arXiv:2111.04483v2 [econ.GN] 9 Nov 2021

Revisiting the Properties of Money*

Isaiah Hull[†1] and Or Sattath[2]

[1]Research Division, Sveriges Riksbank, Stockholm, Sweden
[2]Department of Computer Science, Ben-Gurion University, Beersheba, Israel

November 10, 2021

Abstract

The properties of money commonly referenced in the economics literature were originally identified by Jevons (1) and Menger (2) in the late 1800s and were intended to describe physical currencies, such as commodity money, metallic coins, and paper bills. In the digital era, many non-physical currencies have either entered circulation or are under development, including demand deposits, cryptocurrencies, stablecoins, central bank digital currencies (CBDCs), in-game currencies, and quantum money. These forms of money have novel properties that have not been studied extensively within the economics literature, but may be important determinants of the monetary equilibrium that emerges in the forthcoming era of heightened currency competition. This paper makes the first exhaustive attempt to identify and define the properties of all physical and digital forms of money. It reviews both the economics and computer science literatures and categorizes properties within an expanded version of the original functions-and-properties framework of money that includes societal and regulatory objectives.

Keywords: Money, CBDC, Digital Currencies, Quantum Money, Currency Competition
JEL Classification: E40, E42, E50, E51

*The opinions expressed in this article are the sole responsibility of the authors and should not be interpreted as reflecting the views of Sveriges Riksbank.

†Correspondence Address: Research Division, Sveriges Riksbank, SE-103 37, Stockholm, Sweden. Email: isaiah.hull@riksbank.se. Tel: +46 076 589 0661. Fax: +46 8 0821 05 31.

1 Introduction

Technological progress has historically enabled the development of new forms of money with novel and enhanced properties (1–5). The introduction of coins and paper money, for instance, improved portability and cognizability relative to commodity money. Private bank money offered the possibility to earn interest and (eventually) transact digitally. Cryptocurrencies, such as Bitcoin, provided censorship resistance. Central bank digital currencies, which are under research and development at an increasing number of central banks (6, 7), promise to restore public money, but in a digital form. And quantum money, which has been theoretically studied but is not yet technically feasible, could reproduce the properties of cash, but with improved unforgeability guarantees and the ability to transact digitally.[1]

While digital forms of money are now the preferred medium of exchange in many countries (9), the terminology used to describe money is still largely derived from foundational texts on physical currency, such as Jevons (1) and Menger (2). Furthermore, the academic discussion of money's functions that followed these texts appears to have peaked prior to the development of digital currencies, as illustrated in Figure 1 in Section B. Consequently, many concepts that are routinely used in the modern literature on money were crystallized prior to the digital era.

Our intention is to update the standard framework for describing money by incorporating the properties of digital forms of money. To construct an exhaustive list of such properties, we not only review the economics literature, but also examine the parallel computer science literature, which approaches the properties of digital forms of money from a design perspective, focusing on what is achievable given a set of technical constraints. We also evaluate the performance of a selection of broad categories of money with respect to each of these properties in Table 1. This update to Jevons (1) and Menger (2), which builds on recent work on the properties of money (10–14), should have value for those doing research on CBDCs, cryptocurrencies, and digital payment schemes.

Part of the motivation for revisiting the properties of money is to provide better framing for the current period of rising currency competition, which follows an extended era of dominance by public currencies (15). Whereas traditional forms of competition centered around physical proximity and macroeconomic integration (12), emerging forms may center around less familiar concepts, such as throughput, latency, and smart contracts. Competition may happen within a set of uniform currencies, such as cash and bank deposits, or across non-uniform currencies, such as the U.S. dollar (USD) and Bitcoin. Our discussion of currency competition will adopt an inclusive definition that incorporates both.

The framework proposed in this paper could also be used to study the trade-offs inherent in money design choices, such as those discussed in Agur et al. (16) and Ferarri et al. (17). Selecting one set of properties will necessarily entail excluding others. Consequently, placing too much emphasis on a property that is not broadly demanded (or is demanded by regulators, but not consumers) may result in a form of money that underperforms in a currency competition. One clear example of such a trade-off is the choice between untraceability and anti-money laundering (AML) compliance. A less obvious trade-off is between local verifiability, which is a form of forgery detection that does not require a third party, and the ability to secure against human and technical errors by performing backup.

The continued relevance of public money in the 21st century may depend on how well central banks

[1] See Hull et al. (8) for an overview of progress in the theoretical and experimental development of quantum money.

navigate these trade-offs (12, 18–20). In the previous round of currency competition, cash declined in use relative to private bank deposits (9, 15), suggesting that central banks were either incapable or uninterested in retaining control over the medium of exchange. In the emerging round of currency competition, the stakes may be even higher. Widespread adoption of a currency that is not uniform with a country's public money, such as a cryptocurrency or another central bank's CBDC (digital dollarization), could result in the loss of control over both the medium of exchange *and* unit of account, as well as the inability to conduct monetary policy (12). Many central banks appear to have concluded that it will be necessary to issue a form of money that is *digital* in order to counter these threats (6, 7); however, no consensus exists on which other properties are necessary to remain competitive. Furthermore, it remains unclear whether a central bank would even want a CBDC to be truly competitive, as this might risk substantial disintermediation (21).

The return to an era of currency competition raises many regulatory and policy concerns; however, it also offers the possibility of improving money by incorporating the latest relevant technological advances, and extending the set of available regulatory and policy tools. Some have also argued that currency competition is needed to discipline central banks (22, 23). Others claim that the increase in competition from demand deposits has already resulted in institutional improvements (15). The issuance of new forms of money could also lead to improvements in the measurement of monetary aggregates and an improved toolset for tracking consumption in real time during crises.An expansion in the set of viable currencies could also have distributional implications by allowing otherwise marginalized and unbanked persons to transact digitally.

Organization. First, we introduce the expanded set of properties of money and provide a definition for each. We sort them according to the functions introduced in Jevons (1) and Menger (2) and commonly cited in the literature: 1) medium of exchange, 2) standard of deferred payment, 3) store of value, and 4) unit of account. We also include a separate category for properties that enhance a societal or regulatory function. In the cases where a property affects multiple functions, we categorize according to the primary function. In addition to defining each property, we also examine the extent to which it is present in a set of broad categories of money in Table 1. Next, we discuss a selection of properties that apply to pairs or groups of currencies, rather than individual currencies. Finally, we conclude with a discussion of the implications of CBDC and private currency design choices.

2 Properties of Money

This section provides an update to the lists of monetary properties originally defined in Jevons (1) and Menger (2), which are still frequently referenced, but were only intended to describe physical forms of money, such as commodity money or metallic coins. It draws from both the economics and computer science literatures, and provides an evaluation of several broad categories of money within this framework. For each property, we attempt to identify the function to which it corresponds. In cases where there are multiple functions, we categorize according to the primary function.

In general, we attempt to use a positive framing for each property. For example, we use *low* pecuniary transaction cost as a property, rather than pecuniary transaction cost. In some cases, however, the properties we consider are not positive in an absolute sense, but may be desirable in the context of a specific design goal. Consider, for example, reversibility, which is the property that a transaction can be canceled under certain conditions. In some settings, the buyer's protection is the most important consideration and, thus, reversibility takes precedence, while in others, finality is more important and reversibility is undesirable. Other properties may be positive in an absolute sense, but their adoption forces the exclusion of other desirable properties. For instance, both untraceability and anti money laundering compliance could be considered desirable properties, but strengthening one will necessarily require weakening the other. Another such trade-off occurs in the context of quantum money: some *private-key* quantum money schemes are unconditionally secure (e.g. Wiesner's scheme); whereas *public-key* quantum money schemes require computational hardness assumptions (24). As such, the choice between a private and a public key scheme implies a trade-off between the type of verifiability that the scheme supports and the level of security: public verifiability is preferred to private verifiability, but unconditional security is better than security based on computational assumptions.

2.1 Medium of Exchange Function

Jevons (1) describes a medium of exchange as something that is "...esteemed by all persons... which any person will readily receive" and a "means of producing necessities of life at any time." As such, we may convert what we produce into a medium of exchange and then use that medium of exchange to purchase consumption goods. In this subsection, we examine properties of money that relate to its ability to function as a medium of exchange. For a theoretical treatment of money's medium of exchange function, see Wallace (25), Kiyotaki and Wright (26), Oh (27), Kiyotaki and Wright (28), Williamson and Wright (29), and Lagos (30). For experimental work on money as a medium of exchange, see Brown (31), and Duffy and Ochs (32).

Acceptability. In order for money to function as a medium of exchange, it must be accepted as a form of payment. Menger (2) observed that the liquidity of a good influenced its acceptability. This is why commodity money was a popular choice prior to the invention of fiat currencies: commodities were liquid and had intrinsic value, which made it less costly for merchants to accept them as a form of payment. In contrast, acceptability is a substantial limitation for cryptocurrencies and is an important consideration for CBDCs. For a discussion of the conditions that need to be satisfied for a new fiat currency to become "acceptable," see Selgin (33). For a more theoretical treatment of acceptability, see (34, 35).

Accessibility. Bjerg (36) defined the concept of money "accessibility" as the answer to the question: Who can use this type of money? Bech and Garratt (10) use accessibility as one of the four criteria in their proposed taxonomy of money. Within this system, physical cash is considered to be "universally accessible," since any person or entity may easily obtain and use it. To the contrary, central bank reserves are not universally accessible, since they are not available to the general public. We argue that private bank money also has limited accessibility – relative to physical cash and cryptocurrencies – since it is not easily accessible to some groups, such as minors and foreigners.

