On the nature and security of expiring digital cash*

Frank Stajano[0000−0001−9186−6798], Ferdinando Samaria[0009−0001−2045−6190], and Shuqi Zi[0000−0002−0692−6192]

University of Cambridge (United Kingdom)

Abstract. Digital cash is coming, and it could be programmed to behave in novel ways. In 2020, the People's Bank of China ran an experiment during which they distributed free digital cash to 50,000 citizens. But with a twist: they programmed that digital cash to *expire* if not spent within a few days. This fascinating and somewhat paradoxical experiment opens many questions. If the cash expires, why would anyone accept it as payment? If it is intended to expire, can the recipient find ways to make it not expire? We explore a variety of possible attacks on expiring cash, countermeasures to those attacks, and alternative implementations, one based on CBDC and another on a public blockchain. We also discuss the more philosophical question of whether expiring cash is still cash: we argue it cannot be.

Keywords: digital cash · expiring cash · programmable cash · CBDC · cryptocurrency

1 Introduction

It is an easy prediction that physical cash will at some point become digital. Decentralised cryptocurrencies like Bitcoin [26] and Ethereum [8] are mentioned daily in the mainstream press; at the same time all of the world's major economies, not to be outdone, are experimenting with, or at least seriously considering, CBDCs (Central Bank Digital Currencies)[18,17,4,3,1]. Meanwhile, the stealthily emerging rivals of CBDCs are the stablecoins [13] (cryptocurrencies pegged to established traditional currencies like the USD[1]), on which DeFi (Decentralised Finance) traders rely in order to manage liquidity, while escaping both the volatility of untethered cryptocurrencies and the centralised control of CBDCs.

To avoid terminological misunderstanding let us explicitly point out the obvious: what we refer to as digital cash goes well beyond digital payment

* Authors' preprint. Presented at WEIS 2025 (Workshop on Economics of Information Security, Tokyo, Japan).
Revision 47 of 2025-05-19 15:54:35 +0100 (Mon, 19 May 2025).

[1] At the time of writing, the largest cryptocurrency stablecoin is Tether, with a market capitalisation of 140 billion USD.

mechanisms such as online payments, online bank transfers or contactless credit cards, which are already largely ubiquitous. The first key distinguisher is that digital cash *can be transferred directly* between individuals, without the intermediation of a bank and without one of the two parties having to be a merchant. The second important distinguisher is that (at least some incarnations of) digital cash *can be programmed* to perform arbitrary actions, realising the "smart contracts" vision originally put forward by Szabo [31].

As a specific example of programmability, a pioneering experiment was carried out at scale by the People's Bank of China (cfr. Section 4.1) whereby digital cash was distributed to citizens of Shenzhen but programmed to expire if not spent by a certain date [6,7].

In this position paper we explore some of the paradoxes and security problems implicit in the idea of "expiring digital cash". Can it still be considered cash if it expires? What attacks are possible? Can they be guarded against?

The contributions of this work are as follows.

- We list the conflicting requirements and security constraints for expiring digital cash from the viewpoint of the various stakeholders (Section 3).
- We describe the Shenzhen experiment; then, as a thought experiment, we generalise to other possible implementations of expiring digital cash and we investigate possible attacks and countermeasures (Section 4).
- We discuss whether expiring digital cash should still be considered cash and ultimately argue that it can't (Section 5).

2 What do we actually mean by money?

In the words of leading money sociologist Nigel Dodd [14],

> money is an extraordinarily powerful idea.

Yet a precise definition of money is not easy to find. The concept of money is commonly accepted by economic historians as the agreed-upon medium of exchange that resolved the issue of "want of coincidence" in the barter economy, as described in Jevons's classic work [22]: barter works if you can find a supplier of what you want, willing to take what you have in exchange for it. Money comes along to provide a solution to this problem and to offer a more flexible instrument to facilitate exchange and, more generally, commerce. Since not all trade will be simultaneous (which it would have to be in the case of barter), parties who use money will naturally want it to preserve its value over time. Then, to work out if all these asynchronous exchanges are working well or not, participants will sum and subtract amounts as they trade, counting profit or loss in units of money.

In other words, as summarised by a recent report by the US Federal Reserve [18], money has three key functions, namely those of providing a:

- medium of exchange;
- store of value, and

– unit of account.

Starting from Menger's foundational work [25], various properties of money have been proposed as necessary, including for example durability (resistance to repeated use) and portability (ease of transport). But, while important for cash intended as physical money, in the context of *digital* cash these properties can be taken for granted. Other characteristics then emerge, like the following, identified in a report by the European Central Bank [16]:

– secure and resistant to cyber-attacks;
– maintainable, because programmed using best-practice software design principles;
– supportive of end-user privacy;
– interoperable with other digital ecosystems; and
– sustainable, in the sense of not requiring large amounts of energy to be processed.

Since the 1980s, starting with Chaum's pioneering inventions including mix networks [12], blind signatures [9] and multiple-spending detection [11], various attempts have been made at providing some form of non-physical cash that could be transferred digitally while retaining some of the key properties of cash, such as anonymity, divisibility and unforgeability. But it is only with the emergence of Bitcoin [26] that digital cash reached the mainstream, with Central Bank Digital Currencies playing catch-up.

Cash is a form of money, such as coins or banknotes, generally issued locally by a central authority and commonly used for trade within a given geopolitical realm. The most common example are the central bank coins and banknotes that we all use. They are a form of fiat money created by government decree and not backed by real assets—as opposed to money backed by gold, rare nowadays but commonplace in several major economies during the first part of the Twentieth Century[2].

The terms "money", "cash" and "currency" are often used interchangeably in casual speech. Although it is difficult to find authoritative and universally accepted definitions for these terms, "money" is the most general term, encompassing both of the others. It refers, as we said, to any entity used as medium of exchange, unit of account and store of value[3]. The terms "currency" and "cash", instead, denote money issued by a central bank: both terms refer to the physical coins and banknotes, while only "currency" is used to refer to the specific flavour of money issued by a particular central bank (e.g. USD vs EUR vs CNY). As for non-physical forms of the money issued by a central bank, such as bank account balances, things get murky: bankers tend to consider them

[2] Following the Great Depression of 1929, the UK abandoned the gold standard in 1931. The US did so in 1971.

[3] Note how, under such a definition, privately-issued tokens such as air miles might be counted as money.

currency (it's still USD or EUR or CNY in the account, after all), but not cash; while, confusingly, accountants tend to consider them cash, but not currency.

