDCs and corporate money, like Facebook's now-shuttered Libra, may pose serious challenges for financial privacy.

Introduction: Money, privacy and society

Digitalisation and the breakdown of financial privacy

There are few things more personal yet more revealing than money. Anyone who knows how much money you have, or where, when and on what you spend it, can get a very clear picture of who you are – perhaps even a more accurate picture than the one you have of yourself.

While this has always been the case, the move towards digital money in the modern era has given new urgency to the conversation around money and privacy.

Before computers, money was tangible. It existed as gold, banknotes or entries in a bank's paper-based ledger. All of these are physical things, and so can be physically protected. Dematerialised bits and bytes are far easier to copy, forge or steal. Thanks to digitalisation, financial networks are also much larger, far more complex, and involve a far larger number of non-financial institutions than in pre-digital days.

This has given an almost endless array of third parties practically unlimited access to our financial records, often without our knowing it.

These companies may not be able, or willing, to safeguard our information as well as banks do. Few people for example are probably aware that Paypal routinely shares client transaction data with over 600 other companies.[1] Nor is it just Paypal. As one researcher has put it, today's financial system is like a "panopticon of consumer behavior."[2]

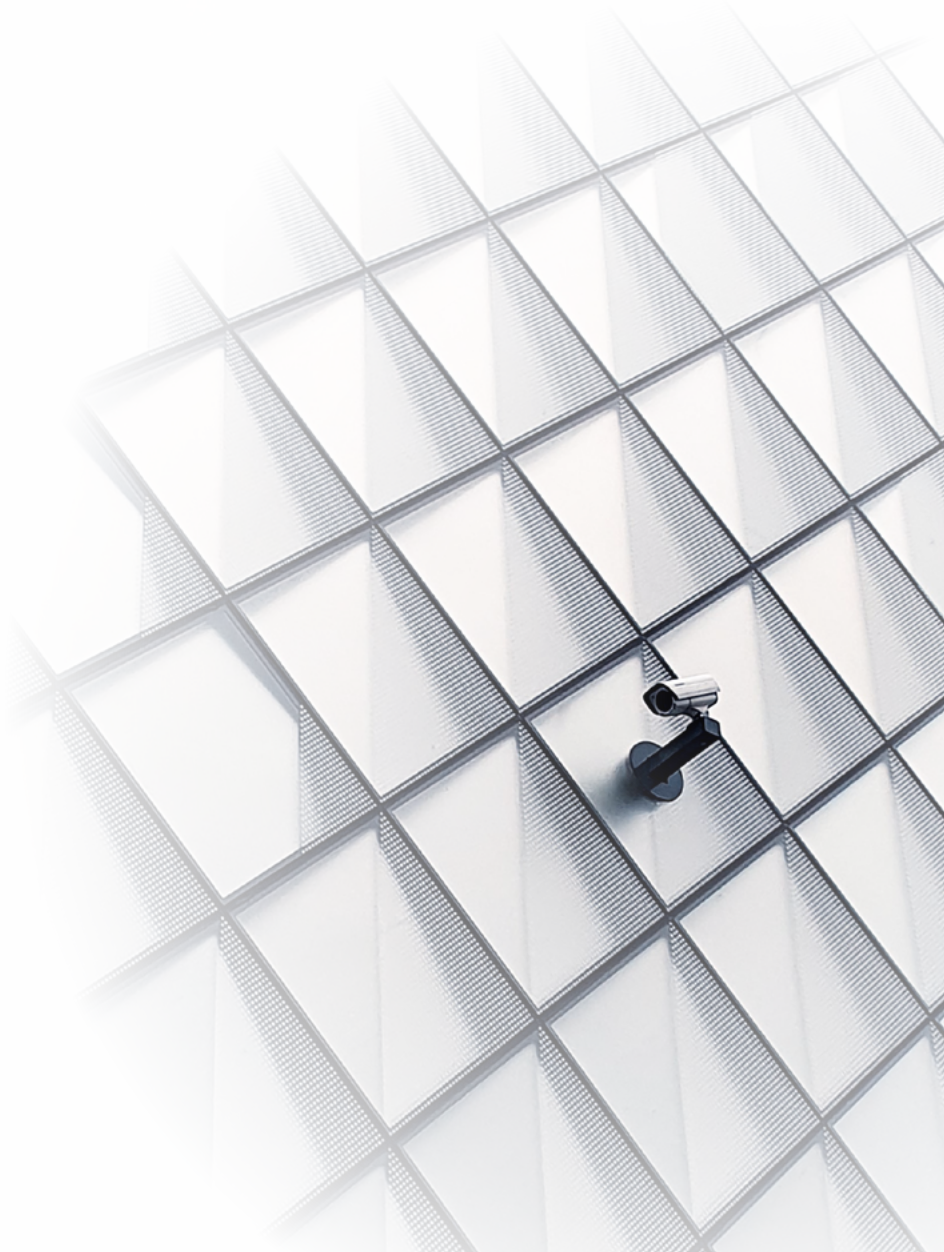
Sources

1. List of Third Parties (other than PayPal Customers) with Whom Personal Information May be Shared, Paypal

2. Can Cryptocurrencies Preserve Privacy and Comply With Regulations?, Geoff Goodell and Tomaso Aste, Frontiers in Blockchain, 28 May 2019.

Cryptocurrencies were founded in part as a response to this state of affairs. But how secure – and how private – are cryptocurrencies, or for that matter the other forms of digital money that are arising today as a side effect of the crypto revolution?

That is the subject of this paper. As we try to show below, while the answer is not necessarily straightforward, the stakes involved can be high. It is therefore a subject that we believe anyone using or investing in cryptocurrencies will want to be aware of.



Traditional cryptocurrencies and privacy

"Bitcoin is probably the most transparent payment network in the world"[3]

