UCL Centre for Blockchain Technologies

Discussion Paper Series

Q3 2022

Discussion Paper 2

Central Bank Digital Cash

A Credible Commitment to Privacy

Ian Grigg, P4P Foundation

Abstract

Central Banks are committing themselves to issue digital cash to retail or end-user customers. In so doing, they face a number of contradictions in their goals. Imposing AML, promoting financial inclusion, and not upsetting term transformation pose challenges. Riding above these challenges is the paradox of privacy: users will only respect digital cash if it is private and they feel safe in their use. This same privacy ensures that the bounty of transaction data will be a prize of great value, to be enjoyed in the breach by a host of enemies. If Central Banks do not preserve the privacy of users' transactions, they will not adopt. As there is no easy or stable balance in privacy in such a dynamic and complex system, this is an undecidable problem, and so Central Banks must take the users' side. To ensure success, I propose that Central Banks must provide a credible commitment to privacy, else see their designs rejected by a sceptical public.

Keywords

CBDC, Privacy Paradox, Financial Inclusion.

CBT

Central Bank Digital Cash
A Credible Commitment to Privacy

Ian Grigg 2021-2022 [1]

Abstract: Central Banks are committing themselves to issue digital cash to retail or end-user customers. In so doing, they face a number of contradictions in their goals. Imposing AML, promoting financial inclusion, and not upsetting term transformation pose challenges. Riding above these challenges is the paradox of privacy: users will only respect digital cash if it is private and they feel safe in their use. This same privacy ensures that the bounty of transaction data will be a prize of great value, to be enjoyed in the breach by a host of enemies. If Central Banks do not preserve the privacy of users' transactions, they will not adopt. As there is no easyor stable balance in privacy in such a dynamic and complex system, this is an undecidable problem, and so Central Banks must take the users' side. To ensure success, I propose that Central Banks must provide *a credible commitment to privacy*, else see their designs rejectedby a sceptical public.

Introduction

A Central Bank Digital Cash (or CBDC) is a new digital payments system in competition with cash, and with banks. Technically, it is an accounting system moving fiat value from one device to another, where that device might be cards, phones or computers. Legally speaking, a CBDC is a contract of value issued by the Central Bank offering both guaranteed redemption for fiat and the right of transfer.

Much research is being done on this topic by Central Banks (CBs), and it will take a long time. For the most part, this delay is because (a) the CBs have not had to issue a new currency, or a new payments technology in a long time, and must recover the knowledge to do this; (b) a CBDC necessarily involves the retail public, and CBs are disjoint from that user community; and (c) there are a number of stark contradictions that they will face.

Let's be clear on one thing. We know how to build the technology to do this, and have been able to do this since the 1990s. Several systems were fielded in the 90s that were capable of reaching this approximate goal across a range of technologies. To name but a few: Mondex, Chipper and Chipknip put money on smart cards across many countries, and they worked offline. David Chaum's eCash (Chaum 1982) and my own Ricardo (Grigg 2000) are software money; eCash was blinded money (untraceable but known person) whereas Ricardo used pseudonyms (traceable but unknown person), the method that was later adopted by Bitcoin.

[1] This paper received useful and critical commentary from George Papageorgiuo and Konstantinos Sgantzos.

When compared to the issuance of a CBDC, Bitcoin brought little that was new or relevant to this equation, as blockchain's decentralised model does not bear directly on centralised issuance, and the smart contract model is clumsy when it comes to describing simple contractual digital cash. And, speaking as someone who issued fiat cash several times in the 90s and 2000s, Tether & friends are still behind the state of the art in terms of governance or operations. But, commercially, crypto has broken ground, and as a competitive powerhouse it has suggested that CBs must compete.

By this caveat, I stress, although the narrative might bubble with excitement about the technology, the hard questions at hand are not about the technology. Or, as Izabella Kaminska put it (Kaminska 2021):

> *But framing the conversation as a technological challenge is nonsensical. All it does is detract from the very real downsides of overly centralised systems and the true nature of the competition at hand, which is a function of interest-rate arbitrage, the sort of privacy users value more (privacy from the state or from data-mining merchants and other private sector entities), and the question of whether deplatforming is effective at all.*

Rather, all of the unknowns are political choices, which need to be turned into policy decisions, before being handed to the IT guys to implement. Of course, these are critical to get right. But they are also problematic - who makes these choices, and in whose interests?

Cui bono? Of these difficult choices, there are several that stand out as competing, and potentially problematic to achieve them all:

1. Anti-Money Laundering (AML) regulations
2. "Financial Inclusion"
3. Zero impact on banking
4. Privacy

I suggest that these choices present hard contradictions, each of which alone could sink the CBDC project. Combined, they are much more problematic, and thus demand a much more serious analysis from Central Banks than has hitherto been seen.

Of these four, one could argue that the first three are business as usual. But the fourth, privacy, is setting up society for a dramatic shift at a fundamental level, one which will move us from a world of private transactions to a world of mass financial surveillance. Such a change in the very fabric of how our society works demands more than Central Bank policy discussions - unwinding the financial privacy that has characterised society for its entire existence is an all-of-society question which will have consequences that few can predict.

For these motives – to examine the all-of-society question of the potential end of financial privacy – let's work briefly through the first three challenges in turn, and then dive more deeply into the fourth.

Challenge 1 - AML regulations

Our first choice, **Anti-Money Laundering,** is a non-choice. In the mid-2000s, Central Banks signed up to the agenda of a secretive and undemocratic organisation called the Financial Action Task Force (FATF), and have since become cheerleaders. The CBs consider it non-negotiable that a digital cash must deliver "financial integrity," a phrase that confusingly covers KYC (loosely derived from *know your customer*), AML (*anti-money laundering*), CFT (*counter-funding of terrorism*), and something to do with taxation.[2] From the perspective of insiders and the CBs themselves, the only thing that matters here are the details of implementation.

Unfortunately, these terms all speak to mass financial surveillance. As Darbha & Arora put it (Darbha & Arora 2020):

> "Maintaining privacy and **complying** with regulations (the latter which requires disclosure of information) present a dichotomy for a CBDC. This is further complicated by **the need for proactive disclosure** to prevent fraud."