We won't participate in this terminological debate. For the purpose of this paper we will refer to both decentralised cryptocurrencies and centralised CBDCs as *digital cash*. The main distinguisher between the digital cash we talk about and the (already widespread, pre-CBDC, yet digitally transferrable) money held in accounts at retail banks is, to us, that digital cash can be transferred between end-users without involving a third party[4] in the transaction. As noted by the European Central Bank [16], this can be implemented

> in two ways: either via distributed ledger technology (DLT) protocols or by means of local storage (e.g. using prepaid cards and mobile phone functionality, including in offline payments). [...] this solution presents challenges with regard to compliance with AML/CFT[5] rules.

As we mentioned in the introduction, digital cash might also be programmable: e-coins that get paid automatically to a designated beneficiary when certain conditions are met. This feature is a formidable addition, because a programmable digital currency can alter its state (in terms, for example, of its persistence or wallet location) conditionally on specific events. The immediate consequence of this is that, unlike its non-programmable relative which is entirely passive, a programmable digital currency is sentient and reacts to its environment.

3 Requirements engineering: what's hard about expiring digital cash?

In this section we describe the problem of expiring digital cash. Who might want digital cash? Why is it hard to implement, and why is it interesting? What are its inherent and seemingly paradoxical contradictions? What properties does expiring digital cash need to have, in order to prevent fraud and unintended behaviour?

First of all: why? A plausible motivation for implementing expiry mechanisms in digital cash, from the viewpoint of a central bank, is to support specific macroeconomic or social policy objectives such as stimulating short-term consumption and preventing hoarding of distributed aid. In 1958, Silvio Gesell [20] proposed a model for market socialism in which money depreciated over time in order to discourage hoarding and stimulate economic activity. In 1969, future Nobel laureate Milton Friedman [19] suggested "helicopter money", a kind of monetary stimulus in which the nation's money supply is increased by directly financing tax cuts or public expenditure (as if free money were dropped

[4] Such as, indeed, a retail bank, a credit card company, the FAANG Internet giant that owns the payment infrastructure that supports your smart phone or smart watch, or any other intermediary.

[5] Anti Money Laundering / Combating the Financing of Terrorism.

from a helicopter) rather than by the central bank buying government bonds. If we were to give Friedman's helicopter money an expiration date, recipients would not be able to hoard it. Indeed, as reported by Kan, Peng and Wang [24], in 2009 a fiscal stimulus program in Taiwan distributed 2.57 billion USD in the form of expiring shopping vouchers—and the use of vouchers as opposed to plain cash introduced the additional constraint of limiting what the aid money could be spent on.

For the 2020 Shenzhen digital yuan pilot described in Section 4.1, the People's Bank of China (PBC) [27] stated that one of the objectives was to "meet the demand for retail payment services in the digital economy" and to "improve the efficiency of the currency and payment system". The PBC's white paper [1] explains that the e-CNY is intended to "carry out pilot programs in a steady, safe, and orderly manner". In other words, one of the reasons for putting an expiration date on the digital cash used in that particular experiment was to *limit the duration of that early live trial* of the e-CNY CBDC. However, another official press release [30] also said that the trial was intended to stimulate consumption and boost domestic demand during the COVID-19 recovery period—thus it was also intended as a small-scale stimulus.

In 2024, Kahn, van Oordt and Zhu [23] proposed a different motivation for expiring digital cash—namely, expiration as a robustness feature for *offline* CBDCs. In such a context, in order to prevent double-spending without the recipient being able to go online to check whether a digital coin is still valid, the value must be stored entirely in a tamper-resistant and trustworthy[6] physical wallet rather than in some external database. But then no backup is possible: if the owner loses the wallet, she loses all the money as well. In the proposal by Kahn et al, however, if the CBDC stored in the wallet has an expiration date, then, if the wallet is lost[7], its owner might eventually ask the central bank to reissue the missing CBDC, which is considerably better than what happens today when losing a wallet full of banknotes.

Why is expiring cash difficult to implement? The defining feature of expiring digital cash is that it gives its holder Alice some purchasing power until some announced expiration date, after which this purchasing power abruptly disappears. This clearly gives Alice an incentive to exercise that purchasing power while it is still available, but at the same time transfers the problem to Bob, the party who would receive the expiring cash. Presumably, in exchange for the cash, Bob is offering Alice a product or service of some value. There are at least two mutually exclusive cases, examined next, each with its own problem.

[6] Trustworthy in the sense that the payee must trust the tamper resistance of the wallet of the payer. The tamper resistance of the payer's wallet protects the payee, not the payer! If the payer can hack her own wallet and double-spend, it is the payee who loses out.

[7] And assuming the wallet was merely lost rather than stolen; or that, if stolen, the thief was not able to unlock it. In other words, assuming that the CBDC in the wallet will eventually expire without having been spent.

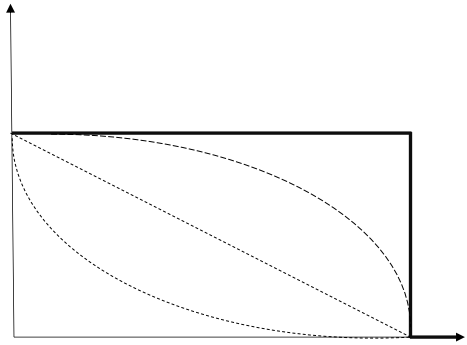

Fig. 1. Time value of expiring cash. The horizontal axis is time and the vertical axis is value. The bold line is the nominal value, while the dashed lines are the actual value when the expiring cash is traded openly in the market, according to linear, time-convex and time-concave models. (It would be interesting to conduct experiments to ascertain the shape of the discount curve that holders of expiring cash would actually use as time approaches the expiration date.)

Case 1: digital cash that remains expiring when paid If the cash retains its expiration date when Alice pays it to Bob, why would Bob accept the expiring cash as payment in the first place?

Note that, even though in theory the expiring cash retains its full nominal value until the expiration date and then abruptly drops to zero (bold line in Figure 1), in a free market we expect that its actual exchange value would gradually diminish as the expiration date draws closer: the shorter the remaining lifetime, the lower the value (dashed lines). Assuming that different coins might expire on different dates (unlike in the Shenzhen experiment of Section 4.1), this would negate the fungibility of cash and lead to adverse selection problems in payments, as explored by Abramova et al [2] in the context of transactions involving cryptocurrency coins blacklisted for having been traced back to the proceeds of criminal activities.

Given that, why would Bob not insist on being paid in regular non-expiring cash, which (as Figure 1 illustrates) is strictly more valuable?

Case 2: digital cash that stops expiring when paid If the digital cash no longer expires after it has been paid once to another party, what is to stop Alice from paying it to Bob in a temporary fake transaction that the two of them immediately undo with a complementary one in which Bob pays back the same amount to Alice in non-expiring digital cash? This loophole would straightforwardly defeat the expiration mechanism[8].