bitcoin.org

Bitcoin is not private

On the surface, Bitcoin seems very private.

You do not have to sign up to use it. There is no company or authority in charge of it. You do not need to reveal any personal information to send or receive coins. As open source code that can easily be examined, users can be sure that there are no secret backdoors or other covert surveillance mechanisms hidden away inside it.

This assumption of privacy has been one of Bitcoin's main draws over the years, attracting idealists of many different stripes concerned with financial and individual freedom. Initially it also attracted a fair number of shady characters, including drug dealers and hackers. It has been estimated that some 25% of Bitcoin transactions in its early days were for illegal purposes.[4]

The bad guys have since had a rude awakening. As people became more familiar with how BItcoin and blockchains work, it became increasingly apparent that blockchains are not very private at all. With a bit of effort, supposedly anonymous Bitcoin transactions can be "de-anonymised", sometimes to an astonishing degree.

In 2019 Qatari researchers revealed 125 transactions linked to dark web sites simply by searching the Bitcoin blockchain for direct links between addresses.[5] Since then, stories of bad guys being caught because they used Bitcoin have been as predominant as those of Bitcoin being used to commit crimes. Today

researchers estimate that significantly less than 1% of Bitcoin transactions are traceable to illegal activity.[6]

Drawing back the curtain on blockchain transactions

In hindsight, this should have come as no surprise. “Traditional blockchains” like Bitcoin, based on public, permissionless distributed ledgers secured by open, community-run consensus mechanisms, have privacy holes practically baked into their design.

A blockchain is a permanent record of all transactions back to the first one. While this unbroken, cryptographically secure chain of information is what keeps the network secure, it also means that anyone can download this transaction history and analyse it at will.

The Bitcoin addresses, transaction amounts and timestamps saved to the ledger are like bread crumbs that can be used to follow a transaction. That’s why we can speak of coins becoming “tainted by the history of all transactions they are involved with”.[7]

The good news for users is that there are ways to make their Bitcoin transactions less traceable.