The basic assumption of AML is that the authorities can see what you are up to, and can stop you, if you are in some sense on their naughty list.

Controls that kick in at a certain limit

Typically, authorities talk about setting a limit - above some number X they can see, and "follow the money," while below X they can't see.[3] From a security point of view, this is unimpressive, as we don't have anything in the computer science or cryptography toolkit that clearly and obviously fixes X as a number that the people can rely upon. Nor, from a political point of view, will a fixed X be acceptable.

To underscore the intent of occasionally changing X to suit local politics, in recent times, the US tax department tried to move one such reporting X down to $600 *annually* (Davison 2021) and the EU voted to set its equivalent X, also aggregated over a year, to €1000. Meanwhile the President of Kenya instructed that its X be lifted to above $10,000 for a single transaction (Indeje 2021).

[2] In this paper, for brevity, I prefer the term AML, and use it broadly to include KYC, CFT, and any other applicable terms such as "financial integrity," which latter is best avoided as a misnomer, as the financial system retains its integrity no matter how much money laundering it suffers.

[3] We can make a similar argument about blocking transactions above X, but that has primarily an economic effect not a privacy effect.

By way of comparison, Kenya's limit would be above their annual average salary. For Americans, this would equate to moving the reporting threshold *for a single transaction* above say $50,000, suggesting a variance in reporting of 100 to 1, without even considering the aggregate demand of the IRS. Not all is in Kenyans' favour as Kenya's tax department went to court to get the right to see all transactions (Juma 2020), suggesting they want to set their X at zero.

Hence any control will necessarily be a dial that can move X up and down at the behest of authorities, at will, and thus X will be arbitrary; in essence, the people are being offered a bait & switch by their Central Banks as they will likely promote a high X in rollout and then find themselves lowering it according to the politics of the day.

Privacy on the other hand says it's none of other people's business, and dangerous to the individual if this information is shared. Legally, privacy is well established in principle with for example US 4th Amendment; *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…"*; Also see EU's Charter of Fundamental Rights, Articles 7, 8, and the UN's Universal Declaration, Article 12.

All of these legal rights suggest that spying on people's transactions on a routine basis is illegal, and only court-supervised access should be permitted.

Thus, Darbha & Arora's point above is not only a dichotomy, it is a pressing legal conflict. The people should be justly scared of any Central Bank that introduces mass financial surveillance over their privave transactions. And the people would have a valid cause to reject the project. To underscore the arbitrariness of the CB's acceptance of the AML agenda without question, these prescriptions from the FATF are on record as having delivered approximately zero benefit after 3 decades of trying, for massive costs to the people (Pol, 2020).[4]

Hence our first contradiction - the CBs want financial surveillance to stop bad people doing bad things. The people do not want financial surveillance, to stop bad people doing bad things to them.

Challenge 2 - Financial Inclusion

The next challenge taken on by Central Banks is **Financial Inclusion**, a euphemism that can be best expressed simply as the desire to ensure that all people have access to means ofpayment. Such access is provided naturally by paper and coin money. Beyond any particular

[4] Dr Pol suggests that the benefit is almost zero, in that it is measured at below 1% and above 0%. As a scientist I would suggest that (a) such a measurement is 'below the noise level' e.g. is approximately zero, and (b) considering the normal error bounds for such a measurement in social sciences, it is as likely to be below 0% as above 0%. That is, we need to investigate the hypothesis that AML causes ML, as much as we need to confirm the FATF hypothesis that AML reduces ML. That polemic noted, I suggest that 'approximately zero benefits' captures the quibble with brevity.

technology, payment is a human right: access to means of payment is a necessary consequence of people's right to be paid for work, and the merchant's right to be paid for their goods. The alternative is dark and stark - people who cannot be paid for their work are slaves, people who cannot pay for their food must rob to eat.

Financial Inclusion originally had a simpler, illusory meaning of access to bank accounts - this was a view championed by international organisations such as the World Bank, IMF, and the NGO charity or aid sector. Hence the arisal of an aphorism - let's bank the unbanked.

But, the term has always suffered. For one, it has become a favoured catch-word in contexts that make little sense. The international aid or NGO world has championed it for 3 decades since the work of Mohammad Yunus and Hernando de Sota, running trial after trial, without everseemingly tying financial inclusion to the actual problems on the ground. More recently, the Central Bank of Bahamas rolled out their 'sand dollar' for motives of financial inclusion in a context that does not suggest it is a big issue (data artist, 2020).

For another, the term is backwards, and it is better to think of Financial Exclusion than inclusion. What is excluding people? In the Global South, people do not have access to bank accounts for several good reasons: they were too expensive, banks were too untrustworthy, or accounts delivered no feature that people want or need. This might be a surprise, but consider that in Africa, the cost of running a bank account is about the same as in the west, around $5 per month, including in areas that boast monthly income around $60. In Africa, bank accounts are luxury items! These people are 'unbanked' in the same sense that people in Kibera don't buy Prada or Rolexes, but nobody talks about Rolexing the UnRolexed.

An observation. When I lived in my first non-Western country, I noticed that many of the houses were built with flat concrete roofs, but unfinished - they had rebar (metal spikes to reinforce concrete) and plastic water pipes sticking upwards to the next missing floor, awaiting further building.

It took me a while to find out why - a local explained that their banks are unsafe as they frequently collapse through insider theft and bad management. People had learnt over time to put their savings into building not into banks. Savers start out with land, and build up the supplies to work on each successive floor; this also explained the piles of concrete blocks and sand sitting beside unfinished houses for many years.

Since then, I've lived in and visited many nominally poor countries, and there's a clear correlation between people saving by building, and the weakness of the banking sector, which you can spot by walking around and looking at the rebar.

Banks in poor countries are also typically unsafe, as it is an easy scam for insiders (tellers) to raid fat accounts, and they collapse more frequently. Perhaps unsurprisingly, banks see someone on a low income as a poor account and loan risk. In summary, Financial Inclusion

might have been an enticing narrative in the West, but it just did not work, *implicitly*, for the economics.