[8] Bob could of course charge Alice a modest "unlocking fee" for the service of converting Alice's digital cash from expiring to non-expiring, but this does not change the substance of the argument. In any case this is a riskless operation for Bob, if Alice's digital cash becomes non-expiring once Bob receives it.

These two cases do not, strictly speaking, exhaust the possible options[9] but they suffice to illustrate that an important design decision must be taken on the matter of transferability of expiration and that neither of these two mutually exclusive approaches is trouble-free.
We identify the following stakeholders, with their respective interests.

The issuer This is the institution (central bank?) that creates the digital cash and programs it to be expiring. Whatever motives the issuer might have for wanting the cash to expire[10], a primary goal of the issuer must be to ensure that the expiration mechanism cannot be circumvented by other parties. In the rest of this paper we assume that the issuer's motive for introducing expiring cash is specifically to support a monetary policy of encouraging consumer spending in a recession and, consequently, of discouraging hoarding of stimulus funds.

The original recipient This is Alice in the above scenario, the party who first receives the expiring digital cash. Alice's motive is to gain the maximum benefit from this unexpected windfall. While in some cases (e.g. relief for victims of natural disaster) Alice might indeed need to spend it all immediately on essential necessities, in other circumstances she might see greater benefit in saving it for an even rainier day instead of spending it all before the expiration date. Thus, whenever Alice's goal is to preserve the purchasing power of the received digital cash for as long as possible, her goal is in direct contrast to that of the issuer, creating an adversarial relationship between them.

The secondary recipient This is Bob, the party from whom Alice might like to buy goods or services by paying for them in expiring digital cash. Bob has not received the direct benefit of a windfall. He must assess whether it is worth his while to trade his goods or services in exchange for expiring digital cash, whereas normally he would receive non-expiring digital cash in exchange for them[11]. The context might be that perhaps, in those disastrous circumstances that required the aid or stimulus, there is nobody around with

[9] One might in theory conceive yet other cases: for example, changing the expiration date every time the cash changes hands, such that every new recipient gets a fresh new period of validity. But the vulnerabilities introduced by this case are very similar to those of Case 2 and thus not worth treating separately; moreover, we cannot imagine a practical monetary policy goal that would require adoption of this case. For brevity, we shall not further discuss this or other additional cases in this paper.

[10] Whether to support a Gesellian monetary policy of forcing recipients to spend rather than save the stimulus money, as done in the Taiwan initiative; or whether to time-limit a live test, as done in the Shenzhen experiment alongside the stimulus motive; or whether to allow refunds for lost digital cash, as per the Kahn et al proposal; or for any other reason.

[11] As we said above, the non-expiring version of the cash is always worth at least as much, and strictly more in free-market conditions where the expiring cash can be traded—although in Case 2 no trading is technically possible if the expiring cash ceases to expire after the first trade. But we are nitpicking.

enough non-expiring cash to buy the goods at their full price[12], and that it is therefore better for Bob to be paid in expiring digital cash than not to be paid at all. However he too, like Alice and everyone else, would much rather receive the same nominal amount in unfettered non-expiring digital cash, if given the choice. If, as in Case 2, the issuer guarantees to take back Bob's expiring digital cash and exchange it for regular digital cash, then Bob will have no objections to this scheme. However, absent this guarantee, as in Case 1, he will have an incentive either to refuse the expiring digital cash altogether or to cheat the system (possibly, but not necessarily, in cahoots with Alice) and therefore his goal, too, will be in conflict with that of the issuer.

4 Implementations, attacks and countermeasures

We open this section by describing the Shenzhen experiment that motivated our enquiry into expiring digital cash. Extrapolating from that context, and with reference to a hypothetical setting in which the issuer creates expiring digital cash for the purpose of dispensing stimulus money along the lines of a Gesellian monetary policy, we then brainstorm a variety of possible attacks and countermeasures (see summary in Table 1), without pretence of exhaustiveness, and keeping an open mind about the fact that expiring digital cash might also be implemented in other ways than through a CBDC, such as through a decentralised blockchain.

Faking sales	4.2	Attack: fake transactions
	4.3	Attack: fake refunds
Buying forbidden items	4.4	Attack: laundering through payment platform
	4.5	Attack: buying assets as long-term store-of-value
Simulating merchant status	4.6	Attack: registering as a merchant
	4.7	Attack: faking the merchant flag
Yield farming	4.8	Attack: collateral for loan
	4.9	Attack: wrapped token

Table 1. Categorisation of the attack types we considered

4.1 Implementation: the CBDC-based Shenzhen experiment

In 2020, the People's Bank of China (PBC) conducted a trial in Shenzhen's Luohu District in which expiring digital cash was distributed to a subset of the

[12] Indeed this might be the very reason why the issuer offered helicopter money to citizens in that region, such as Alice—to stimulate an otherwise stagnant trade.

residents through a lottery. The event was called "Enjoy Gift Luohu Digital RMB Red Envelope" [28]. The "red envelope" is a traditional Chinese gift, often containing cash, given during special occasions such as Lunar New Year, weddings, or festivals as a gesture of good luck.

The expiring e-CNY distributed in the Shenzhen trial only had validity for less than a week, from 18:00 on 12 October 2020 to 24:00 on 18 October 2020. The digital cash could only be spent at one of 3,389 designated merchants in Luohu District that had completed the digital e-CNY system transformation. The holder of the digital cash was not allowed to transfer it to other individuals. 200 CNY ($\approx$ 30 USD at the time) was distributed to each of 50,000 individuals, for a total of 10,000,000 CNY ($\approx$ 1.5 million USD).

According to an official statement [30], the trial was intended to stimulate consumption and boost domestic demand during the COVID-19 recovery period, but was also a routine test in the development of the digital e-CNY.

The stated usage restrictions meant that Alice could only pay a merchant, not another individual. Arguably this made the handed-out cash more like a coupon or voucher[13] than actual cash that may be spent anywhere. Alice was explicitly prohibited to use this so-called cash to settle a debt with her non-merchant friend Charlie. And, even if Charlie had been willing to accept it nonetheless, he would have ended up being encumbered with expiring digital cash himself—which, as we observed in Section 3 assuming Case 1, would have been worth less to him than the same nominal amount of regular non-expiring digital cash.

We observe in passing that the Shenzhen experiment used Case 2 (in which the issuer guarantees that the designated merchants may exchange the expiring cash they receive from buyers against conventional non-expiring cash). This is therefore the case we assume by default in the hypothetical attacks that we describe in the following sections, unless we explicitly specify otherwise.

