Cryptocurrency

Ingolf G. A. Pernice *Weizenbaum Institute*
Brett Scott *Independent* brettscott@fastmail.com

GLOSSARY
ENTRY

OPEN
ACCESS

PEER
REVIEWED

A draft of this article underwent open peer-review as an **Open Abstract**

Abstract: A cryptocurrency system can be understood as a system intended for the issuance of tokens which are intended to be used as a general or limited-purpose medium-of-exchange, and which are accounted for using an often collectively-maintained digital ledger making use of cryptography to replace trust in institutions to varying extents. Against such a backdrop, the singular term cryptocurrency can mean a token, intended to be used as a general or limited-purpose medium-of-exchange, issued via a cryptocurrency system.

1. Definition

A cryptocurrency system can be understood as a system intended for the issuance of tokens which are intended to be used as a general or limited-purpose medium-of-exchange, and which are accounted for using an often collectively-maintained digital ledger making use of cryptography to replace trust in institutions to varying extents. Against such a backdrop, the singular term cryptocurrency can mean a token, intended to be used as a general or limited-purpose medium-of-exchange, issued via a cryptocurrency system.

2. Origin and evolution of the term

The term *cryptocurrency* entered public usage with the surge of Bitcoin in 2008—a protocol aimed at enabling a network of people connected together via peer-to-peer digital communications infrastructure to issue digital tokens and transfer them between themselves whilst securing the process through cryptography (Nakamoto, 2008). While the original proposition did not use the term *cryptocurrency*, Nakamoto presented the project as a peer-to-peer 'currency' in a network and cryptography mailing list (Nakamoto, 2009).The term 'cryptocurrency', however, soon gained traction in online-chatter (compare HXN (2009) and print media (e.g., Davis, 2011). [1] An early distinction was made between the protocol—using the capitalised term *Bitcoin*—and the tokens, which used the lower-case term *bitcoin*. New bitcoins are 'written into existence' by a network participant (a so-called miner) who has succeeded in transforming the format of a bundle of proposed transactions (of previously issued bitcoins, along with a single request to issue new ones as a reward) in such a way that the bundle can be hitched to a chain of previously hitched bundles.

The remainder of this section attempts to explain how this protocol, and immediate descendants, might have shaped the term *cryptocurrency*.

---

1. An online search on Google Trends and Google Ngrams indicated that the term *cryptocurrency* was not used before the inception of Bitcoin.

2.1. The role of cryptography in early cryptocurrencies

The word stem *crypto* within the term *cryptocurrency* might be seen as surrogate for *cryptography*, but could also have emerged from the cypherpunk movement, who identified "anonymous cash and other untraceable payment systems" (De Filippi & Wright, 2018, p. 19) as enabling feature within a *crypto-anarchy* (Ludlow, 2001, p. 4). Bitcoin's mission of leveraging "cryptographic proof instead of trust" (Nakamoto, 2008, p. 1) resonates with the above. The exact protocol specifications of Bitcoin and its descendants are summarised in Scheuermann and Tschorsch (2016). Cryptography enters its architecture in various ways. A few examples are the integrity of, and consensus on a joint transaction history as well as the authorisation setup for sending tokens. However, the use of the surrogate *crypto* for Bitcoin is slightly arbitrary in the sense that earlier attempts at creating digital currencies (compare e.g. Chaum, 1988) relied heavily on cryptographic techniques as well. Nevertheless, it might seem justified by the fact that cryptography plays a far more central role for Bitcoin than it does for national currencies.

2.2. Monetary characteristics of early cryptocurrencies

Loosely speaking, the modern fiat monetary system consists of physical and digital credits—issued by state central banks, state treasuries, and private commercial banks—which circulate under a legal system that guarantees their redemption. The number of credits expands through issuance, after which they can be transferred in the course of exchange among those who use them, before being retired when they are returned to the issuers. This composite system of expandable-contractable credits is what we refer to as 'money' in everyday parlance. In this context, the term *cryptocurrency* is controversial, because—from its inception—the name has simply *assumed* that the tokens are money tokens. The controversy is amplified by the fact that enthusiasts sometimes use the term performatively to make the normative point that crypto tokens 'should be money', or—alternatively—to deny that what we currently call 'money' is in fact money. One strategy to negotiate these language politics is to initially strip the money assumption from the tokens by giving them the generic name *crypto-tokens*, and then listing their uncontroversial characteristics to compare them with fiat credits.