Chief among these is to generate a new address for each transaction - a simple but effective precaution that is now standard practice in many wallets. Users can also make use of various mixers and tumblers, services which “wash” coins by combining transactions together until their origins can no longer be ascertained for sure.

Over time many traditional blockchains have added privacy features to their protocols too, either by design or as a result of updates made for other reasons. As we recently pointed out in a separate paper, Bitcoin’s Taproot upgrade is such a case.[8]

Such precautions can only go so far. As long as a blockchain remains public, there will be those who will analyse it to tease out its secrets. The blockchain, according to one expert, is an

"open source researcher's dream."[9]

The two major privacy holes in traditional blockchains

There are two main areas through which blockchains can leak information.

For one, there are the "on-and-off ramps" to the chain. Most people buy and sell cryptocurrencies through exchanges. The majority of exchanges today are regulated legal entities, and so required by KYC/AML laws to collect their customers' personal information and make it available to law enforcement if presented with a warrant.

Merchants who accept Bitcoin are another potentially large security hole. If the merchant is sloppy, for instance by using the same Bitcoin address over and over again to receive payments, then this address will be known – and be a powerful clue to correlate transactions to unknown user addresses.

Many online merchants also routinely share their data with third parties, meaning that information about a user's Bitcoin transaction could end up in many different hands. This can increase the amount of information that can be used to draw such correlations.[10]

The second major security hole for cryptocurrencies is the blockchain itself. Specialists with a deep technical understanding of how blockchains work and the requisite resources are today able to analyse blockchains to an astonishing degree. This has helped create a new blockchain analytics industry populated by companies focused on doing just this.

It has become a big business. Companies like Chainalysis, CipherTrace, MerkleScience, Elliptic and others offer financial institutions, law enforcement, regulators and others a wide variety of services based on de-anonymising blockchain transactions.

Such analytics involve a lot of sophisticated techniques, often augmented by artificial intelligence, including things like clustering algorithms, web scraping, scam database monitoring, and dust attacks.[11]

These techniques are highly technical, and users need not necessarily understand how they work. The important thing is to understand that they do work. The truth is that public, permissionless cryptocurrencies based on the Bitcoin blockchain model are hardly private at all.

Sources

3. Protect your privacy, bitcoin.org.
4. Are Privacy Coins Better Investments Than Bitcoin? The Motley Fool, 30 July 2021
5. Your Sloppy Bitcoin Drug Deals Will Haunt You for Years, WIRED, 26 Jan 2018.
6. Crypto-crime & caveats, Thomson Reuters, 29 March, 2021
7. Ibid bitcoin.org.
8. Bitcoin Suisse Decrypt Episode 18 - Taproot - Sowing the Seeds for Bitcoin DeFi
9. Tracking Illicit Transactions With Blockchain: A Guide, Featuring Mueller, Brenna Smith, 1 February, 2019.

Privacy coins

"IRS-CI is seeking a solution with one or more Contractors to provide innovative solutions for tracing and attribution of privacy coins."[12]

- United States Internal Revenue Service Criminal Investigation Agency

New coins to improve privacy

Technological advance is often a cat and mouse game.

As blockchain analytics companies improved their techniques to de-anonymise transactions, privacy-minded technologists and entrepreneurs began to look for ways to counter them.

Seeing that the original blockchain model was not secure, several decided to build new types of blockchains with more robust privacy characteristics. This was the birth of "privacy coins".

Privacy coins are designed to do what it says on the tin: provide true privacy and anonymity for monetary transactions. They typically do this in one of two ways: a) by encrypting cryptocurrency transactions so that it is impossible to tell who the parties are or what the amount was, and/or b) making it difficult if not impossible to follow the trail of the transactions.[13]

Many of the techniques used to accomplish these goals, like stealth addresses, zero knowledge proofs or ring signatures, come from the cutting edge of cryptography and computer science.