4.2 Attack: fake transactions

As we noted when we introduced Case 2 in Section 3 on page 5, whenever the digital cash no longer expires after it is acquired by the secondary recipient, an obvious attack becomes possible: the secondary recipient Bob could complicitly convert the digital cash of the original recipient Alice from expiring to non-expiring and return it to her, while charging an unlocking fee. Several variations are possible on this general pattern, as seen in this Section and in Sections 4.3 and 4.4.

Alice pretends to buy an item from Bob. On payment, the expiring cash received by Bob becomes non-expiring. Bob returns it (minus an unlocking fee) to Alice. She does not collect the item, which might not even exist: the whole transaction could be totally fake so long as Bob, owing to his status as merchant, is able to redeem the expiring digital cash from the issuer in exchange for regular digital cash.

[13] As in the already-cited much larger Taiwan fiscal stimulus program of 2009 [24].

The victim, in this attack, is the issuer, whose intended monetary policy is violated when Alice and Bob break the expiration mechanism. If the issuer can trace all financial transactions[14], it may be able to detect the attack by spotting the pattern whereby Alice pays Bob and then Bob pays back Alice (almost) the same amount. However, Bob might pay back Alice using a less traceable channel (e.g. physical cash), making detection harder.

The issuer might also demand to see the receipt for the goods that Alice claims to have bought from Bob, and the physical goods matching that receipt, or proof that they have been destroyed. Such a check would be onerous for the issuer; to scale it to the whole population while limiting costs, the issuer might adopt a sampling approach, using Wheeler's strategy [32], by making the penalty for violating the rules sufficiently high as to make it not worth for Alice and Bob to attempt the attack even though their probability of being subjected to a spot check is low.

4.3 Attack: fake refunds

In this variant of the attack of Section 4.2, Alice purchases an actual product (say a TV set) from Bob with expiring digital cash, and Bob processes this sale as normal. After the expiration of the cash, Alice returns the item. Bob restocks the item and refunds Alice in non-expiring digital cash or in non-expiring store credits[15]. Compared to the attack of Section 4.2, this one has the advantage of offering Bob some plausible deniability: the refund is a normal business practice and Bob was not able to refund Alice using the same payment medium she used (as is customary to protect the merchant from frauds by the purchaser) because her cash had expired; so Bob has the perfect cover story for refunding Alice in non-expiring cash.

As before, this attack only works in Case 2, because it relies on Bob's ability to return the expiring digital cash to the issuer (thanks to his status as merchant) in exchange for regular digital cash.

Again, the victim in this attack is the issuer, since Alice and Bob cooperate to defeat the expiration mechanism.

The fact that Bob covers his tracks with a plausible cover story makes detection of this attack slightly harder for the issuer, even if it is able to observe money flows. However, to counter this attack, the issuer might apply anomaly detection: if the issuer monitored the ratio between returns and sales for each merchant, fraudulent merchants would stand out if they engaged in this attack at scale.

One might think that another possible countermeasure from the issuer might be to force the merchant to refund the item with expiring digital cash. But what

[14] Not inconceivable if we are talking of a CBDC and the issuer, who controls it, leans more towards traceability than towards privacy.

[15] The former case is more advantageous to Alice, because the refund is fully fungible and she can spend it anywhere rather than just at Bob's. In recognition of that, Bob might reduce or waive his restocking fee (effectively an unlocking fee) in the latter case.

would be the expiration date of the refund? If it is the same as that of the cash used for the original payment, Alice's workaround is to ask for a refund after the original digital cash has expired (assuming that the warranty on the TV lasts longer than the expiring cash with which she purchased it). If instead the refund grants Alice additional time to spend the returned cash[16], she has thus managed to extend the duration of her original expiring cash, so this is still an attack, even though its power is now reduced.

4.4 Attack: laundering through payment platform

In this further variant of the attack of Section 4.2, a third-party payment platform acts as intermediary, allowing Alice to deposit her expiring digital cash onto an account she holds there. The assumption is that, when Alice deposits her digital cash onto the platform, the platform becomes the secondary recipient (even though it is not a merchant) and is therefore able to return Alice's expiring digital cash to the issuer and redeem it for regular digital cash. We still assume Case 2, as in Sections 4.2 and 4.3.

The platform then provides options to convert Alice's balance into digital credits (e.g. Alipay), or into prepaid cards from itself or various other issuers, or into any other forms of money. At that point, the expiration restriction has been removed. Alice may, even after the original expiration date, use the digital credits to buy real goods, resell the prepaid cards to third parties for cash, or even withdraw the balance for cash directly. As ever, Alice will incur an unlocking fee: either a straightforward platform fee or perhaps, in the case of prepaid gift cards, a reduced platform fee plus a slight reduction in the redeemable value when reselling the less-fungible prepaid gift card if it is locked to a particular store.

Once more, the victim is the issuer, since Alice and the platform cooperate to break the expiration mechanism.

The enabling assumption of this attack seems not to hold for the Shenzhen experiment, since a payment platform would not qualify as one of the 3,389 designated merchants. Perhaps a dishonest designated merchant might stage this attack by *also* acting as a payment platform, in the same way that some newsagents also sell basic groceries and have a post office licence. But then the issuer might detect the attack by monitoring not only whether Bob is a designated merchant but also whether, in that particular transaction for which he wants to redeem the non-expiring equivalent of the incoming expiring cash, he sold an approved item as opposed to taking an incoming deposit. As with the countermeasures discussed in Section 4.2, the issuer might perform random checks and demand to see receipts (from Alice) and sales logs (from Bob).

[16] For example an imaginary but plausible policy that we are making up on the spot might be that purchases made with expiring cash are only refunded with new expiring cash *with the same leftover duration*. In other words, if Alice buys the TV with cash that expires a week later, and then returns the TV for a refund three months later, then Bob repays her with new digital cash that expires a week after the refund.

4.5 Attack: buying assets as long-term store-of-value

Alice purchases assets that retain long-term value, such as precious metals, collectibles, real estate, non-perishable commodities, art, foreign digital cash or prepaid store cards[17].

Alice may use the assets herself (arguably in full compliance with the issuer's original intentions, although the issuer might have wanted to limit what she could buy to specific asset categories) or resell them for cash at a later date.

Here too, once again, the victim of the attack is the issuer, whose intended monetary policy is violated when Alice defeats the expiration mechanism.

As for possible countermeasures, similarly to Section 4.2, the issuer might carry out random spot checks, with heavy fines as deterrent. First of all, the issuer might indeed check that Alice only bought approved items from approved vendors. Second, the issuer might do further spot checks some time later, asking Alice to prove that she still has the item (though it may be harder to ask her to prove that she *consumed* a perishable and legitimately-bought item; but then a consumable would be harder for Alice to use as a long-term resaleable asset for mounting this attack). If the issuer could observe all digital cash flows in and out of Alice, it might be in a position to notice whether Alice resold an item; but Alice might receive payment in so many alternative ways that it would be hard even for a powerful issuer to be certain to have monitored them all.