But in the 21st century, two new contrasting developments emerged to change the approach to Financial Inclusion. Firstly, the invention and rapid deployment of *mPesa* in Kenya showed that banking and unbanking wasn't what it was about. Instead, a simple non-bank payment product from a mobile phone telecommunications company ("telco") did the trick, and as millions of micro-businesses could suddenly and safely pay remotely for goods, Kenya experienced what iswidely recognised as a financial miracle. This experience directly validates the Central Banks' desire to consider Financial Inclusion as a plausible goal, and to issue a separate money as digital cash to meet that goal.

Secondly, a new blockage emerged, as Financial Inclusion changed character with the introduction of deliberate and aggressive moves to exclude people. The global rollout of AML, accompanied by the motive of *suspicion*, created explicit financial exclusion as policy; it increased the expense of payments accounts, and made providers more untrustworthy as payments were blocked and reversed, and accounts were frozen or closed for arbitrary motivesdelivered by bank compliance personnel struggling to apply suspicion over sparse transaction data (or, by artificial intelligence engines badly trained to exclude at a much lower cost).

Central Banks will be unable or unlikely to improve reliability for inclusive payments with digital cash because they have already decided that AML is required, and it works very well to exclude in a digital system. CBs will not be able to assist in financial inclusion because they are on the side of financial exclusion. This is a shame, because the human rights aspect of giving people access to payments clearly trumps that of fighting an ineffective and unwinnable war against money laundering - a choice that, perhaps uniquely in the world, the Central Bank of Kenya (CBK) made correctly in supporting mPesa for all.

An anecdote. Back in Kenya in the early 2010s, we were talking to CBK about how our proposals for social savings were to work (Grigg 2021). Once they understood what we were trying to do, they were all smiles and they opened up with chatter and anecdotes.

Mpesa was the big thing in Kenya, so all conversations turned to this. One such story stuck with me: they shared with us their observations of how the big money was moving using mPesa. In essence what was happening was this - local merchants were loading up SIM cards to full capacity, which if I recall correctly was around $10k worth, more than an annual average salary, and they were trading the SIMs directly, *as if money*.

That is, in some big deal, a payer would hand over to his payee a plastic baggie of SIMs with the PIN number written on each. The payee would insert each in turn into their own phone, and check that Safaricom would recognise the SIM as being fully loaded to the limit of $10k. And in this way, the bag of cards was recognised for its entire value.

Now, at one level, it was a laugh to hear how limits were bypassed by the savvy street traders.

But far more important was how the CBK was dealing with it. They were watching! They weren't fussed about it in the slightest. They had intelligence! It struck me that these guys were wise; much wiser than that steady stream of idiot white visitors, called the Wazungu, from the various and many lettered international agencies such as FATF, IMF, WB, UN and so forth, those that came blind and cloth-eared, aiming only to promote their one-size-fits-all WEIRD prescriptions[5].

The CBK was conducting actual real risk analysis, a thing that the Wazungu did not have, because they could not see the wood for the trees.

How then did Kenya manage the miracle, when so many others failed? There were many factors but a few highlights include (Omwansa 2012):

- When mPesa was rolled out in 2007, the AML measures that cause financial exclusion were not as strong as they are today, and CBK was able to slow and dampen the impact of exclusionary measures until mPesa had achieved full reach across the economy.
- The issuer, Safaricom, was a non-bank, specifically a telco, and therefore had no conflict of interest with protecting its other payments, of which, more in the next section.
- mPesa was the first, and thus banks were taken by surprise.
- Once they woke up to the danger, CBK ran interference to stop the banks from destroying mPesa.
- The political system was aligned more with Safaricom than with the banks; the President's family was a big shareholder in the privatised national telco.

This is by way of recognising that these factors, critical for mPesa's success in bringing an entire country's worth of poor into digital payments, are hard to replicate. Choosing financial inclusion, or fighting financial exclusion, is in contradiction to the place that today's Central Banks find themselves in.

Challenge 3 - Zero impact on the banks

Next, **impact on the banks**. If the CB's digital cash works, people will hold balances in this digital unit; indeed one can suggest that the leading metric of success for the project will be howmuch balances the people hold, in comparison to other holdings, especially cash at bank and cash in pocket. In effect, any reduction of bank deposits and of cash holdings will be useful evidence of the success of the CBDC.

In classical digital cash thinking, CBDC is cash, and is for example uninsured and losable.[6] It would not be considered as equivalent to cash held in bank accounts, and thus would not count

[5] WEIRD stands for Western, Educated, Industrialised, Rich, Democratic - a comment on policies and practices invented for those countries but applied without thought to others, generally with bad outcomes. Wazungu translates roughly as aimless or blind wanderer.

[6] By "classical thinking" I mean the theory and practice developed in the 1990s, but note that some re-thinking is to be expected.

as *deposits* to banks. Indeed, we could suggest that if digital cash works as expected, people won't need bank accounts for much of their activity, as routine daily and monthly payments consume the vast majority of most people's balances. The retail individual banking customer will only want bank accounts for *credit* functions such as cards, overdrafts, mortgages, car leases, emergencies, and some savings if interest rates ever rise again. Perhaps that's it?

Yet, historically, banks have reacted aggressively to competition in payments (Dowd 1996). This aggression is in parts because (a) to banks, deposits are subsidised by government and industry structure, and are thus ultra-cheap and safe loans to the bank, (b) a base of depositors allows banks to upsell profitable credit and other services, (c) they earn fee revenue in payments flow, which has become a serious component under today's era of low interest rates, and (d) the rise of deep data processing in the digital pattern of payments.

At least for (a) above, the banking world has frequently granted itself a quasi-monopoly on payment instruments - because, their narrative says, without very strong protective barriers, banks would lose deposits and then be less able to issue the loans that drive the expansive sideof the economy. Whether we like banks or not, it is a fact that collecting all of the public's deposits *on demand* and turning them into loans to the public *at term* is a very important pillar ofthe operation of the economy. Some would even say that this function, called *term transformation*, is the very definition of banking, and the very reason why Central Banks are essential. Central Banks are of course very aware of this issue, and supportive of this power.