Cognizability. Jevons (1) defines the cognizability of money as

> the capability of a substance for being easily recognized and distinguished from all other substances. ... Precious stones, even if in other respects good as money, could not be so used, because only a skilled lapidary can surely distinguish between true and imitation gems.

Primary Function	Property	Commodity Money (Gold)	Physical coins (USA coins)	Physical bills (USA bills)	Central Bank Reserves (Bank reserves at the Federal Reserve)	Bank deposits (USA bank savings account)	CBDC (No mature realizations)	In-game currency (PokéCoin)	Cryptocurrency (Bitcoin)	Cryptocurrency with DApps (Ethereum)	Privacy oriented Cryptocurrency (Zcash)	Stable Coin (Tether ERC-20 USD)	Private-Key Quantum Money (Wiesner's scheme [no realization])	Public-Key Quantum Money (Farhi et al. scheme [no realization])
Medium of Exchange†	Acceptability†	✗	✓	✓	✗	✓	✓	✗	−	−	−	−	✓	✓
	Accessibility	✓	✓	✓	✗	−	✓	−	✓	✓	✓	−	✓	✓
	Cognizability†	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
	Digital	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Divisibility† and mergeability	−	−	−	✓	✓	✓	✓	✓	✓	✓	✓	−	−
	Ease-of-use	✗	✓	✓	✓	✓	✓	✓	−	✗	−	−	✓	✓
	Latency	✓	✓	✓	✓	✗	✓	✓	−	✓	−	✓	✓	✓
	Local verifiability	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
	Low computational tx cost	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
	Low pecuniary tx cost	✓	✓	✓	✓	−	✓	✗	📈	📈	✓	📈	✓	✓
	P2P transfer mechanism	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓
	Portability†	−	−	−	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Proof of payment	✗	✗	✗	✓	✓	✓	✗	✓	✓	✓	✓	?	✗
	Reputation	✓	✓	✓	✓	✓	✓	✗	−	✗	✗	✗	✓	✓
	Reversibility	✗	✗	✗	✓	✓	?	✗	✗	✗	✗	✓	✗	✗
	Smart contracts	✗	✗	✗	✗	✗	✓	✗	−	✓	✗	✓	✗	✗
	Throughput	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓
	Transferability	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
	Transparency	✗	✗	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
	Untraceability	✓	✓	✓	✗	−	?	−	✗	✗	✓	✗	−	✓
Standard of Deferred Payment†	Legal tender	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓
Store of Value†	Backup	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
	Durability†	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	−	−
	Interest-bearing	✗	✗	✗	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗
	Outside	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓
	Proof of reserves	✗	✗	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗
	Scarcity†	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Supply measurability	✗	✓	✓	✓	✓	✓	✗	✓	✓	−	✓	✓	✓
	Tax evadability	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓	?	✗	✓
Unit of Account†	Cost of currency exchange	✗	✗	✗	✓	✓	✓	✗	✓	✓	−	✓	✓	✓
	Fungibility†	✓	✓	✓	✓	✓	✓	✓	−	−	✓	−	✓	✓
	Stability†	−	✓	✓	✓	✓	✓	−	✗	✗	✗	✓	✓	✓
Societal or Regulatory	AML Compliant	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	−	✓	✗
	Censorship resistant	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✓
	Identity-based	✗	✗	✗	✓	✓	✓	−	✗	✗	✗	✗	✓	✗
	Public	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✓
	Resource efficiency	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓
	Unforgeability	✓	✓	−	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 1: Properties of money.

The table categorizes instantiations of broad categories of money according to the extent to which they exhibit different properties. Each row contains a property of money, categorized by the primary function to which it corresponds. Each column refers to a broad category of money, along with a representative example, given in parentheses, and is used to determine which properties apply. A † indicates that a property or function appeared in the original Jevons-Menger framework. A ✓ indicates that a form of money has a property, a − indicates that the property is present but weaker than in the best available implementations, an ✗ indicates that it is not present or not satisfactory, and A ? indicates that we are uncertain whether the property will hold. The 📈 symbol represents a volatile transaction cost. The precise definitions of less familiar forms of money are given in Appendix A. For the purpose of this table, we assume that quantum money is issued as a CBDC and, thus, has the properties of public money. It is also, of course, possible that it could be issued privately. In cases where there is lack of supporting information, we assume that the property is present if 1) it is trivially implementable with existing technology, 2) there are no binding legal or institutional constraints that prevent it from being implemented.

While the need for cognizability declined in the 20th century, it may once again become important in the emerging era of currency competition. Increased fragmentation in the monetary system, driven by a rise in the popularity of cryptocurrencies, other forms of private money, and competing CBDCs may make it difficult for users to identify counterfeit and fraudulent products. Indeed, theory suggests that reduced cognizability could result in increased counterfeiting and fraud (37–39).

The quantum money literature provides a refinement to the concept of cognizability that requires that a unit of money that is verified once – and, thus, appears to be valid – must also pass further verification attempts. This rules out acts of sabotage, where the attacker harms others, but does not benefit monetarily.

To understand this refinement, consider the case where malicious Mallory has valid bills, but tampers with them in such a way that they pass verification on the first attempt, but fail on subsequent attempts. Mallory sends that money to honest Alice who accepts the bills after they pass the (first) verification attempt. However, when Alice attempts to spend the money, it will fail the (second) verification attempt. Therefore, Alice is harmed, even though Mallory does not gain anything directly from the attack. This standard of cognizability is difficult to achieve in the context of quantum money, where the outcome of verification is not necessarily deterministic (40–43).

Digital. We define a form of money as "digital" if it can be exchanged remotely.[2] Existing quantum money schemes fall into the "digital" category of money, since transactions are conducted through the exchange of information, rather than the exchange of physical tokens.

Divisibility and mergeability. Divisibility is typically interpreted as a relative measure. Lee and Wallace (44), for instance, use the ratio M/s, where M is the per capita money stock and s is the size of the most common monetary unit. They find that this measure ranged from 25 to 130 in medieval Europe; whereas, it was closer to 40,000 for the United States in 2004.[3]

The concept of divisibility has been linked to money's medium of exchange function as early as Jevons (1), but gained renewed relevance in the era of digital currencies. Furthermore, its definition may also need to be revisited, since many forms of modern money, including bank deposits, can be divided into small denominations frictionlessly and without liquidity considerations. Thus, the most common denomination size may no longer be the relevant divisor.[4]

Demand deposits typically allow for divisibility down to the smallest denomination of coin or lower. Cryptocurrencies allow for an even higher degree of divisibility: the smallest denomination of Bitcoin is 1 satoshi, which is 10^{-8} bitcoins. An interesting use-case for such high divisibility is micro-payments (also called micro-transactions), which have been studied extensively in the context of electronic-cash systems.[5]

[2] Bech and Garratt (10) propose a taxonomy of money where "physicality" constitutes one of the four core properties, and where physical is the opposite of digital.

[3] Prior to the 19th century, money was not widely available in small denominations (45, 46). While may have been optimal (44), it also likely that it impeded the functions of money.

[4] Jevons (1) makes the following connection between money's divisibility and its capacity to serve as a medium of exchange: "a minor inconvenience of barter arises from the impossibility of dividing many kinds of goods. A store of corn, a bag of gold dust, a carcase of meat, may be portioned out, and more or less may be given in exchange for what is wanted. But the tailor, as we are reminded in several treatises on political economy, may have a coat ready to exchange, but it much exceeds in value the bread which he wishes to get from the baker, or the meat from the butcher. He cannot cut the coat up without destroying the value of his handiwork. It is obvious that he needs some medium of exchange, into which he can temporarily convert the coat, so that he may give a part of its value for bread, and other parts for meat, fuel, and daily necessaries, retaining perhaps a portion for future use."

[5] See, e.g., (47), and (48), and the references therein.

One such example relates to the main challenge in file-sharing peer-to-peer networks, such as BitTorrent (49), which is to discourage free riding (50). A simple way to encourage users to upload is to provide pecuniary incentives; however, this is challenging in a setting where there is no trust between the transacting parties. Fine-grained divisibility is useful because it permits payments for small chunks of data, eliminating the possibility of abusing the system.[6] There are existing solutions that claim to use an approach that is similar to the one mentioned here.[7] In contrast, existing quantum money schemes would not allow for frictionless divisibility.

In addition to divisibility, forms of money differ in the extent to which units can be merged together, a property which we will refer to as mergeability. Gold, for instance, can both be divided into arbitrarily fine units and also merged by melting the pieces together.

Mergeability is always achievable by collecting multiple units of the same denomination. However, storing more units may require more resources. With respect to physical cash, mergeability can be measured as the minimum number of units required to sum to an arbitrary number, x. For instance, in an economy with an idealized form of cash, which comes in denominations of 10^k for $k \in \mathbb{N}$, the mergeability scaling would be at most $10 \cdot \lceil \log_{10}(x) \rceil$.

Other forms of money, such as bank deposits and cryptocurrencies, achieve perfect scaling. That is, they do not require more resources to store more value.

For example, in an economy that uses precious stones as commodity money, the amount of resources needed to store N stones of a given size is higher than the amount needed for $N - 1$. However, if multiple types of precious stones are used, this will naturally result in different "denominations," allowing for the exchange of two low value stones for a higher value stone.

Ease of use. The cognizability of money is closely related to its ease of use. While cognizability refers to the difficulty of determining whether a piece of money is valid, ease of use refers to the difficulty of conducting a transaction with a unit of money, part of which will involve determining whether it is valid. Survey evidence suggests that perceived ease of use may be an important factor in determining whether or not an individual is willing to use a new form of money, such as a cryptocurrency (51).