4.6 Attack: registering as a merchant

Alice registers as a designated merchant in order to earn the licence to redeem expiring cash back into non-expiring cash. When she receives the handout in expiring digital cash, she pays it to herself (or, more precisely, to her merchant persona, which would have to be a different digital wallet) thereby unlocking it.

Once again, the victim in this attack is the issuer, whose monetary policy is violated by Alice breaking the expiration mechanism.

This attack is not particularly strong because we assume it would be trivial for the issuer to discover it through anomaly detection analysis of the financial flows. Unless Alice actually started a real business, she would stand out as a merchant who redeems expiring cash but has no sales.

4.7 Attack: faking the merchant flag

In this variant of the attack in Section 4.6, Alice pretends to be a merchant not by registering as one but by some low-level hacking of whatever flag indicates the status of her wallet as a merchant's wallet. The attack is predicated on Alice's technical ability to do so. Whether this is at all realistic (and it might not be) depends on the implementation. If she succeeds, she gains the same ability

[17] Of course the different kinds of assets have different volatilities and this will factor into Alice's decision of which to pick, alongside other considerations such as ease of storage, ease of resale, fungibility, perishability etc.

(of converting expiring cash into non-expiring) as in Section 4.6, and proceeds accordingly.

Once again the victim of this attack is the issuer, for the usual reason.

This attack seems particularly weak, firstly because it depends on the existence of some technical vulnerability in the implementation of the merchant wallet, and on Alice's ability to exploit it; and secondly because it will be easy for the issuer to verify at the back-end whether Alice is truly a designated merchant (regardless of the flag on Alice's local wallet) before redeeming the expired cash.

4.8 Attack: collateral for loan

This attack is qualitatively rather different from the others so far described. It is also the first of our attacks that applies to both Case 1 and Case 2.

Alice puts down her expiring cash as collateral for a loan, to be repaid (in non-expiring cash) before the expiration of her cash. In exchange for this guarantee, the lender lends her the same amount in non-expiring cash. minus a lending fee. Alice disappears, taking with her the borrowed non-expiring cash. The lender sees she does not repay the loan on the agreed date, so he repossesses the collateral. However, shortly afterwards, the collateral expires and becomes worthless. As a result Alice has converted her expiring cash into non-expiring (minus the lending fee), while the lender has lost all the cash he lent her. For once, the victim is not the issuer but our new character, the lender.

There are, however, a few objections.

First, under the terms and conditions of the Shenzhen experiment, the lender would not qualify as a designated merchant. Therefore (a) Alice would not be able to pay him in the first place; and (b), even if she did, he would not be able to redeem the expiring cash if he needed to repossess the collateral; therefore, with awareness of point (b), he should never consent to loan anything to Alice, even at a premium, since her collateral offers him no guarantee of recovering his loan. However, if we relaxed the Shenzhen terms and conditions and we allowed Alice to pay her expiring digital cash to anyone, then the scenario would still be plausible under both Case 1 and Case 2.

In Case 1, the collateral eventually expires: if the lender does not redeem it before then, he loses it. If he attempts to redeem it, though, in the time window between the expiration of the loan and the expiration of the cash, he will find that, on the open market, it is worth less than its nominal value because of the "haircut" described in Figure 1. A rational lender would want to ensure that the collateral covers him in full in case of Alice's default; so, before issuing the loan, he would demand an additional premium from Alice to compensate for the estimated haircut at the (future) time of loan redemption.

In Case 2, instead, after having been paid to the lender, the collateral no longer expires. The lender is able to cash in the full amount of the collateral if Alice defaults. As a result, Alice would still win (having converted her expiring cash into non-expiring), the lender would be covered by redeeming the collateral in non-expiring cash from the issuer and would thus be indifferent to the attack,

and the victim would now be the issuer, whose monetary policy would be violated by Alice having broken the expiration mechanism.

Second, the attack as we originally described, in which the loser is the lender, relies on Case 1 and on the carelessness of the lender. The lender only loses out if, in Case 1, he fails to redeem the collateral before it expires (or, worse, if he fails to notice that the collateral expires in the first place). A careful lender would immediately cash in the collateral as soon as the loan expired unpaid. Then he would not suffer any attack, as he would recover his loan in full (assuming he also got the additional premium to cover the haircut). Alice would have converted the expiring cash into non-expiring, thus again cheating the issuer, but would have had to pay the haircut premium for that. In Case 2, as we already said, the lender is protected from the attack because his collateral does not expire, and the victim of the attack is the issuer.

In terms of countermeasures, the terms and conditions of the Shenzhen experiment are a preventive safeguard against the attack because, as we said in the first point above, they prevent Alice from paying the lender because he is not an approved merchant.

Without the Shenzhen restrictions, in Case 1 the obvious countermeasure is for the lender to redeem the collateral as soon as the loan expires unrepaid (and of course to demand the haircut premium before agreeing to the loan). In Case 2, where the victim is the issuer, the usual countermeasure of Section 4.2 (namely probabilistic spot checks on whether Alice spent the cash in the prescribed way) might still detect and deter the attack, but it would be reasonable to object that the issuer ought to have imposed Shenzhen-style constraints in the first place as a much better safeguard that would have prevented the attack altogether.

4.9 Attack: wrapped token

In DeFi, wrapping a digital asset consists of placing it in secure storage and minting a new token of equivalent value on a different blockchain. It is commonly done to facilitate cross-chain compatibility, for example to be able to trade Bitcoin on the Ethereum blockchain.

In this attack, a variation of the one in Section 4.8, Alice wraps her expiring digital cash in some non-expiring cryptocurrency and then passes on the wrapped token to merchant Bob who accepts it at face value, exchanging it for non-expiring cash or an asset of equivalent value. In Case 1, when the cash inside the wrap expires, it is Bob who loses out. In Case 2, it is the issuer. In either case, Alice has converted her cash from expiring to non-expiring.

Here too, in Case 1 the attack is predicated on Bob's carelessness: in other words, it only works if Bob does not notice that the cash inside the wrap has an expiration date (otherwise he would be wise not to accept it, or at least not to accept it without a commensurate haircut premium, and in any case to redeem it for non-expiring cash before its expiration).

The fact that Bob is a merchant rather than a lender makes this attack possible under the Shenzhen terms. Since the Shenzhen terms imply Case 2 (expiring cash becomes non-expiring as soon as an approved merchant receives

it), the attack becomes a variation of the "fake transaction" of Section 4.2 or of the "fake refund" of Section 4.3.

