SUERF
The European Money and Finance Forum

SUERF Policy Brief
No 273, February 2022

Revisiting the Properties of Money


By Isaiah Hull and Or Sattath*

Keywords: Money, CBDC, digital currencies, quantum money, currency competition.

The canonical functions-and-properties of money framework was introduced in the late 1800s by Jevons (1876) and Menger (1892). It was primarily intended to describe physical currencies, such as commodity money, metallic coins, and paper bills. While it proved to be a reliable and enduring set of criteria over the century that followed, it is no longer clear that it meaningfully describes the properties of money in the digital era. In this policy brief, we will discuss recent work by Hull and Sattath (2021), which provides a comprehensive update to the Jevons-Menger framework, drawing from both the economics and computer science literatures.

* **Isaiah Hull**, Sveriges Riksbank; **Or Sattath**, Ben-Gurion University of the Negev.

The Emerging Era of Currency Competition

During much of the 20th century, public money held a special status as the default form of payment. This eroded with the rise of private bank money, which displaced physical cash as the preferred medium of exchange. Since private bank money is uniform with public money, central banks maintained control over the unit of account, but never regained influence over money's role in retail payments.

This separation of monetary functions is unusual, as the unit of account role has historically been held by the dominant medium of exchange. This was observed as early as Jevons (1876). As Brunnermeier et al. (2019) argue, the features of money have become unbundled and are likely to experience further unbundling during the digital era. This could mean an even greater erosion in the relevance of public money if national currencies face strong competition for the unit of account role.

Until recently, central banks were reluctant to respond to their declining role in retail payments; however, many have recently begun projects to restore public money in some form (Boar et al. 2019; Barontini and Holden 2019). There is broad agreement that such money must be digital to compete in the modern payments system, but there is otherwise no consensus on what other properties are desirable. Hull and Sattath (2021) examine the set of all properties a digital currency can embody, focusing on hard and soft tradeoffs that are inherent in design choices. We provide a selection of illustrative properties in the sections below.

A Medium of Exchange for the 21st Century

Properties like durability, fungibility, stability, and acceptability were what constituted a viable medium of exchange candidate in the 1800s. It is unclear, however, whether such properties remain sufficient to describe desirable forms of money in the 21st century. Additionally, while most of the Jevons-Menger properties were unambiguously positive, many of the properties of digital currencies involve hard or soft tradeoffs.

Table 1 provides a summary of the main properties of money identified in Hull and Sattath (2021) and their embodiment in currencies. The rows list the properties and the columns provide representative currencies for each category of money. The paper defines and discusses each these properties and example currencies in detail.

An example of a modern property that entails a hard tradeoff is backup, which permits a user to store copies of money, allowing for recovery in the event of loss or device failure. This might appear to be an unambiguously positive property, but including backup precludes local verification, a property introduced by Aaronson (2009) that permits counterfeit detection without the involvement of a trusted third party. Including both features in a single currency makes counterfeiting trivial, which forces a currency designer to select one or the other.

Reversibility is another modern property that appears to be unambiguously positive on initial inspection, but, in fact, entails a tradeoff. Allowing for transactions to be reversed under certain circumstances provides users with recourse against fraud and scams. Card payments, for instance, may allow for the reversal of transactions without consent from both parties; whereas payment with physical currencies can only be reversed if both parties agree. While reversibility can make a payment instrument more attractive, it will necessarily increase latency – that is, the amount of time it takes a transaction to settle.

Another tradeoff involves the traceability of money: that is, the amount of information available about transactions and transactors. Whereas transactions involving physical currency do not automatically generate records and, thus, have a low degree of traceability, digital payments – including cryptocurrencies – often

produce a digital trail that can be used to identify the transactors and the amount transacted. Bitcoin, for instance, has a high level of traceability as a consequence of its public ledger (Ron and Shamir 2013). ZCash, in contrast, offers shielded transactions that explicitly aim to reduce traceability.

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	✔	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	✔
	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, and a ? indicates that we are uncertain whether the property will hold.

As Auer and Böhme (2020) and Allen et al. (2020) argue, there is a fundamental tradeoff between financial crime prevention and untraceability. Furthermore, if achieving untraceability requires the sacrifice of automatic record-keeping, it may also make it difficult to replicate the convenience of digital payments. Consequently, as Agur et al. (2019) argues, making untraceability a core feature of money risks transforming it into a cash substitute, rather than a digital currency substitute. For central banks, this could achieve the opposite of what is intended with a central bank digital currency (CBDC).

Thus, with respect to modern currencies, selecting and implementing a set of properties is not merely a technical problem. It involves navigating a set of tradeoffs that will determine who uses the currency for what purpose. If the objective is to provide a widely transacted form of money, then it may not be optimal to select a set of properties that is appealing to a small subset of users if they induce tradeoffs with properties valued by the general population.

A New Function for Money and its Role in Currency Competition

The Jevons-Menger framework describes money as serving as a medium of exchange, a store of value, and a unit of account. The updated framework in Hull and Sattath (2021) adds societal and regulatory functions, which have grown in importance and application in the digital era. This function of money differs from the other three in that it is not directly concerned with the experience of transactors; rather, it uses money design as a means of achieving other societal objectives.