Then, for all of these reasons we can expect banks to fight aggressively against the CBDC. This is to be expected, even in the Global South where banking products are not competitive, simply because of the way banks think – in Kenya we knew a senior banking analyst whose unofficial mission was to kill mPesa, even as bank accounts were unsuitable for the larger population. Indeed, it was this reaction that killed the rollout of mPesa across wider Africa, as banks in other countries made mPesa impossible to roll out by hook or by crook. Banks are also behind the ongoing war against cash, as they see every cash transaction as a stolen opportunity. In a recent win, banks were able to scare people away from using cash in the recent COVID19 epidemic.

To address these concerns, the CBs are building compromises into the CBDC product.

One compromise is to outsource the customer-facing part of the business to the commercial banks. Initially, this was considered sensible because the Central Banks have no capability in retail operations, and, as rolling out a new customer-facing infrastructure would be a heavy lift, it's possibly wiser to use the available customer-facing resources and networks that already exist in the market. This then results in a two tier architecture where banks will own their portionof customers, to some extent alleviating the competition between CBDCs and deposit accounts.

One might reasonably critique this arrangement as suggesting that the CBs are not the right agents to get involved in a retail product, but the counter to that is that the network effects of a money are so strong that one single issuer is likely to dominate. One can also point to the

obvious flaw in the argument that banks are the right commercial customer-facing agents; telcos are actually a lot more adept at this because they already have the secure platform, theyalready deal in low levels of money, and the mPesa experience is proof that it works.

A second compromise is to lean more heavily on AML than is warranted. The unfortunate logic is that if banks employ hard AML on digital cash, they can reduce the effectiveness of digital cash, and thus preserve the rightful territory of payments to themselves. Indeed, we could reasonably ask if the motive of "protecting the banks" is a bigger factor than the more customary"financial integrity" excuse; we can certainly expect the banks to promote AML for their own mission of reducing competition. Which reveals a form of hubris: AML fails at effectiveness inits headline tasks (Pol, 2020), but hands to its employers a powerful weapon: *carte blanche* to discriminate against whosoever is not wanted.

And so the fundamental contradiction is revealed between the banks' competitive hatred of alternate payment systems, and the Central Banks' promise to do no harm to the banks. CBs would like to have their cake and eat it too, but the outcome of compromise is a simple weakening of the digital cash product, one that imperils the entire project.

Which reveals the paucity of the CB's mission thinking. What was it they were trying to do in the first place? What was the particular benefit that made CBs want to do this? If banks can so easily manage to corral the CBDC back into their custody, was the mission really that important?

Challenge 4 - Privacy

The above gives a brief description of three of the factors that make the CBDC an inordinately difficult goal, brief because of space, and only because we want to show something of the map where it impacts privacy.

Now turning to **privacy**. The ECB revealed that the #1 requirement of the users they surveyed was privacy (Arnold, 2021). That matches my experience - in past efforts, consumers may not have been vocal about this issue, but when they detected that privacy is inadequate, they quietly avoided the product. And especially, note that (a) early adopters are more privacy conscious than those who follow, (b) they have an outsized say in who follows, and (c) that anymoney is extremely dependent on network effects. Money needs mass adoption in order to be money.

Another anecdote. While I was doing a stint working on the über-private Chipper smart card money system of the late 1990s, in the Netherlands, a country known then for its obsessive approach to privacy, I happened to be at a party. With lots of drugs, which is normal in Amsterdam, not that I took the opportunity.

And at this party was a chap who was tagged as a local dealer of recreational product. Now, I'd long since learnt that if you want to do anything in the security world, you have to know both your customer and your customer's enemy. This sounded like an ideal chance to kill two birds with one stone, so I struck up a conversation about dealing, and we got around to talking about digital cash.

Over beers, he was very forthcoming and helpful on his trade, so I reciprocated and told him about this new form of super privacy money coming out. And I asked, "would you use this for your deals?" He said, absolutely not. He was unequivocal on this point.

Surprised, I asked why not, and he replied, words to effect, "it won't be private. No matter what they say or what people think, the government will ensure it won't be private." That put a new perspective on things for me, because, firstly I'd just spent some time telling him how private it was, and secondly, I knew the security team. They were good, strong, honest people. Dutch people, obsessed with privacy! They'd worked for 2 years on the security model, and *it was private*. Dammit!

Which left me thinking, a digital cash would surely gain a mark of privacy quality about it, if we could only get the dealers to use it. Or, any criminals, really. But I wasn't clear on how to sell this marketing proposal to anyone else...

Given the attention of early adopters within the *product adoption cycle*, it is critical, crucially critical to get privacy right up front, in order to create a positive climate for roll-out. And, by the by, we could probably measure the success of the privacy goal by checking how the bad guys perceive and use the system, as shown above with CBK.

This is just the dynamics of how payment systems work. In essence you can't fudge the privacy aspect, you can't leave it until later or lean on vague marketing words. It's got to be solid. Rock solid.

Diving Deep in Privacy

That turns out to be a pretty big challenge, as there will be sceptics. Let's dive deeper into this thing called privacy.

In the security world, we talk about threats – often using the phrase "what's your threat model?" ("WYTM?").

We can start that discussion by asking, *who* is the threat here? For privacy, there is a long list: thieves, neighbours, family, employees & employers, data miners, BigTech, police, tax, spooks, social security, random other government departments… Indeed, it is fairer to say that, by default, *everyone is a threat to your privacy*.

Therefore, in privacy engineering, we generally start from a principled position of "it's none of your business" and allow nobody to access a person's data. This is actually something that people work on, and that search has sparked such innovations as public key cryptography, the original eCash design of blinded signatures (of which there is a long and studied literature) and disappearing messages. Privacy engineering is a thing.

However, Central Banks are authorities, and authorities are not independent, rather they are beholden to many different interests. For example, one of their interests is having detailed data on what people are doing with money, for monetary policy and other reasons. Hence, CBs will not adopt the notion that "it's none of their business" because they believe that what you are doing with your money is indeed their business.