Regarding countermeasures, in Case 1 (non-Shenzhen) the situation is similar to that in the previous Section 4.8: Bob must demand a haircut premium before accepting the wrapped token and must redeem it for non-expiring cash as soon as possible. From a socio-technical and usability-centric viewpoint, however, we note that this remedy is not quite so simple in practice—deception is at the root of many scams [29] and blaming the victim for carelessness is not a working solution. Neither is demanding the potential victim's attention every time, even with the good intention of preventing scams: the user's attention is limited, so is their compliance budget [5], and crying wolf exhausts both quickly. Better interface and interaction design is called for, in order to defeat the fraudster.

In Case 2 (possibly Shenzhen), Bob is safe if he knows he will get back non-expiring cash from the issuer. If the issuer wants to prevent Alice from making her received cash non-expiring,the countermeasures of Sections 4.2 and 4.3 apply—that is to say, probabilistic spot checks on whether Alice and Bob are violating the spirit of the rules by not engaging in a genuine sale of an approved article, with heavy penalties as deterrent.

4.10 Trivial countermeasures

Shenzhen trial aside for the moment, if digital cash were untraceable then an issuer would not be able to enforce restrictions on where it is spent. Conversely, if the issuer had perfect visibility of all digital cash transactions, many of the attacks that attempted to circumvent the issuer-imposed restrictions would be trivial to detect.

Depending on where the underlying digital cash implementation is situated on the privacy spectrum—from the total observability favoured by dictatorships and law enforcement on one extreme to the total untraceability favoured by civil libertarians and criminals on the other—the technical ability of the issuer to detect attacks and enforce restrictions on the use of the digital cash is modulated accordingly.

While Bitcoin's original blockchain attempted to protect privacy of digital cash users by making them pseudonymous, this lack of traceability was promptly exploited by criminals, who used Bitcoin as the currency of the Dark Web (drugs and arms trade, extortion, ransomware etc). For crime prevention reasons, most governments impose strict KYC/AML[18] regulations on the use of money of any kind, whether traditional or digital. CBDCs, being government-endorsed, will undoubtedly be based on a strong KYC/AML foundation. Cryptocurrencies, as they become mainstream, are being subjected to similar regulations: acquiring and holding Bitcoin legally, these days, requires interacting with approved and highly regulated exchanges that will insist on KYC/AML.

[18] Know Your Customer is a process by which banks and other financial intermediaries are required to verify their customers' identity. Anti Money Laundering, which includes KYC, is a series of checks intended to identify suspicious transactions and prevent money laundering and financing of criminal activities.

All this to say that it is unrealistic to expect cash-like anonymity and untraceability for any implementation of (expiring) digital cash that went mainstream, whether based on CBDCs or cryptocurrencies.

From an intellectual viewpoint, the greater the powers of traceability and control the issuer has over the digital cash, the easier and less challenging the problem of enforcing the rules becomes, at the expense of privacy and civil liberties for the citizens who use the digital cash. If the issuer can observe every transaction, most attacks are detectable. If the issuer can also revoke individual digital cash units, the effects of most attacks can be reversed, if not prevented altogether.

Indeed the attacks in Sections 4.2, 4.3, 4.4 and 4.5 are all trivially defeated by the issuer specifying what the original recipient is allowed to do with the received expiring digital cash and then making those digital cash units worthless unless spent in compliance with those terms. The party who loses out when the cash expires might be the secondary recipient rather than the original recipient but, if so, this obviously imposes a strong incentive on the secondary recipient not to accept expiring cash other than for transactions that fully comply with the issuer's policy. Besides, the issuer might impose additional punishments on the original recipient (or indeed on both parties) for mis-spending the expiring cash in violation of the agreement under which it had been originally gifted.

Although we do not have full details on the technical implementation of the expiring e-CNY used in the Shenzhen experiment, it was obviously an instance of a CBDC issued by the People's Bank of China. We therefore assume that the PBC retained full observability of the whereabouts and ownership of each digital cash unit in circulation, as well as the ability to revoke individual digital cash units. The issuer would thus have had the technical ability to detect, defeat and punish almost all of the attacks we described.

For this reason, from a research perspective we move on from the Shenzhen experiment. There is no great research challenge in defending the security of CBDC-based expiring digital cash for an all-seeing and all-powerful issuer.

4.11 Alternative implementation: decentralised expiring digital cash

Let us instead consider the alternative hypothetical scenario in which the issuer creates expiring digital cash not as a specially programmed CBDC but on a public programmable blockchain. As a motivation we might again imagine that the issuer of the expiring digital cash, this time a government agency rather than the central bank, wishes to distribute aid to certain beneficiaries (e.g. to stimulate the economy during a recession, or to help a population hit by a natural disaster) provided that the aid is used for specific purposes, rather than hoarded or wasted on luxury items. Whether the aid consists of existing money that the issuer had already set aside or (as in the case of helicopter money) of new cash printed for that purpose, in this scenario the issuer of the expiring digital cash transfers that cash onto a public blockchain and creates the expiring digital cash there, with an appropriate smart contract.

It is this smart contract that defines the conditions under which the digital cash expires and what happens to it on expiration. Obviously, expiration will occur when the expiration date is reached; but also when the digital cash is used in transactions that do not comply with the terms under which it was issued. On expiration, the digital cash returns to the issuer: it becomes worthless to whomever held it at that time, but it does not disappear from the system[19].

To what extent can the issuer's terms and conditions on the use of the aid be codified in a smart contract? Can the blockchain tell whether the recipient is one of the designated merchants? Can the blockchain tell whether the item being bought in the transaction is among the approved ones? The only constraints that can be codified in the smart contract are the ones corresponding to predicates that can be automatically verified.

Will the smart contract implement Case 1, where the digital cash expires at the specified date regardless of who holds it, greatly reducing (perhaps even destroying) the acceptability of the digital cash by third parties? Or will it implement Case 2, where the digital cash stops expiring when first spent, as in the Shenzhen experiment, ensuring that the digital cash will be spendable but laying the system open to the many attacks we described? Could any of these attacks be successful in the decentralised scenario? This largely depends on the previously highlighted point: how many of the issuer's terms and conditions can be codified in the smart contract? Those terms that can be codified will be automatically enforced. The others will probably create loopholes and, most likely, corresponding attacks. It will then be a burden for the issuer to detect and pursue those violations off-chain after the fact.

All of the above questions might be worth investigating further in future work. While a government agency and a public blockchain make strange bedfellows, the question of how to ensure the security of a programmatic feature of digital cash (in this case: expiration under certain conditions) without having full KYC observability and full control of the underlying platform is an interesting research problem.

5 If it expires, is it still digital cash?

It should come as no great surprise that implementing robust and secure expiring digital cash is much simpler in a fully traceable centralised environment than in a privacy-protecting decentralised one—provided one trusts the central authority not to abuse its far-reaching powers. Not just the power of snooping but also the even more ominous power of selectively revoking the currency units of the individuals it dislikes.