One example of a property that falls under this new function is anti-money laundering compliance. Constructing a form of money that offers strong money laundering detection and compliance properties will entail increasing its traceability. This will diminish the experience of legitimate transactors who would prefer to have more privacy or anonymity. Such tradeoffs could be especially challenging for central banks to navigate, since they may feel compelled to adopt properties that achieve societal and regulatory goals, even if they make the currency less competitive in the process.

Some private currencies also have societal objectives. Cryptocurrencies, for instance, are designed to be censorship resistant (Khattak et al. 2016). This contrasts with private bank money, which can be censored by authorities that want to prevent certain users from transacting in the financial system. As argued by Allen et al. (2020), a currency's capacity for censorship resistance is directly related to its degree of decentralization. As such, achieving the societal goal of providing censorship resistance – for instance, by replacing a trusted third party with a digital ledger – may require a degree of decentralization that induces unappealing tradeoffs from the perspective of users.

As competition heightens between public money, private bank money, and other private digital currencies, constraints related to societal and regulatory functions may advantage one form of money over another. This may raise the question of whether currencies that are at a disadvantage can afford to sustain such objectives. Alternatively, societal functions that are seen as critically important to preserve, such as the capacity to detect and disrupt terrorism financing, could ultimately be imposed as a regulation on all digital currencies. This might appear to level the playing field, but it would also disadvantage forms of money that have a competing societal objective.

Conclusion

The era of public currency dominance ended with the rise of private bank money. In many countries, public money is now the preferred unit of account, but plays only a secondary role in retail payments. The forthcoming era is likely to witness further unbundling of the functions of money, as well as growth in the importance of monetary properties that have not yet been extensively explored in the economics literature.

Many of these new properties of money, which are described in Hull and Sattath (2021), entail tradeoffs that are non-trivial for users. As such, a currency supplier must decide which properties are essential from the

perspective of its users, rather than attempting the infeasible task of creating money that embodies all desired properties. This, we expect, will determine how well a currency performs in the competitive era on the horizon.

In addition to the proliferation of new forms of money and new properties, money also has a new function, which is to achieve societal and regulatory objectives. This function has grown in importance in the digital era and may place constraints on the performance of both public and private currencies.

References

Aaronson, S. (2009). Quantum Copy-Protection and Quantum Money. *Conference on Computational Complexity* (pp. 229-242). IEEE.

Agur, I., Ari, A., & Dell'Ariccia, G. (2019). Designing Central Bank Digital Currencies. *Working Paper No. 19/252*.

Allen, S., & others. (2020). Design Choices for Central Bank Digital Currency: Policy and Technical Considerations. *IZA Discussion Papers*.

Auer, R., & Böhme, R. (2020). The technology of retail central bank digital currency. *BIS Working Paper*.

Barontini, C., & Holden, H. (2019). Proceeding with Caution -- A Survey on Central Bank Digital Currency. *BIS Papers*.

Boar, C., Holden, H., & Wadsworth, A. (2020). Impending arrival - a sequel to the survey on central bank digital currency. *BIS Papers*.

Brunnermeier, M., James, H., & Landau, J. (2019). The Digitalization of Money. *National Bureau of Economic Research*.

Hull, I., & Sattath, O. (2021). Revisiting the Properties of Money. *Sveriges Riksbank Working Paper Series No. 406*.

Jevons, W. (1876). Money and the Mechanism of Exchange. New York: D. Appleton and Co.

Khattak, S., & others, a. (2016). SoK: Making Sense of Censorship Resistance Systems. *Proceedings on Privacy Enhancing Technologies.* Warsaw: De Gruyter Poland.

Menger, K. (1892). On the Origin of Money. *The Economic Journal*, 239-255.

Ron, D., & Shamir, A. (2013). Quantitative Analysis of the Full Bitcoin Transaction Graph. *Financial Cryptography and Data* (pp. 6-24). Springer.

About the authors

Isaiah Hull *is a senior economist at the Research Division of Sveriges Riksbank. His research is focused on computational economics, including applications of machine learning and quantum technology.*

Or Sattath *is an assistant professor of computer science at Ben-Gurion University of the Negev. His research interests include quantum cryptography and quantum computing.*

SUERF Publications

Find more **SUERF Policy Briefs** and **Policy Notes** at www.suerf.org/policynotes

SUERF
The European Money and Finance Forum

SUERF is a network association of central bankers and regulators, academics, and practitioners in the financial sector. The focus of the association is on the analysis, discussion and understanding of financial markets and institutions, the monetary economy, the conduct of regulation, supervision and monetary policy.

SUERF's events and publications provide a unique European network for the analysis and discussion of these and related issues.

SUERF Policy Briefs (SPBs) serve to promote SUERF Members' economic views and research findings as well as economic policy-oriented analyses. They address topical issues and propose solutions to current economic and financial challenges. SPBs serve to increase the international visibility of SUERF Members' analyses and research.

The views expressed are those of the author(s) and not necessarily those of the institution(s) the author(s) is/are affiliated with.

SUERF Secretariat
c/o OeNB
Otto-Wagner-Platz 3
A-1090 Vienna, Austria
Phone: +43-1-40420-7206
www.suerf.org • suerf@oenb.at