Zero-knowledge proofs, for example, are a set of techniques that allow someone to prove mathematically that he or she is in possession of a certain piece of information without revealing that information. A subset of these, called ZK-SNARKS, can be used to prove the validity of transactions on a blockchain without revealing anything about those transactions. Ring signatures are a way of collectively signing transactions so that

it is impossible to tell who signed which. They effectively hide individual transactions in a crowd.

There are also coin mixers, which jumble coins used in transactions in a way that makes it much harder to trace them. Services like Tornado Cash on Ethereum or the Coinjoin mixer as used by the Wasabi or Samourai wallets for Bitcoin work by pooling the transactions of a large group of users into a single pot, and then pulling the money out from a different address. The code of the mixer assures that the right parties receive the correct amount of funds, but there is no way to link a sender and a receiver directly.

Finally, there are projects that aim to bring privacy to the protocol level. On Ethereum, both the Aztec protocol, which aims to provide "the ultimate security shield for the Internet of money,"[14] and MatterLabs[15], whose zkSync scaling solution also adds transaction privacy, are good examples of these.

Not all privacy coins are private

So do these coins really provide absolute privacy to their users? The answer is generally yes, but with some caveats.

Firstly, not all privacy coins offer the same levels of privacy.[16] While Monero, for example, offers privacy by default, other popular privacy coins, like ZCash or Dash, offer their privacy features as an option that the user needs to choose.

In the case of ZCash, currently only about 5% of users do so. This small number potentially weakens privacy, as it makes it harder to hide transactions in the crowd, and hence easier for analytics techniques to work.

Secondly the rise of privacy coins has spurred efforts to find ways to penetrate their shields. In one famous example, the IRS has put a bounty out to fund research into de-anonymising privacy coins, and has since awarded contracts worth USD 1.25 million to companies on Monero's trail.[17]

Ironically, providing full privacy by encrypting transactions of a cryptocurrency may, at least in theory, pose a security risk to the currency itself. If all transactions are encrypted, it can be hard to keep track of how many coins are in circulation. This can open the door to counterfeit coins, and make it hard for

cryptocurrencies to enforce caps on their amount of issuance.

Privacy coins are also often harder and more expensive to use than traditional cryptocurrencies, reflecting the tradeoff between security and ease of use that is an axiom of computer science.

Last but by no means least, privacy coins exist in a kind of legal limbo at the moment. Some countries, like South Korea and Japan, have banned them outright. In others, like the US, they are legal for now. As governments beef up their cryptocurrency regulations, particularly in terms of anti-money laundering (AML) and know-your-customer (KYC) requirements, this may change.

It is therefore quite possible that privacy coins that are legal to use today will become illegal to use in the future. For many users, especially mainstream ones, being on the wrong side of the law is not an option. This is a problem that even the most robust privacy technology cannot solve.

Sources

12. US Internal Revenue Service - Criminal Investigation, Request for Proposal 2032H8-20-R-00500, 4 September 2020.
13. For a good short overview, see Privacy Coins 101, The Legal Examiner, 23 September, 2021..
14. aztec.network.
15. matter-labs.io.
16. This section is heavily indebted to What are privacy coins?, Cointelegraph, October, 2021.
17. What Are Privacy Coins? Monero, Zcash, and Dash Explained, Decrypt, 31 May, 2021.

Corporate currencies and privacy

"Corporate money and governmental CBDCs are both terrible ideas and go against the values of the crypto ecosystem."

Sebastian Bürgel, Founder of the HOPR protocol

The rise and fall of Facebook's Libra

A fascinating development coming out of the cryptocurrency revolution is the prospect of private corporations issuing their own digital money. This issue recently came to the fore with Facebook's now stalled Libra project. Because it raised a lot of privacy issues, it is worth looking at in some detail.