Someone who, perhaps inspired by Chaum's pioneering work [10], took the stance that cash-like anonymity ought to be a defining property of digital cash,

[19] Except perhaps in the case of helicopter money: if the expiring digital cash was issued on the blockchain as counterpart for digital cash that had been printed for that purpose, on expiration the issuer might decide to destroy the new digital cash, reversing the inflationary pressure caused by its creation.

might at this point argue that *expiring* digital cash cannot be digital cash, if it has to give up its anonymity in order to be implemented securely—although, to be fair, they might have to say the same of most CBDCs, given their requirement to comply with KYC/AML/CFT regulations.

Similarly, someone who took the stance that being a store of value is a defining property of money and thus of digital cash might at this point argue that *expiring* digital cash does not qualify as digital cash, because it no longer retains its value after expiration—although, to be fair, they might have to say the same of many cryptocurrencies, given their wild volatility (several orders of magnitude over a few years).

Furthermore, as we noted in Section 4.1, something that can only be spent at specific merchants and on specific goods sounds more like a coupon, a voucher or a store card than cash, which instead is totally fungible and can be spent anywhere and on anything. The European Central Bank published in 2012 a study on "Virtual Currency Schemes" [15] (as distinct from real currencies like the USD or the EUR) that encompassed, under that umbrella term, schemes as diverse as air miles, Second Life's Linden Dollars and the then nascent Bitcoin. They noted in passing that the total value of Frequent Flyer programmes had been reported by *The Economist* in 2005 as having already surpassed the M0 dollar money supply (banknotes and coins in circulation). A distinguishing feature of the various kinds of virtual currency schemes, which the report accordingly classifies into three buckets, is their convertibility to and from real-economy money: the Type 1 virtual currency cannot be converted; the Type 2 can be bought with real money but not vice-versa; whereas the Type 3 enjoys bidirectional convertibility with real money. It is significant that the terms and conditions of the Shenzhen trial explicitly prevented recipients of expiring e-CNY from transferring them to other individuals. Naturally, such restrictions can be circumvented by trading the virtual currency in a (black) market, which always inevitably happens, legally or illegally, when there is enough demand. Indeed, Jenjarrussakul and Matsuura [21] studied the liquidity of the many loyalty point programmes available to customers in Japan, concluding among other things that the virtual currencies with the greatest liquidity experienced the more significant security incidents. Clearly, vouchers that can be exchanged for only a limited range of goods are less attractive than fungible cash, and quite distinct from it. In that sense, the expiring e-CNY distributed during the Shenzhen trial did not enjoy the same purchasing power as genuine CNY, given the restrictions on where, when and on what they could be spent. On that basis, we do not believe they ought to be counted as cash[20].

Crucially, we observe that the practice of handing out cash that can only be spent within a certain period and on certain items and at certain retailers is not

[20] Admittedly, the fact that the expiring cash of the Shenzhen experiment came with these additional restrictions is not in itself a proof that no other form of digital cash that we might envisage could be expiring and still count as cash. But remember our more general comment about store of value, and see our next consideration that it's not actually the cash that's expiring.

fundamentally a feature of the medium of exchange (digital or otherwise) but rather of the *agreement* that regulates the transaction.

We argue it is improper, or at least misleading, to speak of "expiring digital cash" and thus to attribute the expiration to the medium of exchange. The expiration is not a feature of the cash (which, if it expired, could no longer be considered a trustworthy store of value): it is instead one of the many terms of the contract between issuer and recipient, which could very well be implemented with traditional non-digital, non-programmable cash. The issuer might say:

> I grant you this gift of X dollars on condition that you spend it according to these terms (spend it by this date, only on a subset of these designated items, only buying from these approved suppliers, etc etc). If you violate these terms, you will have to repay the gift and also pay a fine.

This is simply a contractual agreement and has nothing to do with the payment medium, whether digital, programmable or otherwise. It does not require expiring digital cash in order to be implemented or enforced.

While we do not question that the described functionality might have plausible uses, a much clearer mental model than "expiring cash", in our view, is that *what expires is the agreement, not the digital cash.* The donated cash does not expire, it just changes hands when the underlying contract says it should.

6 Conclusions

A large class of attacks on expiring digital cash (Sections 4.2–4.7) is aimed at circumventing the expiration mechanism. We observe that most of these attacks are easy to detect, deter and remedy in a centralised context where the issuer retains traceability and control over the digital cash. But centralisation puts large powers in the hands of a principal that might misuse them, not just against fraudsters but against political opponents.

Another class of attacks (Sections 4.8–4.9) is instead aimed at defrauding third parties by tricking them into accepting expiring cash without fully realising the consequences. Such attacks are based on deception and distraction. The way to counter them involves good interface and interaction design.

Having envisaged and analysed a non-exhaustive but representative variety of attacks, and while acknowledging that a CBDC-based solution is both easier to implement and more likely to happen than its decentralised alternative, we believe there might be merit in studying the hypothetical scenario in which the issuer of the expiring digital cash does not have full control of the platform. Future work investigating that under-explored area of the design space might lead to interesting discoveries for DeFi security.

With all that said, though, we believe that "expiring digital cash" is an oxymoron. If it can only be spent on certain things and in certain shops, if it expires and loses its value, it's not really cash. And in fact, we argue, it doesn't even expire: it just changes wallet. A more accurate mental model, in our opinion, is to view the cash as non-expiring and the gift as expiring, according to the terms of the contractual agreement between giver and receiver.

Acknowledgements We are grateful to Hashem Pesaran for encouraging and perceptive comments. All remaining infelicities in the paper are the sole responsibility of the authors.