Tokens of early cryptocurrencies are *data objects* created through accounting, much like the act of typing out the number '1' creates the mental image of a 'thing'. This is what is referred to as a 'token', but they are 'blank tokens'. An example of a blank token in the physical world might be a clear plastic token with no inscription or rights attached to it. Bitcoin tokens, similarly, are *empty signifier*s, somewhat like

the digital equivalent of blank physical tokens, but with strict supply limits [2]. These blank digital tokens however, are promoted with a name and branded logo that serves as a mental image for them, without which they would be almost entirely featureless. The tokens can be said to be *digital bearer instruments*, in the sense that transfers can only be initiated by the possessor of a private key that can unlock an 'unspent transaction output'. The 'bearer-instrument-like' nature is one reason why cryptocurrency sometimes gets referred to as 'digital cash' (physical cash being the bearer-instrument form of fiat currency). The tokens move around—Bitcoin and some of its descendants are processing hundreds of thousands of transfers of tokens every day (compare Hileman and Rauchs, 2017). Furthermore, they have a *price* measured in fiat currency and their tokens can be split into smaller pieces, or combined into larger ones. The fact that split-able and lump-able tokens with a fiat currency price can be moved gives the system a 'moneylike' feeling, and—under a shallow definition of money as *something that is issued and moved around in association with commerce*—the term *cryptocurrency* feels loosely plausible in everyday conversation.

Most 'purchases' conducted with bitcoin tokens, however, take the form of *countertrade*. The token, priced in fiat currency, is compared to a good or service, priced in fiat currency, and from this comparison of two fiat currency prices emerges an exchange ratio between the token and the good or service. This is the conceptual equivalent of superimposing a pair of two-way fiat currency transactions over each other and cancelling out the money flows, giving the residual appearance of the crypto-token being used as 'money' to 'pay' for a good or service.

Nevertheless, Bitcoin is used primarily for speculation (Baur, 2018)—buying the token with fiat currency with an intention to resell it for fiat currency—rather than using it to countertrade ('pay') for goods and services. This speculation (compare, among others, Yermack, 2015; Glaser et al., 2014; or Cheah, 2015) drives volatility in the fiat currency price of tokens, which—when analysed through the lens of the conventional 'functions of money' paradigm favoured by economic textbooks (money as a medium-of-exchange, a store-of-value and a unit-of-account), poses problems for the 'moneyness' of the tokens. Not only are they not widely accepted in exchange for goods and services, but they are not widely used to price things, and attempts to provide prices are unintuitive [3] (Yermack, 2015). They also strug-

---

2. Note that the notion of a "blank token" refers here to economic intuition rather than technical implementation. In Bitcoin and its descendents no "coins" exist, but only transaction outputs that are transferable and arbitrarily divisible.

3. Usual consumer goods priced in Bitcoin, for example, are represented by tiny decimal numbers.

gle to consistently 'store value', if we interpret that to mean 'maintain stable purchasing power' (which in the case of Bitcoin means 'maintain fiat price and countertrade ratios'). Put simply, while a person can generally predict how many bags of sugar US$ 100 will command in a month, they will be very uncertain as to how much sugar they can obtain through Bitcoin countertrade in a month.

3. Issues currently associated with the term

Beyond these debates about the validity of the original use of the term *cryptocurrency*, the term has been destabilised by the proliferation of alterations to traditional cryptocurrency systems. The role of cryptography and 'moneyness' implied by the diverse token designs varies considerably and will be discussed in the remainder of the section.