> *"Anonymised/aggregate data on the use of the digital euro should be available to the Eurosystem under any privacy option for statistical, research, supervisory and oversight purposes, including to fight fraud/illicit activities."* (ECB 2022)

Further, limitations on the privacy of money is not without precedent; even cash for example has technologies built in to breach the privacy of payments. A century or so ago, serial numbers were added onto notes following a rash of kidnapping cases in the USA, in which the kidnappers could cash out safely as the notes were really, actually untraceable. Adding serial numbers to all notes gave a way to trace where the ransom was being spent, and gave a lead toinvestigators.

If it happened to cash - the holiest of holies in the privacy world - then it will happen to digital cash. We've already stated that AML will be an article of faith in CBDCs, so we can assume that the starting point is that all digital cash will be traceable and identifiable as to the persons inany transactions. The ECB calls this its baseline position:

> *"Transparent to intermediary*
> *Checks during onboarding*
> *Data transparent to intermediary for AML/CFT purposes"* (ECB 2022)

The BIS has also put a heavy stake in the ground - not only will digital cash carry solid KYC, they are going to expand from there, solve the 'identity problem' and put all sorts of other personal data into the system (BIS 2021). Space does not permit us to examine this flight of fantasy (see for example Grigg 2021), but suffice to say that this is currently the BIS thinking, which we can assume is advice that all CBs will be comfortable adopting, even as they will find it difficult to implement in a free and democratic society.

Then, following from the above discussion, we can assume that the data will exist. The next question then is, who gets to enjoy it?

Who has access to the data?

Let's start with no-one. Not a soul. As a thought experiment, because some of us technologists know it can be done, and therefore it should be done! [7]

Unfortunately, the claim of *no-one* will be subject to a number of exceptions. Let's count them.

The Intelligence Community

The first exception is the spooks. The intelligence community (IC) are basically those who are sanctioned (permitted) to conduct crimes on behalf of the state. Spying, and other similar crimes such as stealing intellectual property and military secrets, kidnappings, regime changes, fraud, renditions, torture and assassinations, are allowed by the IC: they are "legal" when initiated within an initiating country against a target country, but are basically and obviously totally illegal inside every country they are done to. Indeed, being caught spying in somebody else's country is probably the most illegal thing that can be done, it gets a poorer reception than murder or robbing a bank - in war time, being caught spying on the battlefield gets you summaryexecution, which means death *without trial*.

One outcome of living in the IC is that people within it are very comfortable with breaking the law, and they only get slightly uncomfortable when it's done in their jurisdiction, to their own people, and then, only if they get caught. The spooks are masters of not getting caught! For them, laws might apply in principle, but need not apply in practice.

Which leads us to our first answer: the spooks will be given access to the entire database, because if not, ***they'll steal it***. Doesn't matter how they do it, and space does not permit us to dwell on this, but suffice to say it is 100% sure that they'll steal it.

Not that this is a serious consideration because it is also entirely sure that the IC will be in the room and will steer the technical design of any digital cash so that it's easy for them to access. How do we know? Because they are in the room for every other similar system; the IC is interested in wherever cryptography standards are being created or deployed at scale, such as mobile phones. Every major corporation that ships cryptography will do it with the IC's oversight, which means backdoors, and standards that use cryptography are nudged by the ICaway from our defensive mission and towards their offensive mission. It gets worse - now they have expanded their purview to wherever data is touched including data protection (EC 2021)

[7] Many technologists will rush forward and say that we can solve this problem of privacy with what we call exotic cryptography - blinded money, zero-knowledge proofs, ZK-SNARKs and the like. But, firstly, these things are not mainstream, and are scary for a reason. Until they've stood the test of time, and especially proven they can be simply treated as black boxes with solid characteristics, they are more likely to be too brittle to be trusted in the very important goal of protecting users' privacy against persistent attackers. Secondly, this misses the entire point ofthis discussion, which is about whether we choose private money, not how to build it. And thirdly, combining these two points, if some exotic cryptography is deployed, *because privacy*, how are we to tell whether it is real, or it is backdoored somehow?

and digital services (Fanta 2022). Every major system that tries to hide important data has somewhere some person who represents the needs of the IC.

It's just the way they work. You might not spot their influence, but that's only because they live in the shadows. Once you know the tricks of their trade, they can be spotted.

In conclusion, the spooks will have access. To everything. Supporters will rush to claim civil society, anti-terrorism, misinformation and so forth, but it's not our role today to judge their today excuses (a fascinating subject that it is). Let's just assume the spooks have it.

We have our first exception. Who's next?

The Police

How about the police? We could for example say that the police will have access if they get a particularised court order from a judge, pursuant to probable cause. This will be a strong protection as judges know what that means and won't grant an order without seeing some evidence.

This will work, but only for a time, because the spooks will eventually get sick of the crimes going on and will leak the information to the police. For example, in the USA, the NSA was caught sharing intelligence information on crimes with 19 different domestic agencies, and evengoing so far as to teach the police how to lie to the judge - by the creation of a false train of evidence to convince the judge that it was based on some other random source such as a tip- off, an insider or a lucky traffic stop.

They called it *parallel construction*, I call it perjury, obstruction of justice, contempt of court, conspiracy, deception and probably some more crimes thrown in. One can understand the frustration of the NSA and other spying agencies. They've often got the taps on all the criminal gangs, they hear who gets knocked off and who is about to get hit. Why not share it with the police?

The point here is to not judge their actions but to point to the power of human nature. The information will flow, if it is useful. For example, consider the various and many pandemic track & trace systems (Venkataramakrishnan 2021):

> *"In response to the coronavirus pandemic, the Singaporean government set up a contact tracing system reliant on a central database, allowing staff to rapidly locate and contact those who may have been exposed to coronavirus. Such a trade-off in personal privacy for the public good may have been deemed acceptable during a crisis, but a change in policy now allows the police to access this data."*

This process of human nature will happen with the people inside the CBs - the ones who have to manage the secret tracking for the spooks. They will eventually set up access to the police,

or if they show some moral spine, they will be replaced with people who are comfortable with doing it, which is called a *secret cell* in the trade.

That's our second exception. Perhaps we are comfortable with the police having some access? After all, we've nothing to hide because we've done nothing wrong.

The Banks

If the list of exceptions could be particularised and made strong, then this would be perhaps a credible commitment. But it cannot.