References

1. "Progress of Research & Development of E-CNY in China". Technical report, People's Bank of China, July 2021. URL http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf.
2. Svetlana Abramova, Pascal Schöttle and Rainer Böhme. "Mixing Coins of Different Quality: A Game-Theoretic Approach". In Michael Brenner, Kurt Rohloff, Joseph Bonneau, Andrew Miller, Peter Y.A. Ryan, Vanessa Teague, Andrea Bracciali, Massimiliano Sala, Federico Pintore and Markus Jakobsson (Editors), "Financial Cryptography and Data Security", pages 280–297. Springer International Publishing, Cham, 2017. ISBN 978-3-319-70278-0. https://doi.org/10.1007/978-3-319-70278-0_18. URL https://fc17.ifca.ai/bitcoin/papers/bitcoin17-final40.pdf.
3. Bank of England and HM Treasury. "The digital pound: a new form of money for households and businesses? (Consultation Paper)", February 2023. URL https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf.
4. Bank of Japan. "The Bank of Japan's Approach to Central Bank Digital Currency", October 2020. URL https://www.boj.or.jp/en/about/release_2020/data/rel201009e1.pdf.
5. Adam Beautement, M. Angela Sasse and Mike Wonham. "The compliance budget: managing security behaviour in organisations". In "Proc. New Security Paradigms Workshop 2008", pages 47–58. ACM, 2008. https://doi.org/10.1145/1595676.1595684. URL http://hornbeam.cs.ucl.ac.uk/hcs/people/documents/Adam%27s%20Publications/Compliance%20Budget%20final.pdf.
6. Biagio Bossone and Ahmed Faraghallah. "Expiring money (Part I)", November 2022. URL https://blogs.worldbank.org/allaboutfinance/expiring-money-part-i.
7. Biagio Bossone and Ahmed Faraghallah. "Expiring money (Part II)", November 2022. URL https://blogs.worldbank.org/allaboutfinance/expiring-money-part-ii.
8. Vitalik Buterin. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform", 2014. URL https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf.
9. David Chaum. "Blind Signatures for Untraceable Payments". In David Chaum, Ronald L. Rivest and Alan T. Sherman (Editors), "Advances in Cryptology", pages 199–203. Springer US, Boston, MA, 1983. ISBN 978-1-4757-0602-4. https://doi.org/10.1007/978-1-4757-0602-4_18. URL http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF.
10. David Chaum. "Security without identification: transaction systems to make big brother obsolete". *Communications of the ACM*, **28**(10):1030–1044, October 1985. ISSN 0001-0782. https://doi.org/10.1145/4372.4373. URL https://chaum.com/security-without-identification/.
11. David Chaum, Amos Fiat and Moni Naor. "Untraceable Electronic Cash". In Shafi Goldwasser (Editor), "Advances in Cryptology—CRYPTO '88", volume 403

of *LNCS*, pages 319–327. Springer-Verlag, 1990, 21–25 August 1988. ISBN 978-0-387-34799-8. https://doi.org/10.1007/0-387-34799-2_25. URL https://chaum.com/wp-content/uploads/2021/12/Untraceable_Electronic_Cash.pdf.
12. David L. Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms". *Commun. ACM*, **24**(2):84–88, February 1981. ISSN 0001-0782. https://doi.org/10.1145/358549.358563. URL https://dl.acm.org/doi/pdf/10.1145/358549.358563.
13. Jeremy Clark, Didem Demirag and Seyedehmahsa Moosavi. "Demystifying stablecoins". *Communications of the ACM*, **63**(7), July 2020. URL https://dl.acm.org/doi/pdf/10.1145/3386275.
14. Nigel Dodd. *The social life of money*. Princeton University Press, 2014.
15. European Central Bank. "Virtual Currency Schemes", October 2012. URL https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.
16. European Central Bank. "Report on a digital euro", October 2020. URL https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.
17. European Central Bank. "Annex 1: Functional and non-functional requirements linked to the market research for a potential digital euro implementation", January 2023. URL https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs230113_Annex_1_Digital_euro_market_research.en.pdf.
18. Federal Reserve. "Money and Payments: The U.S. Dollar in the Age of Digital Transformation", January 2022. URL https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf.
19. Milton Friedman. *The optimum quantity of money and other essays*. Aldine Publishing Company, Chicago, IL, USA, 1969.
20. Silvio Gesell. *The Natural Economic Order*. Peter Owen, 1958. URL https://www.silvio-gesell.de/the-natural-economic-order.html.
21. Bongkot Jenjarrussakul and Kanta Matsuura. "Analysis of Japanese Loyalty Programs Considering Liquidity, Security Efforts, and Actual Security Levels". In "13th Workshop on the Economics of Information Security (WEIS 2014)", June 2014. URL https://econinfosec.org/archive/weis2014/papers/JenjarrussakulMatsuura-WEIS2014.pdf.
22. William Stanley Jevons. *Money and the Mechanism of Exchange*. D. Appleton, 1875.
23. Charles M. Kahn, Maarten R.C. van Oordt and Yu Zhu. "Best Before? Expiring Central Bank Digital Currency and Loss Recovery". *Journal of Money, Credit and Banking*, 2024. https://doi.org/https://doi.org/10.1111/jmcb.13208. URL https://onlinelibrary.wiley.com/doi/abs/10.1111/jmcb.13208.
24. Kamhon Kan, Shin-Kun Peng and Ping Wang. "Understanding Consumption Behavior: Evidence from Consumers' Reaction to Shopping Vouchers". *American Economic Journal: Economic Policy*, **9**(1):137–153, 2017. URL http://www.jstor.org/stable/26156428.
25. Karl Menger. "On the Origin of Money". *The Economic Journal*, **2**(6):239–255, 06 1892. ISSN 0013-0133. https://doi.org/10.2307/2956146.
26. Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system", October 2008. URL https://web.archive.org/web/20140320135003/https://bitcoin.org/bitcoin.pdf.
27. People's Bank of China. "E-CNY: main objectives, guiding principles and inclusion considerations". In Bank for International Settlements (Editor), "CBDCs in

Emerging Market Economies", volume 123 of *BIS Papers*, pages 45–54. Bank for International Settlements, Basel, 2022. URL https://www.bis.org/publ/bppdf/bispap123_e.pdf.

28. Shenzhen Special Zone Daily. "Luohu distributes 10 million CNY in digital RMB red envelopes", October 2020. URL https://www.sz.gov.cn/cn/xxgk/zfxxgj/zwdt/content/post_8164358.html. Original article in Chinese.
29. Frank Stajano and Paul Wilson. "Understanding scam victims: seven principles for systems security". *Communications of the ACM*, **54**(3):70–75, March 2011. URL http://www.cl.cam.ac.uk/~fms27/papers/2011-StajanoWil-scam.pdf. Revised version of Tech Report UCAM-CL-TR-754. .
30. State Council of the People's Republic of China. "Detailed Rules for Implementation of Digital RMB Pilot Programs Announced", October 2020. URL https://www.gov.cn/xinwen/2020-10/09/content_5549918.htm. Original article in Chinese.
31. Nick Szabo. "Formalizing and Securing Relationships on Public Networks". *First Monday*, **2**(9), Sep. 1997. https://doi.org/10.5210/fm.v2i9.548. URL https://firstmonday.org/ojs/index.php/fm/article/view/548.
32. David Wheeler. "Transactions using bets". In Mark Lomas (Editor), "Security Protocols", pages 89–92. Springer, Berlin, Heidelberg, 1997. ISBN 978-3-540-68047-5. https://doi.org/10.1007/3-540-62494-5_7. URL https://link.springer.com/content/pdf/10.1007/3-540-62494-5_7.pdf.