Announced in 2019, Libra was meant to be a decentralised, global digital currency based on a purpose-built blockchain and run by the Libra Association, a non-profit consortium whose members at the time of founding included not just Facebook, but such names as MasterCard, Visa and eBay. According to the original plan, the blockchain would not be proprietary but would be built as an open source project. The Libra Association would also not be run by Facebook, but by all of its members in concert.

Libra promised many of the same benefits of traditional cryptocurrencies, and did so on a large scale. It would be available globally, and so support financial inclusion, especially among Facebook's millions of users in underdeveloped countries. It would be a platform for low or no cost remittances. As a de-facto global stablecoin – the original Libra token was meant to be backed by a basket of global currencies and cash equivalents – it would spur innovation and provide something

of a level playing field for global businesses, including small businesses in developing countries looking to do business in developed markets. Combined with the global nature of Facebook and other Libra Association members, that could have meant a great deal of reach indeed.

These were all lofty objectives. But almost immediately after the project was announced, it faced heavy criticism and pushback from governments and privacy advocates. The outcry was so strong that Facebook was forced to alter and then scale down the project.

With Libra 2.0, Facebook abandoned the idea of a stablecoin backed by a basket of currencies in favor of a model in which there would be national versions of Libra backed by the national currencies of individual countries. This was not enough to quell the criticism, and Facebook eventually abandoned Libra altogether, downsizing the project and rechristening it Diem.[18]

Two main areas of concern doomed Libra. The first had to do with systemic risk and monetary sovereignty. Policy makers were afraid that a Facebook coin, because of the vast number of Facebook users, would immediately become a systemically relevant global currency. It therefore would represent a potential risk to the global financial system.[19] More importantly for many governments, a parallel currency used regularly by three billion people around the world could rob individual governments of control of their own monetary policy. This was a red flag.

The second area of concern was privacy. There were fears that Libra would give the companies backing the project, who already held troves of their users' personal data, access to their financial transaction histories as well. Facebook took great pains to insist that this would not be the case. But at the time Facebook was mired in a number of other data privacy scandals, including Cambridge Analytica, and its claims lacked credibility in many circles.

The double-edged sword of private money

It is interesting to speculate what might have happened if Libra had been developed by a consortium of global tech and financial giants that did not suffer from Facebook's reputational baggage. A globally available, corporate-backed cryptocurrency would have been seen by some as a stunning victory for the cryptocurrency movement. Others would no doubt have viewed

this as a terrible blow to the cause of financial privacy that has drawn so many to that movement.

Such speculation is relevant because, while Libra may have failed, there is no reason to think that other such projects might not arise some day. Blockchain technology makes this fairly easy to do, and the success of Bitcoin serves as a tantalising model.

The idea of full-on corporate money is not far-fetched if you consider that we already have hundreds of thousands of proto-corporate currencies in circulation today in the form of loyalty points, mileage points, and similar types of programs. These are already considered privacy nightmares by many as they are often designed not just to foster loyalty, but also to collect customer data. It is hard to imagine that large-scale corporate currencies issued by companies with business models based to an extent on data collection would not to some extent be driven by a desire to collect more data as well.

Loyalty points may not be considered “real money” today mostly because they are not interoperable: they only work on certain platforms and/or for certain items. Blockchain technology can not only make it much easier and cheaper to issue such private currencies in the form of crypto-tokens, it can also make it much easier to exchange this money between different entities.

The more broadly these coins can be exchanged, the more widely they can and likely will be accepted as a medium of exchange by large numbers of people – especially if they are somehow more convenient or more useful than other means.

In other words, they will become money.

Sources

18. See diem.com. The project’s future remains uncertain. See e.g. Is Diem doomed?, Tech Monitor, 21 October, 2021.

19. France: We can’t allow Facebook’s Libra in Europe, Reuters, 12 September, 2019.

Central bank digital currencies and privacy

"The window is still open to guarantee privacy for users of digital currencies, but we have to get the balance right between privacy and compliance."[20]

Thomas Moser, Alternate Member of the Governing Board,

Swiss National Bank

Central banks are now very interested in digital money

Because they deal with money issuance themselves, it is probably not surprising that central banks have long had an interest in cryptocurrencies.