Latency. Latency is defined as the time it takes for a transaction to settle. There are several potential causes of increased latency. Physical constraints are one: the speed of light, for instance, could add an order of a second for every round of communication needed in a digital transaction. A Bitcoin transaction is confirmed only after it is mined in a block, which takes 10 minutes on average (52). In other systems, such as credit cards, an inquiry into whether a transaction is fraudulent might incur a delay if the payer is asked to confirm the details of the relevant transaction. Note that latency is weakly coupled with the notion of reversibility.

[6] For example, if a payment of 1 cent occurs after 1MB, a free rider might try to download 1MB of the file, and then "run away" without paying. This free-rider might try to download the other parts of the file from other users, or other mechanisms. Naturally, in such systems, these types of strategies can be easily automated. If payment of a 10^{-6} cent is done after 1 byte, the user cannot download and "run away" with more then 1 byte, which renders this attack useless.

[7] Tokens worth at least $62 million USD that can be used in this market are currently in circulation as of January 2020. Evaluating the credibility of these services and tokens is outside the scope of this paper.

Local verifiability. Local verifiability means that counterfeiting can be detected without the involvement of a trusted third party. It was introduced as one of the necessary properties of a public-key quantum money scheme by Aaronson (53), but can also be used to evaluate the desirability of any form of money, including physical bills and coins, which can also be locally verified by checking markers of authenticity. In contrast, private bank money, private-key quantum money, and cryptocurrencies are *not* locally verifiable, since they require communication either with an authenticator or a digital ledger. Jevons (1) argued that precious gems were not sufficiently cognizable, since counterfeits were difficult to detect without expertise, which can be viewed as an early evaluation of local verifiability. Finally, note that a scheme cannot have both local verifiability and backup; otherwise, it will be trivial to construct counterfeit bills that pass verification.

Low computational cost. The main computational resources needed to participate in a transaction are the time complexity required to make and verify a transaction, network connectivity, liveliness, storage, memory, and power consumption. Informally, time complexity is the number of computational steps needed to perform or verify a transaction. And liveliness is the requirement that both participants to a transaction be online at least periodically.

Bank deposit transfers via contactless chip debit cards are an example of low computational costliness: all of the power needed is supplied over the air.[8] In contrast, the original Bitcoin client was computationally costly: users had to download the entire blockchain before they could send or receive bitcoins.[9]This, of course, creates a burden for the users, both in terms of the storage requirements and network capacity. Already, in his original manuscript, Nakamoto suggested using a Simplified Verification Protocol (SPV), which would reduce both storage and network communication requirements. The security risks increase only slightly when one uses SPV wallets, rather than a full node. Indeed, SPV is used in most of the recommended mobile Bitcoin clients today, and none of the mobile clients support full validation.[10]

Private (shielded) transactions in ZCash have a high time complexity, storage and communication cost, since users have to download the full block-chain, store it, and perform an intensive computational task using that data (54).

Low pecuniary transaction cost. Some payment instruments, such as bank transfers and credit cards, incur a pecuniary cost in the form of a fee imposed on the sender or receiver. To the contrary, transactions using physical cash do not.

Most cryptocurrencies require the sender to pay a transaction fee. This fee determines the priority with the order is handled. Especially during price surges, transaction fees tend to rise, as the demand for transactions rises. The fee structure differs from that of a credit card transaction, since it depends mostly on the total level of demand in the system, rather than on the amount of the transaction. This is similar to a check, which typically incurs a fixed fee per transaction that is not proportional to the amount.

Private-key quantum money schemes may, in principle, impose a validation fee, depending on the arrangement of the scheme. In contrast, public-key quantum money schemes do not require a third party to participate in the transaction, so no fee could be imposed, as is the case with physical cash.

[8] Chip cards are denoted Integrated Circuit Cards (ICCs) in the EMV specification.

[9] As of October 2021, it is more than 370GB, making it impractical for mobile phones. Source: `https://www.blockchain.com/charts/blocks-size`.

[10] Source: `https://bitcoin.org/en/choose-your-wallet?step=5`.

P2P transfer mechanism. Bech and Garratt (10) categorize forms of money by the mechanism used to transfer value. They define a peer-to-peer mechanism as one where "...transactions occur directly between the payer and the payee without the need for a central intermediary." They also point out that "On a computer network, the peer to-peer concept means that transactions can be processed without the need for a central server."

Portability. Portability is commonly referenced as a necessary property of money (1). The need for portability is likely what lead to the creation of "representative money," such as notes that could be converted into a commodity, to replace the use of the commodity itself as a form of money. While portability might appear to be trivially satisfied for all digital forms of money, it can be hard to achieve in certain cryptocurrency schemes. Until recently, ZCash shielded transactions required access to the entire blockchain, which created substantial storage requirements that could be prohibitive for mobile payments.

Proof of payment. Suppose Alice pays $1 to Mallory, the malicious merchant, to purchase a product. Mallory takes the $1 bill for inspection, secretly replaces it with counterfeit money, and then passes the counterfeit bill to Alice, claiming that the money she paid with was invalid. This form of fraud cannot be done with other forms of payment. For example, with an (idealized) credit card service, there could be no such disagreement between Alice and Mallory, since the credit card company, which is assumed to be honest, serves as an intermediary. More generally, a "proof of payment" protocol can be used to prevent such disagreements. Bitcoin, for example, currently supports such a protocol (55).[11]

On the other hand, public-key quantum money transactions leave no record and, similar to cash, do not offer an obvious means of achieving proof of payment. One possible workaround could be the following. Suppose Alice wants to send $10 of quantum money to Mallory. Instead of sending it all at once, she could divide the payment into 1000 iterations. In each iteration, she would send 1¢and expect a digital signature approving the payment in return. If Mallory fails to provide such a signature, Alice would abort. The worst case scenario is that Alice would not have a proof of payment for 1¢. It is hard to imagine such a process being conducted with physical cash, but electronic forms of money could incorporate it at the protocol level, without most users even being aware of its existence.

Reputation. One determinant of acceptability is the trust that users have in a form of money or in its issuer. As such, reputation or "brand trust" may provide valuable information about a form of money's capacity to function as a medium of exchange and has the advantage of being evaluable prior to issuance. CBDCs, for instance, may be evaluated in terms of a central bank's reputation for maintaining price stability. Similarly, privately-issued digital currencies, such as Facebook's Diem (56) may be evaluated in terms of the issuer's name recognition or reputation for technical prowess.

Reversibility. In general, payment with physical forms of money, such as coins and bills, cannot be reversed unless both parties consent. This differs from digital forms of payment, such as private bank money, transferred via debit transaction, which allows for the reversal of transactions under certain circumstances. Allen et al. (57) discuss a broader term, rectification, which also allows a user to correct information about

[11] As far the authors are aware, the Bitcoin Lightning Network – a second layer built on top of Bitcoin – does not provide a proof of payment.

themselves, and argue that a currency's rectifiability is typically increasing in the extent to which its ledger system is centralized.

With respect to quantum money, public-key schemes do not communicate with a trusted third party and do not leave a record. Thus, reversibility is not possible. Reversibility for private-key quantum money could be introduced, by allowing for an escrow period before settlement, hence, introducing a trade-off with latency.

The reversibility of a CBDC will depend on the scheme that the central bank adopts. In general, schemes that are identity-based and centralized will afford a greater degree of reversibility.

Smart contracts. Buterin (58) describes smart contracts as:

> *... systems which automatically move digital assets according to arbitrary pre-specified rules. For example, one might have a treasury contract of the form "A can withdraw up to X currency units per day, B can withdraw up to Y per day, A and B together can withdraw anything, and A can shut off B's ability to withdraw". (...) What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.*

Bitcoin provides a scripting language which can be used to design simple smart contracts: notable examples include *multi-sig(nature) transactions*, in which the consent of m-out-of-n parties is needed to spend bitcoins; and *atomic cross-chain swaps* (see page 18), which allow Alice and Bob to trade two cryptocurrencies without trusting each other (59).

More expressive platforms, such as Ethereum, allow for greater flexibility, which has enabled the development of decentralized finance (DeFi) and decentralized autonomous organizations (DAOs) (60, 61); however, there are two main disadvantages to adopting an expressive platform: i) bugs, which are extremely hard to rule out in expressive platforms, could result in fraud or reputational damage; and ii) increased platform complexity, which arises in part from the difficulty of correctly calibrating fees to take into account the computational cost for miners or validators.

Allen et al. (57) argue that CBDCs should not offer a scripting language to third-party developers for smart contracts, but should instead hardwire in a limited set of contracts to reduce the prevalence of bugs. Quantum money does not solve the consensus problem or any variant of it, and existing constructions do not provide functionality for smart contracts.

Throughput. In the context of payments, throughput measures the amount of transactions that can be processed in a system at a point in time. It is closely related to the concept of scalability in cryptocurrencies and other forms of digital payment (57). Physical cash faces no bottleneck that limits throughput. Credit card networks, in contrast, do face limitations, but have high rates of throughput. VISA and MasterCard, for instance, have claimed to be able to process 24,000 and 44,000 transactions per second, respectively (62). In contrast, cryptocurrencies are typically low-throughput forms of payment. Bitcoin, for instance, processes at most 7 transactions per second and would need to change its protocol to substantially increase this rate (59).

Finally, public-key quantum money does not rely on any central bottleneck for verification and, thus, could achieve high throughput.

Transferability. Transferability means that a form of money can be either physically or digitally transferred from one owner to another. Some historical forms of money, such as the large stones used on the Island of Yap (63, 64), had transferable ownership, but could not be physically moved. Certain forms of in-game money, such as PokéCoin, may not be resalable and, thus, may either be spent or saved, but not transferred.