3.1. The role of cryptography in today's cryptocurrencies

A useful classification of projects from a technical standpoint involves rights for writing and reading transaction records. Peters et al. (2016) introduced a popular categorisation that can be used to classify the underlying infrastructure of cryptocurrency systems along the dimension "public" vs. "private" and "permissioned" vs. "permissionless". In public-permissionless systems every participant in the network (node) can read transactions and write others to the ledger. For public-permissioned systems, only authorised nodes can write. In private permissioned systems, finally, even reading is restricted to authorised nodes. The more "private" and "permissioned" in its underlying infrastructure a system is, the further it is from the cypherpunk vision.

An example of a recent development trend holding true to the aim of replacing trust by cryptographic proof found in archetypal cryptocurrencies (compare Nakamoto, 2008; and Genkin et al., 2018) are so-called privacy-preserving cryptocurrencies or 'privacy coins' (e.g., Zcash, n.d.; Monero, n.d.). They are closely related to archetypal cryptocurrencies and replicate their public-permissionless setup of rights to read and write. As "alternative cryptocurrencies designed with the goal of providing stronger privacy guarantees than Bitcoin" (Genkin et al., 2018) they even *increase* the use of cryptography to ensure anonymity. As a consequence of their focus on privacy, however, they are leading to rising concerns with respect to anti-money-laundering and law enforcement (compare Tziakouris, 2020; or Ferrari, 2020).

The broad trajectory in recent years, however, has been to *decrease* the centrality of

cryptography in the respective implementations. Even permissioned payment systems run by corporations but still called *cryptocurrencies* entered the stage. [4] Eyal (2017) concludes that "if attendees at recent blockchain events are any indication, cryptocurrencies have caught the attention of the mainstream financial technology (FinTech) sector" (Eyal, 2017, p. 39). With traditional business starting to experiment with the technology inspired by Bitcoin, system requirements—and with it the respective security setups and use of cryptography—changed. The economic design for these more centralised payment systems led to the reestablishment of trusted third parties or intermediaries for token creation to a certain degree.

While many novel *cryptocurrencies* are far from the crypto-anarchist roots of archetypal token designs, the general idea of the replacement of trust in institutions or their internal governance mechanisms by cryptography still plays a role in all *cryptocurrency* designs. However, given that even fiat bank payments use cryptography for *security,* mere reliance on cryptography for security should not enter a definition of cryptocurrencies. [5]

3.2. Monetary characteristics of today's cryptocurrencies

Early cryptocurrencies had the declared intent of creating 'digital cash' or currency (see section 1.1.), but the proliferation of crypto token forms have destabilised how this is conceptualised. Not all development strands feature the objective of proposing general purpose monetary tokens.

First-layer tokens (e.g. Ether) that underlie smart contract platforms [6] (e.g. Ethereum), and informally even second-layer tokens (tokens running on respective platform) are called *cryptocurrencies*, but they exist first and foremost to activate smart contracts rather than aiming to provide a payment solution for goods and services more generally (see Bartoletti, 2017). Nevertheless, this more 'limited purpose' focus can be a strength, insofar as smart contract activation can be seen as a *real service* accessible via possession of the token, thereby 'anchoring' the tokens into a 'real economy', albeit one in cyberspace.

---

4. Compare e.g. Diem (n.d.) and their reception in the press e.g. New York Times (Popper & Isaac, 2020).

5. We would have liked to rely on the unifying element of blockchain-based technology (which supposedly amalgamates all the cryptographic tools of a cryptocurrency) here. However, noting that this term is similarly unclear and vague as the term to define, we abstained from that step.

6. A summary of the research around smart contract platforms is given in Macrinici et al. (2018) while Bartoletti et al. (2017) and Alharby et al. (2017) review different platforms. While generally similar to cryptocurrency systems, their tokens are part of the security setup and used as medium-of-exchange between smart contracts.