Until recently this interest had been largely academic. Facebook's announcement of Libra changed all that, acting as a kind of wake-up call to central banks around the world that they had to take cryptocurrenices and blockchain technology much more seriously. Today the majority of central banks are actively investigating using blockchain or other technologies to issue digital versions of fiat currencies for general purpose use – what have become known as central bank digital currencies or CBDCs.

Government-issued digital money could have a major influence on cryptocurrency markets. CBDCs might become strong competitors for cryptocurrencies, potentially rendering the latter irrelevant. Alternatively they could drive large-scale adoption of cryptocurrencies by helping ordinary people get used to the idea of electronic money and digital wallets. If CBDCs are built on blockchains, they could have a very positive effect on the blockchain industry too, as central banks turn to blockchain companies to help them realise their projects.

So what is a CBDC exactly?

At its simplest level, a CBDC is a digital currency issued by a

central bank. While central banks issue digital money today, they do so indirectly by crediting the electronic ledgers of large financial institutions.

Banknotes currently represent the only central bank money that citizens can use directly. A CBDC would be a digital token that would represent a claim against the central bank itself and, like cash, be able to circulate directly among the population.

Issuing such a CBDC could be done in one of two ways.

In what is known as a wholesale CBDC, the central bank issues the coins only to financial institutions, who in turn circulate them among businesses and private individuals. This is analogous to how the system works today. Central banks could also bypass banks and issue a CBDC directly to citizens. This is known as retail CBDC, and, if realised, would represent a major change to the current monetary system.

There is a lot that speaks in favor of CBDCs. They eliminate counterparty risk. There can be no bank runs and no defaults unless the government itself defaults. A retail, direct-to-citizen issued CBDC would also make it much easier than it is today for central banks to get money to citizens in an emergency, for example a pandemic or as part of a Universal Basic Income program.

Unlike cash or digital money today, CBDCs could in theory make use of smart contract technology to create programmable money. CBDCs could be programmed to automatically deduct taxes during transactions, or to automatically pay interest to the bearer (or deduct it if central banks wish to introduce negative interest rates). That in turn could give central banks a much more direct control over monetary policy than they have today.

CBDCs will have a wide range of privacy issues

But many people, including central bankers, worry about CBDCs too. There are concerns about how they might disrupt the current banking system, for example by disintermediating banks and causing bank runs. They worry about security: it is a bad thing if a bank gets hacked, but generally only affects that

bank's customers. It would be an unmitigated disaster if the digital currency of a sovereign nation was compromised. Central bankers also struggle with the thorny legal and regulatory issues that CBDCs raise.

There are privacy concerns as well. How serious these are depends to a large extent on whether the CBDC is account-based or token-based.

In an account-based CBDC, all citizens would have an account at the central bank and payments would be made by debiting and crediting accounts. That means the central bank would be privy to all the transactions made by everyone in the country. Such information could be advantageous of course, particularly in fighting crime. But it would require the central bank to collect, store and secure an almost unfathomable amount of data.

Developing an account-based CBDC for an entire country would be a very expensive and technically challenging undertaking. Central banks would therefore likely sub-contract CBDC development to private companies. That could place all this sensitive information in private hands.

A centralised, account-based CBDC would also be a security nightmare, with the central bank accounts representing a tremendous honeypot to potential hackers, criminals and spies. It would also be a single point of failure.

Such issues could be avoided by issuing a token-based CBDC. Like Bitcoin, token-based CBDCs would be digital bearer instruments that could be exchanged directly between individuals, and would not require any central bank account, or any bank account at all.

Token-based CBDCs raise some interesting privacy questions as well however, especially for the central banks issuing them. A central bank could release a completely anonymous retail CBDC that, like banknotes, cannot readily be traced. As this would be a potential boon to criminals and terrorists, it is safe to assume that most central banks would want to issue token-based CBDCs that contain features that allow them to be traced

to some degree, and if needed removed from circulation.