Transparency. Transparency can be either involuntary or optional. Since involuntary transparency is the opposite of untraceability, we will focus on the optional case. Zcash provides a clear example of this: users who want anonymity and privacy can have it; however, those who want transparency also have a mechanism for achieving it. Bitcoin also supports a similar notion called "hierarchical deterministic wallets" (59, 65).

Optional transparency allows for the limited and voluntary exchange of information. This might include business partners who want to provide each other transparency with respect to their accounts, but do not want to provide such information to the public at large.

Physical cash does not produce records and cannot provide a mechanism for optional transparency. Bank accounts may offer a view-only permission to users that the account holder selects and, thus, can provide optional transparency. Most CBDC schemes could also provide a similar functionality.

Untraceability. Untraceability (or anonymity) makes it difficult to identify the users that are involved in a transaction (66). Full untraceability is hard to achieve without *privacy*, which entails hiding the existence and details of a transaction. This includes – perhaps most importantly – hiding the amounts involved (67).

Auer and Böhme (68) and Allen et al. (57) argue that there is a fundamental tradeoff in CBDC design between untraceability and anti money laundering compliance. Chaum et al. (20) propose a CBDC scheme that would allow for anonymity while still using the central bank as a trusted third party. Agur et al. (16) argue that CBDCs that focus on anonymity as a core property will tend to be substitutes for cash, rather than bank deposits. The decline of cash might increase the demand for digital forms of money that provide a strong form of untraceability.

Bitcoin has a low level of untraceability as a consequence of its ledger, which is open for everyone to inspect (69). Some cryptocurrencies have improved upon Bitcoin by using various cryptographic techniques. These privacy-enhancing technologies for cryptocurrencies require various trade-offs. For example, ZCash (70, 71) requires a *trusted-setup*, which reduces the level of unforgeability. Additionally, private or "shielded" transactions are four times bigger in size (2KB, instead of 0.5KB[12]). As of August 2021, the number of non-private transactions is an order of magnitude larger than the private transactions transactions.

In a private-key quantum money scheme, the central bank participates in every transaction and, thus, untraceability is not possible. Furthermore, quantum bills used in private-key schemes have unique (classical) serial numbers, so users do not have any privacy or anonymity with respect to the bank. In public-key quantum money schemes, the central bank itself is only involved during the minting and issuance of money, so it provides the same level of privacy and anonymity as physical cash.[13]

[12] Source: `https://z.cash/upgrade/`

[13] A bill has a serial number, which can be used to perform tracking. Consequently, coins afford more privacy and anonymity.

2.2 Standard of Deferred Payment

A standard of deferred payment is a broadly or legally accepted means of repaying debt. While it is often excluded from the list of functions of money, it was discussed in Jevons (1) and may provide a substantial advantage to public money in currency competitions.

Legal tender. While private bank money is a *de facto* acceptable means of discharging debt and paying taxes, central bank issued currencies are typically the only form of money that is *de jure* acceptable and, thus, "legal tender." While having legal tender status is likely to improve the acceptability of a form of money, it does not necessarily imply that it must be legally accepted as payment for goods and services (72).

2.3 Store of Value Function

Jevons (1) and Menger (2) both argued that one function of money was to act as a store of value. That is, goods and services can be converted into money, stored for a period of time, and then converted into other goods and services for the purpose of consumption. This allows producers of perishable goods to sell them immediately and store their value in a medium that does not rapidly depreciate. For a discussion of the store of value property in the economics literature, see (73), (74), and (75).

Anti-theft prevention. Forms of money differ in their capacity to prevent theft. Since theft prevention will depend on the use of best practices and, thus, will vary across users, we do not attempt to rank it across forms of currency. In general, applying the best practices when safeguarding digital forms of money will allow for a high standard of security while having a minimal impact on the money's capacity to carry out its functions. Compare, for instance, the use of one-time passwords for digital money to lockbox banking for commodity money. It is clear that the latter more substantially inhibits money's medium of exchange function. With respect to cryptocurrencies and CBDCs, key management is a particularly important dimension of anti-theft security. Secure hardware, such as hardware wallets, can be used as an effective anti-theft mechanism, but should not be the basis for achieving unforgeability in a currency (57).

Backup. The ability to back up a form of money provides protection against computer failure and loss. Cash and coins cannot be backed up, since they are physical tokens that are not traceable to an individual. Cryptocurrencies, such as Bitcoin, can be backed up by saving a private key. There are, of course, many practical aspects of a good backup system.

Bitcoin, as well as many other cryptocurrencies, support a standardized mnemonic based system (76), and provide the following motivation for it:

> *A mnemonic code or sentence is superior for human interaction compared to the handling of raw binary or hexadecimal representations of a wallet seed. The sentence could be written on paper or spoken over the telephone.*

In addition, Bitcoin supports a passphrase that would be needed to access the backup (77). This adds another layer of security to withstand, for example, an "evil maid attack" from an adversary who gains physical access to the backup.

In contrast, public-key quantum money schemes cannot be backed up, since the quantum states underlying the money cannot be copied and there is no public record of transactions. In principle, a central bank could put a mechanism in place to provide backup for private-key quantum money, such as the scheme introduced in Coladangelo (78).

Durability. Prior to the development of metallic coins, the durability of a form of money was an important consideration. Jevons (1) identifies corn in ancient Greece, olive oil in the Mediterranean, and jewelry in pre-colonial North America as goods that were sufficiently durable to fulfill the functions of money. All digital forms of money that offer a form of backup satisfy a higher standard of durability than is achievable with any physical currency. Those without backup, including quantum money, are as durable as the device on which they are stored. See Taub (79) for a theoretical analysis of durability in the context of commodity money.

Interest-bearing. Physical cash is not associated with an account or a record of ownership and, thus, cannot be interest-bearing; however, competing forms of money, such as bank deposits, cryptocurrencies, and CBDCs do not have an equivalent limitation and could, in principle, bear interest. As Brunnermeier and Niepelt (14) discuss, constructing a CBDC with an interest rate gives the central bank another tool for conducting monetary policy. Furthermore, negative interest rates on CBDCs could be used to extend the effective lower bound (ELB) if physical cash eventually disappears due to lack of demand (10, 80), which could be useful during slow recoveries (81).

An interest-bearing CBDC could also have negative implications for financial stability by disintermediating the financial sector (21); however, some argue that a well-designed CBDC could avoid this (82).[14] Garratt and Zhu (83) argue that an interest-bearing CBDC would put a lower bound on deposit rates, forcing larger banks to increase rates to compete when they could otherwise rely on network effects to lock-in customers. George et al. (84) argue that having the option to adjust the rate on a CBDC would allow the central bank to achieve monetary autonomy and exchange rate stability.

Outside (or inside). Forms of money are said to be either "inside" or "outside."[15] Inside money, such as private bank money, is an asset for the holder and a liability for the issuer. Outside money, such as central bank-issued fiat currency, is an asset for the holder, but is not the liability of any private entity. The distinction between inside and outside money has seen increasing attention in the literature recently, as economists have attempted to describe the properties of new forms of money (10, 12, 14, 85). Most existing quantum money schemes, including both private and public schemes, involve a trusted third party to perform issuance and – for private-key schemes – to perform verification. That entity is typically assumed to be a central bank, but, in principle, could be a private company or organization. As such, quantum money could be produced as either inside or outside money. Note that we use a checkmark in Table 1 to indicate that a form of money is outside money, but do not take an stance on the desirability of the property.

[14] Thus far, central banks have been hesitant to propose CBDC instantiations that include an interest rate, which may indicate that substantial concerns about disintermediation remain.

[15] Alternatively, inside money is sometimes called "private"; whereas, outside money is called "public."

Proof of reserves. This property allows participants (typically exchanges) to attest that they have some reserve that surpasses their liabilities. In cryptocurrencies, this is done by digitally signing a message using all the private keys in their control (59, Section 4.4). A similar functionality could be achieved with bank deposits where a customer could prove her reserve to others by showing her digitally signed bank statement. In the above two examples, note that cheating is still possible by colluding with others who are in control of the money (e.g., by borrowing temporarily).

Scarcity. Scarcity is defined in the context of social wealth by Walras (86) as: "All things, material or immaterial ... that are useful to us and ... only available to us in limited quantity." The scarcity of commodity money primarily refers to its natural abundance and the cost of extracting additional units. The scarcity of fiat currencies, including CBDCs and CBDC-based quantum money, is determined by the central bank's supply rule and the difficulty of counterfeiting. Cryptocurencies, such as Bitcoin, are sufficiently scarce to satisfy this definition.

Supply measurability. Some forms of money, such as cryptocurrencies, can provide accurate measurements of the amount of money in circulation. Central banks also periodically provide measurements of the amount of physical bills and coins minted and put into circulation. In addition to this, some cryptocurrencies are also able to provide information about the projected future path of supply.[16] For example, with Bitcoin, an adversary with the majority of the hashing-power could steal other's people money in certain cases; however, even such an adversary cannot issue more than 21 million bitcoins.

Supply measurability can be hard to achieve, especially in privacy oriented cryptocurrencies, due to "hidden inflation" – an unrecorded increase in the money supply – which could occur due to invalid computational assumptions or bugs in the code.[17] This is not only a theoretical risk: such a flaw occurred in the implementation of ZCash (see Supplementary Material A).[18] Interestingly, there is no definitive way to know whether that bug was exploited, and therefore, what is the total supply of ZCash. In Ethereum, the amount of ether in circulation is known, but there are only few guarantees regarding future amounts.[19]

Tax evadability. From a user perspective, forms of money that do not facilitate the assessment and collection of taxes may be considered more desirable. In the services industry, for example, employees may prefer to receive tips in the form of physical cash to avoid creating a paper or electronic trail that could be used to impose taxes. Additionally, foreign investors operating in a country with a history of financial repression may want to ensure that their funds are not subject to surprise taxes or confiscation. A form of money's tax evadability is positively related to its untraceability and censorship resistance, and inversely related to its level of AML compliance. This tension is an instructive example of the distinction between monetary properties that facilitate functions that provide private value and those that achieve a societal or regulatory function.