What about the banks? We already killed that one as the BIS has already stated that an individual can only have one CBDC account, so, as a consequence, each bank has to have access to all known CBDC accounts to at least find out if yours is already set up. And they'll find a way to encourage you to open up the transaction records so they can be more holistic intheir financial surveillance. But it's even easier than that.

Another anecdote. While (still) working on the über-private Chipper solution, I found a manager who was trying to whip his card out of the reader at exactly the right time to crash the protocol.

Let me explain: in a classical digital cash protocol on smart cards, 1990s style, each card would have a little spot inside it with a value for the money. My spot might have 100, yours 200. When I pay you, we now have to do a "dual database transaction", instantaneously, on both databases. As a fundamental of computer science, instantaneous between 2 different places never works, and nobody's built a quantum smart card yet, so it has to be serialised - one after the other.

If say, your spot increases by 50 to 250, and then mine decreases by 50, we have an interesting problem. My manager mate can whip his card out just after the first action, and then he's got 50 extra, and I've still got my 50! Woot! Free money… which in the trade was known as the *evergreen card*.

Or we could do it the other way around: decrease mine and only then increase yours afterwards. It's just a protocol choice, and this second way is generally how smart card money was done. But it still leaves the problem of what happens when you whip out your card at the precise wrong point, because now we - or I! - have the *lost money problem*.

Recalling that knowing your customers was critical to this business of security, I asked him why he wanted to lose his money. Because, he said, then he'd go up to the support office, and ask them to get it back!

My ears were buzzing at this point. This was a good question, and I was somewhat self-disgusted at not asking it myself. OK, *how are they going to get it back?*

"They'll look in *the database*, confirm it happened, then restart the transaction!"

I didn't hear the last part, because by now my ears had been blown off by the alarm bells. At this point I was very carefully going back in my mind to read the first part above, over and over again. "They'll look in the *database…*" What *database*?

And so the whole house of cards collapsed. Talking to everyone I was able to figure out what had happened.

1. The Central Bank of the Netherlands ("De Nederlandsche Bank" or DNB) had ordered the Chipper team to store all the transactions into a database so that in the event of a *meltdown* (another term of art, meaning that somehow, crooks found a way to really spank the system and make it completely compromised), then the damage could be debugged andrepaired.
2. The security team, and the whole company, were dead set on privacy, so the compromise was to keep the database entirely secret, and only 2 senior managers were trusted with special access.
3. Then the "lost money" problem turned up, and the 2 trusted people had to dive in, check the database, and proceed to recover the money.
4. Then, more lost money, and more and more… so the 2 special people handed access to the support team so they could deal with it more routinely.

And all of this happened while everyone (else) in the company still believed the system was private. Massive institutional cognitive dissonance!

And of course, I was now pondering my own beliefs, as the drug dealer had been right, and I'd been a muppet to believe the narrative.

Considering the above anecdote: you're happily doing your digital cash thing, and then a problem occurs. Doesn't matter what problem, as it's software, and problems always occur. So you pick up the phone to your local support agency, which is almost certainly your sponsoring bank (see Challenge 3 above) and ask for help.

You describe the problem… What is the bank going to do?

Of course, the bank must solve the problem, otherwise, happy customer becomes angry customer. Today, if anything, systems need more support because consumers have become more demanding, less tolerant and less willing to blame themselves. And, not to forget, it's *money*; whilst banks might be annoyed by a minor complaint, for the customers this is at minimum a red flag, and at maximum a loss of their earnings.

The banks will need to engage seriously on this, and of course, as their customer service agents, the banks will need to turn angry customers into happy customers. The help desk operator will need to see all your activity. Oops! The customer won't be able to just provide it on the spot, for various security and other reasons - the help desk operator will need an independent path of access so that they can discover what really happened, and choose the appropriate mitigation.[8]

And so we have our 3rd exception - the help desk will have access, else *no help*, no growth, and no success.

The Taxman

Let's move right along. Consider taxation. The tax department in your country will look at that treasure trove of payment information and quite fairly, in its humble opinion, decide it needs it. For example, the US Treasury recently proposed a rule that any recipient should report any annual aggregate inflows/outflows exceeding $600 of crypto directly to the IRS (Davison 2021).

As we the people will assume that the tax department doesn't have it, because *privacy*, then we will all use CBDC for all our dodgy deals. The tax department will of course hear about this, and appeal to the courts for a blanket order to get access, or to the parliament for a blanket law. It will probably be rejected, and that will be expected, so the taxman will try again. The more we the people are using it for private transactions, the more the money works, the more the tax department will want access. So they'll try again and again.

Eventually a sympathetic judge or parliament will let the taxman have it - and order whoever has the data to open it up.

This reveals a paradox of privacy - the more the privacy, the more we trust and use the money; yet the more the privacy, the more our trust, the greater the value of breaking it, and the more the tax department will fight to get it. Perversely, a corollary to the paradox is that once that privacy is broken, the more those who want privacy will flee to other methods; will those that are left with nothing to hide be enough to sustain the system?

It is without a doubt that eventually the tax department will have access. Once that happens, we now have civil authorities involved outside the initial core set of actors. Which means that any similar government department that has a plausible story can do so as well - this is the nature of precedents.

Pandemic? Sure, health authorities need to know who is buying banned drugs in pharmacies. Immigration? It is unfortunate that undocumented workers can access digital cash, but we can

[8] We can supercharge this example by considering a major robbery of digital cash from a major merchant. Happy merchant discovers that their day's takings have disappeared! Of course, the fast return of funds will be demanded, else, happy merchant becomes angry merchant, and they will turn off the terminals. Big oops!

track and trace them, and show how they're being paid for work they are not permitted to do. Dirtbag fathers skipping out on child support? We can't have that. Social security will need access because of the amount of benefits fraud.

Our 4th exception then is every "official" agency that has a good case to make. Which is a lot of them.

Your Enemies

And, once a half dozen or more "trusted" authorities get access, that means anyone can have access - for a fee. All private investigators will have their friends inside the authorities who for a little consideration will do searches. For example, if you end up in that unfortunate story known as divorce, any secret expenses you paid for with super private digital cash with your new dating partner might be presented in court. Oops!