The question then is to what degree. It will be a great challenge for central bankers to find the right balance between privacy and security. Their solutions will influence how financial privacy in the digital realm develops, either for good or ill.

Sources

20. As presented at the Crypto Valley Conference 2021.

Conclusion: Privacy and the individual crypto user

"Individuals in a free society have a natural right to privacy, including financial privacy."

While it is important for society to protect individuals, individuals in a free society also have a natural right to privacy. This includes financial privacy.

The traditional financial system tries to provide this through legislation and through the expectation that financial institutions guard our financial information. In the decentralised world of crypto, the onus is on the individual user to take measures to protect their financial privacy while also remaining within the law. As we have seen, this can be a complex task.

Over time we expect many of the open questions of today to be settled. As crypto increasingly goes mainstream, it will become clearer to users what they can expect in terms of financial privacy, and what is expected of them. In the meantime, users should simply be aware of the issues and take reasonable precautions.

In our opinion, the following are the most important points out of the above discussion to keep in mind.

Be aware of address linkability. Always be aware that all your transactions on a public, permissionless distributed ledger are being recorded. As we have tried to illustrate, even if they are not linked to your personal information directly, under the right circumstances they could be. No matter how many different addresses you might send coins through, their tracks remain visible – forever.

Don't publicise addresses or your crypto activities. This may seem obvious, but there have been many cases of crypto holders, even sophisticated ones, being indiscreet with their information. A classic case is someone posting on social media that they own a certain NFT, which is associated with an Ethereum address. In that moment, the address is known to the

Sources

21. hoprnet.org

world, providing a data point to potentially de-anonymise that person's other transactions.

Your behavior can betray you too. Some of the more sophisticated blockchain analytics techniques involve various types of "fingerprinting" activities. These are about discovering behavioral patterns that can be linked to you. Perhaps you are in the habit of using a certain exchange every day at a certain time of day. Perhaps you do a certain type of trade with select pairs of currencies on certain exchanges or platforms that are unique to you, or you always make a certain type of transaction at a certain time. All of this information is permanently available, and if someone is able to connect the dots on a few pieces, it becomes easier to connect the dots on a lot more. We are all creatures of habit. To protect financial privacy in the crypto world, it can pay to be aware of your habits and what they may say about you.

The "Web2 world" is a potential privacy hole. Identity can also be revealed through simple use of the Internet. Your IP address, for instance, is revealed every time you go online. If you use a centralised exchange, the exchange knows your IP address too, and other crypto transactions from that address can in theory be linked to you. But even a decentralised wallet, unless it is directly connected to a full node, will have a traceable IP address. This is a potential privacy hole too. One way to guard against this is to use a VPN, although here you are putting trust in the VPN provider. Newer solutions, like the HOPR project in Switzerland[21], aim to provide completely anonymous messaging and data transfer at the network level on the Internet by use of a decentralised, trustless network. Such solutions provide a much more watertight and trustworthy solution for all Internet users, including cryptocurrency users.

Tom Lyons

Tom Lyons is an independent communications consultant based in Zurich. Previously an Executive Director at ConsenSys Switzerland, he advises startups, governments and other organisations on communications, messaging and thought leadership.

linkedin.com/in/tom_m_lyons

twitter.com/tom_m_lyons

Dr. Marcus Dapp

Marcus Dapp joined Bitcoin Suisse AG as Head of Research in September 2021. He spent most of his professional life in academic research and teaching with side trips to the public and the NGO sector.

His interest in the effects of digitization on economics and society led him to explore a wide gamut of topics over the years; spanning from open digital innovation, intellectual property rights, open source and data to finally peer-to-peer cryptocurrencies.

Bitcoin Suisse

Bitcoin Suisse AG

CH-6300 Zug

bitcoinsuisse.com