[16] The time-inconsistency problem makes such commitments difficult for central banks, since it would sometimes require implementing an undesirable policy at a future date (87).

[17] Note that "inflation" here refers to the amount of money in circulation, rather than the growth rate of the price level.

[18] See `https://electriccoin.co/blog/zcash-counterfeiting-vulnerability-successfully-remediated`.

[19] See EIP-1559.

2.4 Unit of Account Function

Jevons (1) argues that the unit of account or "common measure of value" function of money typically arises as a consequence of its use as a medium of exchange: "Being accustomed to exchange things frequently for sums of money, people learn the value of other articles in terms of money, so that all exchanges will most readily be calculated and adjusted by comparison of the money values of the things exchanged." Brunnermeier et al. (12) argue that the functions of money may become unbundled in the digital era, such that one form of money may serve as the unit of account while rarely being used as a medium of exchange. In this subsection, we will discuss the properties of money that relate to its ability to function as a unit of account.[20]

In digital settings, prices could be presented according to the unit preferred by the user, and exchanging can be done automatically on the merchant's side. In digital forms of money, switching costs may be sufficiently low that they are not an important consideration in determining which currency to hold. In this case, the need for a currency to be a unit of account is diminished (12).

Cost of currency exchange. Every form of money has a cost associated with its exchange into other currencies. This includes the pecuniary costs incurred by the currency exchange, and the pecuniary and non-pecuniary costs incurred by users. Such costs are higher for some forms of money than others, since the difficulty of exchanging currencies is not uniform. In general, exchanges that are digital, involve highly liquid currencies, and entail minimal risk of fraud will tend to have lower costs.

Dyhrberg et al. (91) evaluate the transaction costs and liquidity of Bitcoin. They find that the quoted spreads across the Gdax, Gemini, and Kraken marketplaces average 5.60 to 22.51 basis points (bps). This is considerably lower than spreads in equity markets, but higher than spreads on commonly traded fiat currencies.

A low cost of currency exchange will tend to enhance a currency's capacity to act as a unit of account, since the unit of account will need to be exchanged frequently.

Fungibility. The notion of fungibility is defined in McCloskey (92) as "... a Latin legal term meaning 'such that any unit is substitutable for another' ... A debt can be discharged with any money, not merely moneys from a particular account." Private bank money, central bank reserves, physical cash, and cryptocurrencies all appear to be fungible; however, as Poelstra et al. (93) have argued, this is not as it seems. For instance, different units of Bitcoin contain different exchange histories that are traceable and may be undesirable. Bitcoin exchanges have even blocked the transfer of Bitcoins that originate with theft. In contrast, units of Zcash can be made indistinguishable and, thus, may be considered to be fungible. The greater capacity for non-fungibility in digital currencies could be seen as a positive property that can facilitate the distribution of helicopter drops, government benefits, and loans (57).

Stability. Black et al. (94) defines price stability as "...maintaining the rate of increase or decrease in an aggregate price index, usually the consumer price index, within tolerable limits."

Fiat currencies maintained by independent, inflation-targeting central banks have largely achieved price stability since the 1990s (95).

[20] For a modern treatment of the unit of account function of money, see (88–90).

In contrast, cryptocurrencies, such as Bitcoin, have notoriously suffered from a lack of stability as a consequence of their supply rules (96). This gave rise to demand for cryptocurrencies with low price volatility, referred to as "stablecoins" (97). Stablecoins rely on one of two mechanism to achieve parity with a target currency: 1) an algorithmic supply rule or 2) a guarantee of convertibility into some asset (20, 98). Thus far, asset-backed stablecoins, such as Tether, have demonstrated a greater capacity for achieving price stability (20, 99).[21]

Quantum money does not rely on the use of a distributed ledger and could be issued as a retail CBDC. As such, it could achieve stability properties that are similar to existing fiat currencies.

2.5 Societal or Regulatory Functions

In addition to the original functions introduced in Jevons (1) and Menger (2), forms of money in the digital era have increasingly begun to embody explicit societal and regulatory objectives. Such functions are not necessarily intended to improve user experience and may even make it worse. We consider such functions in this section.

Anti-money laundering (AML) compliant. Levi and Reuter (101) define money laundering as "techniques for hiding proceeds of crime [which] include transporting cash out of the country, purchasing businesses through which funds can be channeled, buying easily transportable valuables, transfer pricing, and using underground banks." Anti-money laundering is a "routinized set of measures to affect criminal revenues passing through the financial system."

According to Allen et al. (57) anti-money laundering (AML) measures are typically based on three types of laws. The first makes money laundering illegal, whether or not the act it conceals is illegal. The second creates reporting requirements for financial institutions, such as Know Your Customer (KYC) rules, which are intended to detect and hinder money laundering. And the third makes it illegal to attempt to circumvent such reporting requirements.

Forms of money vary in their capacity to achieve AML compliance. We define an AML compliant currency as having two properties: 1) the capability to detect and record illicit financial transfers; 2) the technical or administrative capacity to perform detection and reporting. Cash and bank deposits are examples of forms of money with weak and strong AML compliance properties, respectively. Cryptocurrencies, such as Bitcoin, exceed the capacity of even bank deposits along criterion (1), but lack an authority or mechanism for criterion (2).

Money laundering sometimes falls under the umbrella of "financial crimes." We concentrate on money laundering specifically because it is the most studied financial crime in the literature and the techniques used to prevent money laundering are similar to those used to prevent financial crime more generally. A form of money's capacity to collect taxes and enforce liens (57) could be considered closely related properties.

Censorship resistant. Some governments censor certain forms of online communication. In censorship resistant systems, such acts are challenging by design (102). In our context, censorship could take the form of confiscating money or banning transactions (for example, by dissidents). Forms of money in which trusted

[21] Adrian and Mancini-Griffoli (100) discuss how a public-private partnership could improve asset-backed stablecoins further by using central bank reserves as the underlying asset.

third parties are involved, such as bank deposits and certain stable coins[22] are easier to censor compared to those that do not involve third parties, such as cryptocurrencies (103), cash, and public-key quantum money. Allen et al. (57) argue that censorship resistance is typically an increasing function of the extent to which a form of digital money is decentralized.

Identity-based. Identity-based forms of money, such as bank deposits, require participants to use their true identities; whereas other forms of money, such as cash, do not. For digital money, the requirement to reveal one's identity often arises as a result of AML compliance. Identity-based systems also have the advantage of allowing for the cultivation of an individual's reputation. Credit rating is an example of such a reputational mechanism. A variety of different protocols can be used for identity verification, including in-person verification, online verification, proxies, biometric markers, and social trust networks (57).

A closely related and more common division in the economics literature is the distinction between "account-based" and "token-based" forms of money. Demand deposits, for instance, are a type of account-based money. According to Kahn and Roberds (104), who provide an overview of the economics of payment systems, an account-based system must employ two technologies. The first records all actions taken by an account owner and the second verifies accounts. To the contrary, token-based money – sometimes referred to as "value-based" or "store-of-value" money – relies exclusively on a technology that can be used to verify the validity of a given token, such as a commodity or a unit of fiat currency (104). We do not adopt this definition because it does not distinguish between most modern forms of digital money, such as cryptocurrencies and proposed instantiations of CBDCs.

Public. Public money is any form of money that is issued by a government entity. This includes central bank-issued bills and coins, government bonds, and CBDCs. Some have argued that a transition from private money to public money (e.g. private bank money to a CBDC) would result in a credit crunch. Brunnermeier and Niepelt (14) show that this is not necessarily true and identify the conditions under which the equilibrium allocations would be identical after a swap from private to public money.

Resource efficiency. Forms of money differ with respect to the costliness of issuance and maintenance. Public forms of money, such as central bank issued cash and coins, are arguably less efficient than private bank money, but considerably more efficient than commodity money or cryptocurrencies.[23] According to the U.S. Federal Reserve System, for instance, minting a $100 note costs just 14 cents.[24] Furthermore, the entire cost of currency operations at the Board of Governors was less than 1.1 billion USD in 2021.[25] In contrast, bitcoin mining – the process which prevents double spending and mints new bitcoins – is estimated to account for 0.46% of worldwide electricity consumption as of October 2021.[26] Alternatives to Bitcoin's consensus mechanisms that do not require mining have been both proposed and implemented (105).

[22] E.g., Tether has a black-listing mechanism, see Lines 268–305 in their code.

[23] For commodity money and other forms of currency that can be legally mined or minted, we expect the marginal cost of production to be close to the price of the commodity or money.

[24] For a $100 bill, this amounts to 0.14 cents per dollar. Producing a $1 note costs 6.2 cents.

[25] See `https://www.federalreserve.gov/faqs/currency_12771.htm` for an overview of minting costs for different denominations of U.S. currency.