Same for criminals, who are even more adept at acquiring special sources. Same for hackers who love the challenge of picking up entire databases of privacy information.

And there's our 5th exception: every enemy of yours who has a little money to bribe someone who has access to a support facility of some form. Enough enemies will have access to the Central Bank's private records that your CBDC will be only private from the ordinary, honest people.

What's the good of that?

Consequences

What are the outcomes from this cascading series of privacy breaches?

Everyone will know that the Central Bank's Digital Cash cannot be used for private things. And people will intend to not use it for private things. Which might ordinarily be OK as private things might only be 10% of our daily purchases.

Yet, it isn't that simple:

1. Nobody can predict what comes back to bite them in the future. That is, our private things might only be 10%, but we don't know which 10% they are. Hence, the desire fora blanket privacy commitment is strong and broad, rather than being particularised or narrow - I can't be attacked by you about something you don't know about; as Cardinal Richelieu said in the French Revolution, *"If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him."*
2. Out in the public space, there is already a lot of privacy scrutiny on the CBDCs. Already, outside the narrow insider space of CBs and partners, there has arisen broad and deep scepticism, which will only grow as weaknesses are scrutinised by researchers of

greater or lesser expertise. As the system gets closer to the public eye, it is to those adversarial opinions that the public will turn, rather than the marketing blather of CBs.

3. Early adopters are savvy, and privacy is something they typically know more about than the mass market. They will not be happy with something that clearly sets them up for problems in the future.
4. In contrast, because of network effects, CBDCs will be very dependent on mass adoption.
5. This system is dynamic rather than static. Whatever technology the CBs utilise, it will be tunable; it will come with many switches to flip and knobs to turn in both technical and governance terms. As new threats emerge in the minds of the noisy or political classes, such threats have to be stopped, right? This is the slippery slope that turned Paypal from a new libertarian money into a church cake-baking donation system.

In such an environment, a real risk - a clear and present danger - is that the people reject the CBDC.

Not vocally, not by marching on the Central Bank building and burning it down, but passively, by not adopting it. And if they don't adopt it, then neither will the merchants. And if the merchants don't adopt it, it fails - the iron rule of the double sided market is you need a guaranteed win on one side, and you also need a guaranteed win on the other side.

CBDCs are set up for a guaranteed Fail on both sides. As the Director General of GCHQ puts it, about China's DC/EP (Khalaf and Warrell, 2021):

> *"If wrongly implemented, it gives a hostile state the ability to surveil transactions," [Sir Jeremy Fleming] said. "It gives them the ability . . . to be able to exercise control over what is conducted on those digital currencies."*

Obviously, once they have breached privacy, the CBs are in the driver's seat to exercise control over actions - freezing, blocking, closing, seizing - which outcomes also follow naturally from AML. Fleming is talking about China because that's how China stated it will be done, but he could equally well be talking about any country's digital cash, as Western CBs may not be able to do it any other way.

Which is to suggest that the two most likely outcomes are, (i) a mass financial surveillance system, which has been forced on society, or (ii) the users will reject the system.

The users' goal of privacy is not some polite nicety, not just another feature in a list. Privacy is fundamental to our society, our ways and our life. Our evolution through history is based on privacy of money, and it is only in the last 50 years that digital transactions have offered a way to breach. Privacy of money is not a dial to fiddle with because of policy, it is rather part of our very economy and society.

In order to overcome this barrier, I propose that Central Bankers are going to need *a credible commitment to privacy*.

Central banks will need to *commit* because if it isn't a cast-iron promise, CBs will back out. Such a commitment will need to be *credible* because the public is already sceptical and alreadycritical, and simply won't believe words like "we're more friendly to privacy than Facebook." Users will expect CBs to back out, and will walk away before they give CBs the chance.

"Don't give me problems, give me solutions!"

I do not in this paper aim to provide a full solution. Instead, I fall short of "the solution," at the point of just laying out the difficulties, because I do not believe Central Banks have understood what they are heading into. It is my hope that CBs will take on the issue of privacy more seriously than they so far have, if they understand how severely failure of privacy imperils theirproject – privacy isn't a feature, it's a fundamental right. The users know it and demand it, and woe betide any society that walks blindly into a transparent world.

Having said that – "Don't bring me problems, give me solutions!" rings in my ears. Some discussion of potential solutions could assist. One strategy I propose is:

a) Give the spooks access (they'll steal it anyway).
b) Make digital cash through a 2nd tier bank count as *deposits*. That is, if a bank introduces a customer to digital cash, through a tied app, then digital cash inside that app or wallet, owned by the customer, counts as deposits for the purposes of the bank'sbalance sheet and lending equations.
c) Declare access by anyone (other than bona fide national security business, i.e. the spooks) subject to a strict court barrier: particularised and probable cause. No fishing expeditions, no speculative requests, no tricky contracts that conveniently slip in permission in the fine print.
d) Make all other access a criminal offence with mandatory jail time. Strict liability.

This won't stop the most egregious offences, but it will give pause to the thousands of police, bureaucrats, tellers and supporting personnel who might otherwise desire a look, because reasons, because they're the good guys. Selling off access or pushing for loopholes can rebound and jail time is a strong incentive. Find another way.

This solution has drawbacks.

- It is only a partial solution, as we cannot solve the support problem this way. That's unfortunate because support is a big issue, including being critical to adoption. And I'd say, if we can only support the product by opening up a privacy loophole then that may be too high a price to pay. More thinking is required here.
- Central banks have already handed over their independence mandate to the AML compliance juggernaut, and stopping CBs from sharing the data won't be easy. Could there be another exception? Easily, but every exception opens up the privacy to

criminals and others - compliance departments are big and full of bureaucrats trying to make monthly rent (AML *as* corruption is another fascinating topic, no time today).