[26] See estimates from the Cambridge Centre for Alternative Finance `https://cbeci.org/`

Unforgeability. Forms of money differ with respect to the security scheme employed and, consequently, the level of protection afforded against counterfeiting. Physical cash employs special threads and inks that are difficult to replicate. For the U.S., for instance, Quercioli and Smith (106) find that counterfeits account for roughly 1 out of every 10,000 bills. In contrast, private bank money relies on cryptographic schemes that make computational assumptions about potential attackers, which may be rendered ineffective by advances in algorithms or hardware. Certain existing forms of encryption, such as RSA, may eventually become vulnerable to attacks from quantum computers, which can perform prime factorization almost exponentially faster than classical computers, using Shor's algorithm (107). Bitcoin is also known to be susceptible to quantum attacks (108).[27]

Private-key quantum money, including Wiesner's original scheme (109), achieves "information-theoretic security," which means that an attacker with unbounded computational resources would still be unable to counterfeit a unit. Here, we assume the adversary receives k valid money states from the bank, applies an arbitrary (perhaps inefficient) quantum computation with these states, and submits $m = poly(n)$ alleged money states to the bank, where n is the number of qubits of the money state. We say that the scheme is secure if the probability of the adversary to pass $k + 1$ or more verifications is negligible in n. Perhaps surprisingly, full security proofs for Wiesner's money were given only 3 decades later (110, 111).

Finally, similar to debit card transactions, public-key quantum money schemes must rely on computational assumptions (24), and are not information-theoretically secure. For example, the construction in Farhi et al. (112) relies on the assumption that a certain computational problem in knot-theory is intractable to quantum computers. The reason is essentially as follows: a computationally unbounded adversary can enumerate over all quantum states (up to some precision ϵ) and check whether it passes verification. Since the verification procedure is public, this does not require any cooperation from the bank. Notice that the same approach would not work for private money, since the bank would accept only polynomially-many states from the adversary for verifications; whereas brute-force attacks, such as this one, would require exponentially many attempts. This is essentially the same reason why guessing a short random password takes an exponentially long time.

3 Properties of Currency Pairs and Groups

In some cases, properties of money extend to a pair of currencies or a group of currencies. We consider five such properties in this section. For the sake of simplicity, we do not categorize pairwise and group properties according to function, and do not attempt to determine whether they apply to each combination of currencies in Table 1.

Atomic swaps. The vulnerability of cryptocurrency exchanges to hacking (113, 114) has given rise to demand for an intermediary-free form of cryptocurrency exchange. A technique called an *atomic swap* enables such exchanges between cryptocurrencies through the use of smart contracts. (59, Chapter 10.5). Such technology could also potentially be used in CBDCs to allow for peer-to-peer foreign currency exchange.

[27] In the context of digital currencies, Allen et al. (57) argue that the structure of the digital ledger determines the protection a form of digital money can provide against counterfeiting attempts. Common architectures include full decentralization, role separation, trust dispersal, and threshold trust. See (57) for definitions of the terms.

Interoperability. In the context of cryptocurrencies, interoperability refers to the existence of protocols that allow two independent digital ledger systems to interact through the use of smart contracts (57, 115, 116). Allen et al. (57) propose a notion of interoperability that would allow for a two-layer CBDC. The central bank would manage a layer that corresponds to reserves and has only basic functionality. Commercial banks would then manage a retail layer that contains more customer-centric functionality, but is ultimately backed by holdings in the reserve layer.

Cross-border payments. Allen et al. (57) argue that private digital currencies, such as cryptocurrencies, may improve the efficiency of cross-border payments, since they can potentially improve tracking and can eliminate the need for multiple financial intermediaries to be involved in a transfer. The BIS has also argued that improvements in cross-border payments could be facilitated by making CBDCs interoperable (117).

Uniformity. Uniformity between multiple currencies can be achieved by guaranteeing convertibility at a fixed rate between one currency and another. This allows one currency to take on another currency's store of value and unit of account properties. Brunnermeier et al. (12) point out private bank money (e.g. demand deposits) as an example of a currency that achieves this property. They also argue that the issuance of CBDCs could extend public money to substantially larger group, ensuring the uniformity of money in the era of digitization. Since quantum money could also be issued by central banks, possibly as a form of CBDC, it could also achieve uniformity with physical cash and private bank money. Stablecoins which are pegged to a single currency, such as the US dollar, may also achieve uniformity.

4 Discussion

After an extended period of dominance in the 20th century, national forms of public money have fallen out of favor as a medium of exchange, losing market share to private bank money, even as they retain their status as the preferred unit of account. In the emerging era of intense digital currency competition, central banks have the opportunity to regain control over the medium of exchange through CBDC issuance, but face the threat of losing control over the unit of account to a multi-currency stablecoin, a competing central bank, a digital currency area (12), or a cryptocurrency. Such an event would have substantial implications for monetary policy, financial stability, and regulation. As such, the conservative inclinations of central banks, which normally play a stabilizing role, could instead lead to loss of relevance for public money.

The emergence of new forms of public and private money raises questions about what properties of money are most beneficial in the modern era. Central banks appear to have concluded that new forms of public money need to be digital, but beyond that, there is less agreement on what other properties are desirable. Furthermore, the use of a digital medium opens up the possibility of embedding new supervisory and regulatory functions into money, which may be desirable from a societal perspective, but not from the perspective of an individual user. Our intention in this paper was to provide an overview of this emerging landscape that updates the functions-and-properties framework of money, and that could be useful for both researchers and currency designers.

Acknowledgments O.S. is supported by the Israeli Science Foundation (ISF) grant No. 682/18 and 2137/19, and by the Cyber Security Research Center at Ben-Gurion University.

A Appendix

Below, we provide additional detail about some of the potentially less familiar currencies listed in Table 1.

CBDC (No mature instantiation). Since CBDCs lack a mature instantiation, we considered a generic case where the properties were determined by hard technical constraints, and common legal and institutional restrictions on central banks.

In-Game Currency (PokéCoin). In-game currency is one of the main drivers of game mechanics. Spending on mobile games alone has been estimated to have reached $79 billion globally in 2020.[28] PokéCoin is the virtual in-game currency used in the Pokémon GO game.

Cryptocurrency (Bitcoin). Bitcoin is an electronic payment system (52, 59). Its censorship resistance and global accessibility are achieved mainly by its p2p architecture. Unlike previous e-payment systems, the Bitcoin network was the first to issue its own form of outside money via a process called mining. Mining provides the distribution mechanism of newly minted bitcoins, but even more importantly, plays a crucial role in securing the network against double-spending attacks.

Cryptocurrency with DApps (Ethereum). Decentralized applications (DApps) are software that can be executed on the blockchain. DApps have enabled the development of decentralized financial services, which allow for lending and borrowing without an intermediary (other than the blockchain). Ethereum is a cryptocurrency oriented towards smart contracts.

Privacy Oriented Cryptocurrency (Zcash). Zcash is a cryptocurrency that allows users to enhance the privacy of transactions (71). Each transaction is either "transparent" or "shielded." The transparent transactions provide a level of privacy that is similar to Bitcoin; whereas the shielded transactions use a cryptographic protocol that involves zero-knowledge proofs to provide enhanced anonymity and privacy for transactors. Gross et al. (118) propose the use of a Zcash-like shielding mechanism in a CBDC.

Stablecoin (Tether ERC-20 USD). A stablecoin is a type of cryptocurrency that attempts to achieve reduced price volatility. Tether ERC-20 USD is a stablecoin that is pegged to the value of the U.S. dollar (USD). Tether Limited, which issues the cryptocurrency, claims that its tokens are fully backed by USD reserves. ERC-20 is a protocol that is used for the Ethereum network. A unit of Tether ERC-20 USD is a token, which can be exchanged over the Ethereum blockchain.

[28] See `https://sensortower.com/blog/app-revenue-and-downloads-2020`.

Private-Key Quantum Money (Wiesner's scheme [no realization]). The first quantum money scheme was introduced by Wiesner (109). In a private-key scheme, only the bank branches or the central bank can verify the money, using the bank's secret key (vis-à-vis Public-Key Quantum Money).

Wiesner's scheme uses the No-Cloning Theorem (119) to construct physically unforgeable money, something which is not possible without exploiting quantum phenomena. The scheme was partially implemented in a laboratory setting by Bozzio et al. (120), but faces substantial technical barriers to a full implementation. See Hull et al. (8) for a complete description of Wiesner's scheme.

Public-Key Quantum Money (Farhi et al. scheme [no realization]). Public-key quantum money, a term introduced in (53), refers to quantum money schemes with a publicly available key (algorithm) that can be used to perform counterfeiting detection. This would allow for local verification of money without the involvement of a trusted third party, something which is not possible with digital forms of classical (non-quantum) money. The scheme by Farhi et al. (112) is based on knot theory. See Hull et al. (8) for a summary of the scheme.

B Figures

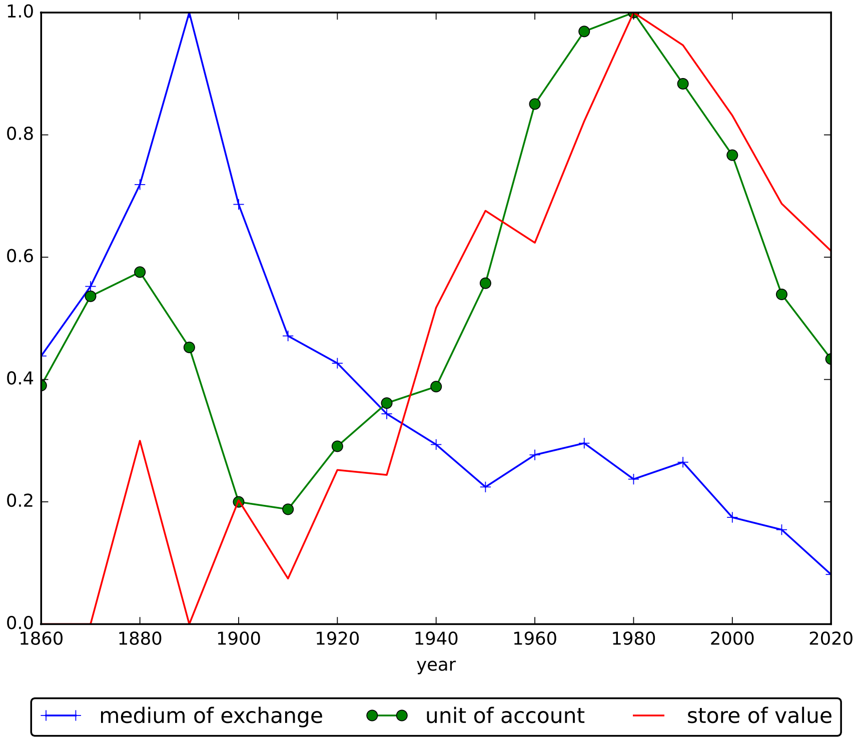

Figure 1: The figure above shows phrase frequencies for the different functions of money in journal articles and books for the 1860-2020 period. Each series is normalized by the n-gram count for "money" and is then divided by its maximum value. The n-gram count data was generated by JSTOR Constellate.

References

[1] W Jevons, *Money and the Mechanism of Exchange.* (D. Appleton and Co., New York), (1876).

[2] K Menger, On the origin of money. *The Economic Journal* **2**, 239–255 (1892).

[3] W Metcalf, *The Oxford handbook of Greek and Roman coinage.* (Oxford University Press, Oxford New York), (2012).

[4] E Wilkinson, *Chinese History: A New Manual.* (Harvard-Yenching Institute Monograph Series), (2013).

[5] D Hartill, *Cast Chinese coins: a historical catalogue.* (New Generation Publishing, London), (2017).

[6] C Boar, H Holden, A Wadsworth, Impending arrival - a sequel to the survey on central bank digital currency (2020).

[7] C Barontini, H Holden, Proceeding with caution – a survey on central bank digital currency, (BIS), Working Paper No. 101 (2019).

[8] I Hull, O Sattath, E Diamanti, G Wendin, Quantum Technology for Economists, (Sveriges Riksbank), Working Paper Series 398 (2020).

[9] T Khiaonarong, D Humphrey, Cash Use Across Countries and the Demand for Central Bank Digital Currency, (International Monetary Fund), IMF Working Papers 2019/046 (2019).

[10] M Bech, R Garratt, Central bank cryptocurrencies (BIS Working Paper) (2017).

[11] D Andolfatto, Assessing the impact of central bank digital currency on private banks, (Federal Reserve Bank of St. Louis, `https://doi.org/10.20955/wp.2018.026`), Working Paper No. 2018-026B (2018).

[12] MK Brunnermeier, H James, JP Landau, The digitalization of money, (National Bureau of Economic Research), Working Paper 26300 (2019).

[13] B Eichengreen, From commodity to fiat and now to crypto: What does history tell us?, (NBER), Working Paper No. 25426 (2019).

[14] M Brunnermeier, D Niepelt, On the equivalence of private and public money. *Journal of Monetary Economics* **106**, 27–41 (2019).

[15] R Kroszner, Currency competition in the digital age in *Evolution and Procedures in Central Banking.* (2011).

[16] I Agur, A Ari, G Dell'Ariccia, Designing central bank digital currencies, (International Monetary Fund), Working paper no. 19/252 (2019).

[17] MM Ferrari, A Mehl, L Stracca, Central bank digital currency in an open economy, (European Central Bank), Working Paper Series 2488 (2020).

[18] M Bordo, A Levin, Central bank digital currency and the future of monetary policy, (NBER), Working Paper No. 23711 (2017).

[19] P Benigno, L Schilling, H Uhlig, Cryptocurrencies, currency competition, and the impossible trinity, (NBER Working Paper No. 26214), Technical report (2019).

[20] D Chaum, C Grothoff, T Moser, How to issue a central bank digital currency. *SNB Working Papers* **3** (2021).

[21] YS Kim, O Kwon, Central Bank Digital Currency and Financial Stability, (Economic Research Institute, Bank of Korea), Working Papers 2019-6 (2019).

[22] F Hayek, *Denationalisation of money: the argument refined: an analysis of the theory and practice of concurrent currencies.* (Institute of Economic Affairs, London), (1990).

[23] A Martin, SL Schreft, Currency competition : a partial vindication of Hayek, (Federal Reserve Bank of Kansas City), Research Working Paper RWP 03-04 (2003).

[24] S Aaronson, P Christiano, Quantum money from hidden subspaces. *Proceedings of the 44th Symposium on Theory of Computing* **ACM**, 41–60 (2012).

[25] N Wallace, The overlapping-generations model of fiat money, (Federal Reserve Bank of Minneapolis), Staff Report 37 (1980).

[26] N Kiyotaki, R Wright, On money as a medium of exchange. *Journal of Political Economy* **97**, 927–954 (1989).

[27] S Oh, A theory of a generally acceptable medium of exchange and barter. *Journal of Monetary Economics* **23**, 101 – 119 (1989).

[28] N Kiyotaki, R Wright, A search-theoretic approach to monetary economics. *American Economic Review* **83**, 63–77 (1993).

[29] S Williamson, R Wright, Barter and monetary exchange under private information. *The American Economic Review* **84**, 104–123 (1994).

[30] R Lagos, Asset prices and liquidity in an exchange economy. *Journal of Monetary Economics* **57**, 913–930 (2010).

[31] P Brown, Experimental evidence on money as a medium of exchange. *Journal of Economic Dynamics and Control* **20**, 583 – 600 (1996).

[32] J Duffy, J Ochs, Emergence of money as a medium of exchange: An experimental study. *American Economic Review* **89**, 847–877 (1999).

[33] G Selgin, On ensuring the acceptability of a new fiat money. *Journal of Money, Credit and Banking* **26**, 808–826 (1994).

[34] N Wallace, Acceptability, means of payment, and media of exchange, (Federal Reserve Bank of Minneapolis), Quarterly review (1992).

[35] A Shevchenko, R Wright, A simple search model of money with heterogeneous agents and partial acceptability. *Economic Theory* **24**, 877–885 (2004).

[36] O Bjerg, Designing new money - the policy trilemma of central bank digital currency, (SSRN, `http://dx.doi.org/10.2139/ssrn.2985381`), Working paper (2017).

[37] E Nosal, N Wallace, A model of (the threat of) counterfeiting. *Journal of Monetary Economics* **54**, 994–1001 (2007).

[38] N Wallace, Chapter 1 - the mechanism-design approach to monetary theory in *Handbook of Monetary Economics*, eds. BM Friedman, M Woodford. (Elsevier) Vol. 3, pp. 3–23 (2010).

[39] TW Hu, Imperfect recognizability and coexistence of money and higher-return assets. *Economic Theory* **53**, 111–138 (2013).

[40] R Radian, O Sattath, Semi-quantum money in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT 2019, Zurich, Switzerland, October 21-23, 2019.* (ACM), pp. 132–146 (2019).

[41] A Coladangelo, O Sattath, A quantum money solution to the blockchain scalability problem (2020).

[42] A Behera, O Sattath, Almost public coins (2020).

[43] B Roberts, M Zhandry, Franchised quantum money (2020).

[44] M Lee, N Wallace, Optimal divisibility of money when money is costly to produce. *Review of Economic Dynamics* **9**, 541–556 (2006).

[45] A Redish, *Bimetallism: An Economic and Historical Analysis.* (Cambridge University Press), (2000).

[46] T Sargent, F Velde, *The Big Problem of Small Change.* (Princeton University Press), (2002).

[47] R Lipton, R Ostrovsky, Micropayments via efficient coin-flipping in *Financial Cryptography, Second International Conference, FC'98, Anguilla, British West Indies, February 23-25, 1998, Proceedings*, Lecture Notes in Computer Science, ed. R Hirschfeld. (Springer), Vol. 1465, pp. 1–15 (1998).

[48] S Micali, R Rivest, Micropayments revisited in *Topics in Cryptology - CT-RSA 2002, The Cryptographer's Track at the RSA Conference, 2002, San Jose, CA, USA, February 18-22, 2002, Proceedings*, Lecture Notes in Computer Science, ed. B Preneel. (Springer), Vol. 2271, pp. 149–163 (2002).

[49] B Cohen, Incentives build robustness in BitTorrent in *Workshop on Economics of Peer-to-Peer systems.* Vol. 6, (2003).

[50] S Jun, M Ahamad, Incentives in bittorrent induce free riding in *Proceedings of the 2005 ACM SIGCOMM Workshop on Economics of Peer-to-Peer Systems*, P2PECON '05. (Association for Computing Machinery, New York, NY, USA), p. 116–121 (2005).

[51] X Gao, G Clark, J Lindqvist, Of two minds, multiple addresses, and one ledger: Characterizing opinions, knowledge, and perceptions of bitcoin across users and non-users in *CHI 2016 - Proceedings, 34th Annual CHI Conference on Human Factors in Computing Systems*, Conference on Human Factors in Computing Systems - Proceedings. (Association for Computing Machinery), pp. 1656–1668 (2016).

[52] S Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2008).

[53] S Aaronson, Quantum copy-protection and quantum money. *Conference on Computational Complexity* **IEEE**, 229–242 (2009).

[54] P Peterson, Reducing shielded proving time in sapling (Electric Coin Co. blog post, `https://electriccoin.co/blog/reducing-shielded-proving-time-in-sapling/`) (2018).

[55] G Andresen, M Hearn, Payment protocol (Bitcoin Improvement Proposal (BIP) 70 `https://github.com/bitcoin/bips/blob/master/bip-0070`) (2013).

[56] TL Association, Whitepaper v2.0 (2021).

[57] S Allen, et al., Design choices for central bank digital currency: Policy and technical considerations, (Institute of Labor Economics (IZA), Bonn), IZA Discussion Papers 13535 (2020).