- It is also going to be an unpopular solution in the political world, as dozens of agencies in each country are already thinking about the potential bounty of all that data. To backtrack on that is going to spark the fiercest pushback from the powers that be, the insiders. But note the paradox of privacy, that bounty is only worth something if the users think it safe from spying, which incentivises all those agencies to breach it.
- Central Bank employees will be surprised that working with statistical data exposes them to strict liability if that data can be de-anonymised, but that's a surprise we the people need them to have. Indeed, nobody in government agencies with access will want (d) above, being mandatory jail time with strict liability. Fair enough, one might say, we didn't expect our bureaucrats to take on liability like that. Or did we? If we the people are to hand over *our very financial lives* to a host of inscrutable and unpunishable agencies, isn't liability, and strong liability, a fair price to ask? Because we the people are going to be facing liabilities if and when our data gets shared, and no government agency will pay the tab for their mistakes. It will all be on us, the unprotected users. If there isn't a balance of liabilities, just why would we do it?

Another approach is proposed in the ECASH bill being prepared for US Congress (Lynch 2022). For privacy, its draft wording requires that it be:

> *"(9) classified and regulated in a manner similar to physical currency for the purposes of anti-money laundering, know-your-customer, counter-terrorism, and transaction reporting laws, and thus not subject to third-party exemptions to a reasonable expectation of privacy;"*

This proposal accepts that the name of each person holding a payment card is known to the authorities, but the transactions between payment cards are treated the same as cash - presumably untraceable. Technically, this proposal expects that a card can do the balance transfer to another card, without each card recording the owner of the other. While providing privacy on paper, we can note that (a) it is only a proposal, and it will have to fight the dozens of agencies who will lobby in Congress committees for their special needs; (b) due to the overall complexity and opacity of a digital cash system, the users will still have difficulty knowing that it is indeed private, and there is no backdoor or bait & switch lurking under the plastic; (c) there is no answer to the meltdown and support issues; and (d) it breaches the Travel Rule which is already in place.

In conclusion, in launching this adventurous mission to deliver private digital cash, Central Banks have truly placed themselves on the horns of a dilemma. How much privacy is needed? A little or a lot? This is an undecidable problem, but if Central Banks don't take on the side of users in this mission, they imperil the project. Central Banks need *a credible commitment to privacy* to bring on the users. Get privacy wrong, and they will set back the field for a decade.

I'm happy to be proven wrong.

References

Martin Arnold, “Europeans raise privacy concerns over digital currency” Financial Times 14th April 2021.
Also see European Central Bank (ECB), “ECB digital euro consultation ends with record level of public feedback” ECB Press release, 13 Jan 2021
https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210113~ec9929f446.en.html

Bank of International Settlements (BIS), “III. CBDCs: an opportunity for the monetary system,” *BIS Annual Economic Report*, BIS 23 June 2021

David Chaum, "Achieving Electronic Privacy," Scientific American, August 1992, p. 96-101
Also see David Chaum. "Blind signatures for untraceable payments". *Advances in Cryptology Proceedings of Crypto 82*. 1983

(Wikipedia) “Chipknip,” accessed 24 Oct 2021
https://en.wikipedia.org/wiki/Chipknip

Sriram Darbha, Rakesh Arora, *“Privacy in CBDC technology”* 2020, Bank of Canada
https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/

The Data Artist, “How many Cbankers does it take to do meaningful CBDC research in the Bahamas?” The Blind Spot 2022
https://the-blindspot.com/how-many-cbankers-does-it-take-to-do-meaningful-cbdc-research-in-the-bahamas/

Laura Davison, “Treasury Rips ‘Misinformation’ on Tax Plan’s Bank-Data Provision”, 14th October 2021
https://www.bloomberg.com/news/articles/2021-10-14/treasury-blasts-misinformation-on-tax-plan-that-faces-hurdles

Kevin Dowd, *Laissez Faire Banking*, Routledge 1996 ISBN 0415137322.
see Chapter 1 “The Evolution of a Free Banking System”
https://iang.org/free_banking/dowd_lfb_intro.html

European Central Bank (ECB), “Digital privacy options,” 2022
https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs220404.en.pdf

European Commission, “Data Protection: Commission sends a reasoned opinion to BELGIUM for lack of independence of its Data Protection Authority,” in *October infringements package: key decisions*, 12th November 2021

Alexander Fanta, “NATO center wants to be allowed to do research with Facebook data,” Netzpolitik.org, 27th January 2022 (in German).

Ian Grigg, “Financial Cryptography in 7 layers,” Financial Cryptography 2000
https://iang.org/papers/fc7.html

Ian Grigg, *Identity Cycle*, 2021
https://iang.org/identity_cycle/

David Indeje, “Kenya’s Treasury to Revise Upwards Reporting on Large Cash Transactions,” 2021 Khusoko
https://khusoko.com/2021/10/20/kenyas-treasury-to-revise-upwards-reporting-on-large-cash-transactions/

Juma, “Court Allows KRA To Access Your M-Pesa Records And Phone Data”, SokoDirectory 2020
https://sokodirectory.com/2020/02/court-allows-kra-to-access-your-m-pesa-records-and-phone-data/

Izabella Kaminska, “Is the central bank panic about the PBOC coin justified?,” Financial Times, 19th April 2021
https://amp.ft.com/content/76e450be-e8b3-40f3-a452-b20284e0bd63

Roula Khalaf and Helen Warrell, “UK spy chief raises fears over China’s digital renminbi,” Financial Times, 10th December 2021

Rep. Stephen Lynch (MA-08), Chair of the House Committee on Financial Services' Task Force on Financial Technology, “H.R. 7231 - The Electronic Currency and Secure Hardware (ECASH) Act,” 28th March 2022
https://ecashact.us/
https://lynch.house.gov/_cache/files/1/7/17e47e5a-2bff-42c1-b509-eb8a50931fa6/BDDFF183213326821B5C88B7F326EABB.ecashact-lynch.pdf

(Wikipedia) “Mondex,” accessed 24 Oct 2021
https://en.wikipedia.org/wiki/Mondex

Tonny Omwansa, *Money, Real Quick*, Balloon View Ltd 2012 ISBN 101907798455

Ronald F. Pol (2020), “Anti-money laundering: The world's least effective policy experiment? Together, we can fix it, Policy Design and Practice,” DOI: 10.1080/25741292.2020.1725366
https://doi.org/10.1080/25741292.2020.1725366

Siddharth Venkataramakrishnan, “Online privacy: a fraught philosophical debate,” Financial Times