[58] V Buterin, A next-generation smart contract and decentralized application platform (White paper.) (2014).

[59] A Narayanan, J Bonneau, EW Felten, A Miller, S Goldfeder, *Bitcoin and Cryptocurrency Technologies - A Comprehensive Introduction.* (Princeton University Press), (2016).

[60] V Buterin, Bootstrapping a decentralized autonomous corporation: Part i (2013).

[61] M Verduyn, *Bitcoin and beyond: cryptocurrencies, blockchains, and global governance.* (Routledge, Taylor & Francis Group, London New York), (2018).

[62] S Herbst-Murphy, Clearing and settlement of interbank card transactions: A mastercard tutorial for federal reserve payments analysts, (Federal Reserve Bank of Philadelphia), Payments center discussion paper (2013).

[63] W Furness, *The Island of Stone Money: Uap of the Carolines.* (J.B. Lippincott Co., Philadelphia), (1910).

[64] M Friedman, The island of stone money, (Stanford, California: Hoover Institution), Working papers in economics, no. e-91-34 (1991).

[65] P Wuille, Hierarchical deterministic wallets (Bitcoin Improvement Proposal (BIP) 32 `https://github.com/bitcoin/bips/blob/master/bip-0032`) (2013).

[66] D Chaum, A Fiat, M Naor, Untraceable electronic cash. *Advances in Cryptology - Proc. CRYPTO '88, LNCS* **403**, 319–327 (1988).

[67] S Athey, I Parashkevov, V Sarukkai, J Xia, Bitcoin pricing, adoption, and usage: Theory and evidence, (Stanford University Graduate School of Business), Research Paper No. 16-42 (2016).

[68] R Auer, R Böhme, The technology of retail central bank digital currency (BIS Working Paper) (2020).

[69] D Ron, A Shamir, Quantitative analysis of the full bitcoin transaction graph in *Financial Cryptography and Data Security - 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers*, Lecture Notes in Computer Science, ed. A Sadeghi. (Springer), Vol. 7859, pp. 6–24 (2013).

[70] E Ben-Sasson, et al., Zerocash: Decentralized anonymous payments from bitcoin in *2014 IEEE Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 2014.* (IEEE Computer Society), pp. 459–474 (2014).

[71] D Hopwood, S Bowe, T Hornby, N Wilcox, Zcash protocol specification (Technical report, `https://raw.githubusercontent.com/zcash/zips/master/protocol/protocol.pdf`) (2016).

[72] Board of Governors of the Federal Reserve System, Is it legal for a business in the united states to refuse cash as a form of payment? (`https://www.federalreserve.gov/faqs/currency_12772.htm`) (2020) Accessed: 2021-03-09.

[73] J Tobin, Money and economic growth. *Econometrica* **33**, 671–684 (1965).

[74] P Davidson, Money and the real world. *The Economic Journal* **82**, 101–115 (1972).

[75] P Weil, Confidence and the real value of money in an overlapping generations economy. *The Quarterly Journal of Economics* **102**, 1–22 (1987).

[76] M Palatinus, P Rusnak, A Voisine, S Bowe, Mnemonic code for generating deterministic keys (Bitcoin Improvement Proposal (BIP) 39 `https://github.com/bitcoin/bips/blob/master/bip-0039`) (2013).

[77] M Caldwell, A Voisine, Passphrase-protected private key (Bitcoin Improvement Proposal (BIP) 38 `https://github.com/bitcoin/bips/blob/master/bip-0038`) (2012).

[78] A Coladangelo, Smart contracts meet quantum cryptography (Working paper.) (2019).

[79] B Taub, Equilibrium traits of durable commodity money. *Journal of Banking and Finance* **9**, 5–34 (1985).

[80] P Beniak, Central bank digital currency and monetary policy: a literature review, (University Library of Munich, Germany), MPRA Paper 96663 (2019).

[81] R Agarwal, M Kimball, Enabling deep negative rates to fight recessions: A guide, (International Monetary Fund (IMF)), Working paper no. 19/84 (2019).

[82] D Andolfatto, Assessing the Impact of Central Bank Digital Currency on Private Banks, (Federal Reserve Bank of St. Louis), Working Papers 2018-026 (2018).

[83] R Garratt, H Zhu, On Interest-Bearing Central Bank Digital Currency with Heterogeneous Banks (2021).

[84] A George, T Xie, J Alba, Central Bank Digital Currency with Adjustable Interest Rate in Small Open Economies (2021).

[85] Y Zhu, S Hendry, A framework for analyzing monetary policy in an economy with e-money, (SSRN), Working paper (2019).

[86] L Walras, *Elements of Pure Economics, or the Theory of Social Wealth.* (London: George Allen & Unwin, 1954. Reprinted, Fairfield: A.M. Kelley, 1977.), (1926) Translated by William Jaffé.

[87] R Moessner, DJ Jansen, J de Haan, Communication about future policy rates in theory and practice: A survey. *Journal of Economic Surveys* **31**, 678–711 (2017).

[88] M Mussa, The welfare cost of inflation and the role of money as a unit of account. *Journal of Money, Credit and Banking* **9**, 276–286 (1977).

[89] L White, Competitive payments systems and the unit of account. *The American Economic Review* **74**, 699–712 (1984).

[90] M Doepke, M Schneider, Money as a unit of account. *Econometrica* **85**, 1537–1574 (2017).

[91] A Dyhrberg, S Foley, J Svec, How investible is bitcoin? analyzing the liquidity and transaction costs of bitcoin markets. *Economics Letters* **171**, 140–143 (2018).

[92] D McCloskey, *Fungibility.* (Palgrave Macmillan UK, London), pp. 1–1 (2016).

[93] A Poelstra, A Back, M Friedenbach, G Maxwell, P Wuille, Confidential assets in *Financial Cryptography and Data Security - FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Nieuwpoort, Curaçao, March 2, 2018, Revised Selected Papers*, Lecture Notes in Computer Science, eds. A Zohar, et al. (Springer), Vol. 10958, pp. 43–63 (2018).

[94] J Black, N Hashimzade, G Myles, Price stability (2009).

[95] L Svensson, Inflation targeting in *Handbook of Monetary Economics*, eds. B Friedman, M Woodford. (Elsevier) Vol. 3b, (2010).

[96] G7, Investigating the impact of global stablecoins (Bank for International Settlements) (2019).

[97] H Hassani, X Huang, E Silva, Banking with blockchain-ed big data. *Journal of Management Analytics* **5**, 256–275 (2018).

[98] M Mita, K Ito, S Ohsawa, H Tanaka, What is stablecoin?: A survey on price stabilization mechanisms for decentralized payment systems (2019).

[99] U Chohan, Are stable coins stable?, (Elsevier BV), SSRN electronic journal (2019).

[100] T Adrian, T Mancini-Griffoli, The rise of digital money. *IMF Fintech Notes* **19/01** (2019).

[101] M Levi, P Reuter, Money laundering. *Crime and Justice* **34**, 289–375 (2006).

[102] S Khattak, et al., Sok: Making sense of censorship resistance systems. *Proc. Priv. Enhancing Technol.* **2016**, 37–61 (2016).

[103] N Weaver, Risks of cryptocurrencies. *Commun. ACM* **61**, 20–24 (2018).

[104] C Kahn, W Roberds, Why pay? an introduction to payments economics. *Journal of Financial Intermediation* **18**, 1–23 (2009).

[105] Y Xiao, N Zhang, W Lou, YT Hou, A survey of distributed consensus protocols for blockchain networks. *IEEE Commun. Surv. Tutorials* **22**, 1432–1465 (2020).

[106] E Quercioli, L Smith, The economics of counterfeiting. *Econometrica* **83**, 1211–1236 (2015).

[107] P Shor, Algorithms for quantum computation: Discrete logarithms and factoring in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, SFCS '94. (IEEE Computer Society, Washington, DC, USA), pp. 124–134 (1994).

[108] S Aggarwal, G Brennen, T Lee, M Santha, M Tomamichel, Quantum attacks on bitcoin, and how to protect against them. *Ledger* **3** (2018).

[109] S Wiesner, Conjugate coding. *ACM Sigact News* **15**, 78–88 (1983).

[110] F Pastawski, et al., Unforgeable noise-tolerant quantum tokens. *Proceedings of the National Academy of Sciences of the United States of America* **109**, 16079–16082 (2012).

[111] A Molina, T Vidick, J Watrous, Optimal counterfeiting attacks and generalizations for wiesner's quantum money in *Theory of Quantum Computation, Communication, and Cryptography, TQC 2012*, Lecture Notes in Computer Science, eds. K Iwama, Y Kawano, M Murao. (Springer), Vol. 7582, pp. 45–64 (2012).

[112] E Farhi, et al., Quantum money from knots. *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference* **ACM** (2012).

[113] P Thompson, Most significant hacks of 2019 — new record of twelve in one year (2020).

[114] Selfkey.org, A comprehensive list of cryptocurrency exchange hacks (2020).

[115] Z Liu, et al., Hyperservice: Interoperability and programmability across heterogeneous blockchains in *CCS 2019 - Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, Proceedings of the ACM Conference on Computer and Communications Security. (Association for Computing Machinery), pp. 549–566 (2019).

[116] AE Gencer, R van Renesse, EG Sirer, Service-oriented sharding with aspen (2016).

[117] B for International Settlements, Central bank digital currencies for cross-border payments (2021).

[118] J Gross, J Sedlmeir, M Babel, A Bechtel, B Schellinger, Designing a Central Bank Digital Currency with Support for Cash-Like Privacy (2021).

[119] W Wootters, W Zurek, A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982).

[120] M Bozzio, et al., Experimental investigation of practical unforgeable quantum money. *npj Quantum Information* **4** (2018).