However, also 'general purpose' tokens are marked by changes. A response to the inherent instability in prices of archetypal cryptocurrency was the advent of 'stablecoins', which try to solve the issue of high volatility in purchasing power of Bitcoin and its descendants (Pernice, 2019). Stablecoins are tethered or pegged to fiat currencies, or 'backed' in some way with assets that have fiat currency prices. They are thus no longer 'blank' empty signifiers, and contain some reference point that is easier to estimate and communicate. There are very different types of stablecoins, and recently several frameworks have tried to unify and abstract existing stabilisation techniques (e.g., Bullmann et al., 2019; Pernice et al., 2019; Moin et al., 2020; Sidorenko, 2019; Clark et al., 2020). A national currency can be 'tokenized' by issuing a digital promise for it on a blockchain system, and such tokenised funds might indeed be categorised as a "new form of electronic money" (Blandin et al., 2019) falling under the respective regulations for e-money, anti money laundering and counter terrorist financing regulations. This might ensure "moneyness" at least from a legal standpoint. With more complex stablecoin designs the legal case is not always clear, but from an economic standpoint their stability in purchasing power might contribute to an increase in their adoption as money in the future. Stablecoins, for now however, haven't seen mainstream adoption in retail markets yet (Bullmann et al., 2019).

4. Conclusion

Many scientific publications simply assume the meaning of the term *cryptocurrency* to be common knowledge or, at most, sketch it roughly. [7] Instead, we followed the evolution of the term starting with Bitcoin to define what *cryptocurrency* is understood as today. The neologism *cryptocurrency* is unstable in its meaning, and is applied to systems with diverse technical architectures and governance systems. Nevertheless, one way to unify the diverse uses of the term is to define it by some common intent among those who claim it, rather than by the diverse means via which that intent is enacted, and regardless of whether the intent is achieved in practice. We find that cryptocurrency systems are unified by being intended to host a *general or limited-purpose medium-of-exchange*, a cryptocurrency, using infrastructure that replaces trust in institutions by cryptography to varying degrees.

To make the term more useful in public discourse, *cryptocurrency* should be coupled with specifying classifications from economic (e.g., Bullmann et al., 2019; Pernice et al., 2019; Moin et al., 2020; Clark et al., 2020), governance (e.g., Zi-

---

7. The meaning of *cryptocurrency* is outlined briefly in White (2014), Lansky (2018), Aggarwal (2018), Chu et al. (2017), Sovbetov (2018) and Härdle et al. (2020).

olkowski et al., 2020; Beck et al., 2018; Hacker, 2019) or technological (e.g., Cachin and Vukoli, 2017; Peters et al., 2016) points of view.

References

Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2017). Quantum attacks on Bitcoin, and how to protect against them. *ArXiv*. https://arxiv.org/abs/1710.10377

Alharby, M., & Van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study. *Computer Science & Information Technology*, *7*(10),1-6. https://doi.org/10.5121/csit.2017.7101 1

Bartoletti, M., & Pompianu, L. (2017). An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns. In M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. A. Ryan, V. Teague, A. Bracciali, M. Sala, F. Pintore, & M. Jakobsson (Eds.), *Financial Cryptography and Data Security* (pp. 494–509). Springer International Publishing. https://doi.org/10.1007/978-3-319-7027 8-0_31

Baur, D. G., Hong, K., & Lee, A. D. (2018). Bitcoin: Medium of exchange or speculative assets? *Journal of International Financial Markets, Institutions and Money*, *54*, 177–189. https://doi.org/10.1016/j.intfi n.2017.12.004

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, *19*(10). https://aisel.aisnet.or g/jais/vol19/iss10/1

Blandin, A., Cloots, A. S., Hussain, H., Rauchs, M., Saleuddin, R., Allen, J. G., & Cloud, K. (2019). *Global cryptoasset regulatory landscape study* [Report]. Cambridge Centre for Alternative Finance, University of Cambridge. https://econpapers.repec.org/RePEc:jbs:altfin:-201904-gcrls

Bullmann, D., Klemm, J., & Pinna, A. (2019). *In search for stability in crypto-assets: Are stablecoins the solution?* (Paper No. 230; Occasional Paper Series). European Central Bank. https://www.ecb.europ a.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf

Cachin, C., & Vukolić, M. (2017). Blockchain Consensus Protocols in the Wild (Keynote Talk). In *31st International Symposium on Distributed Computing (DISC 2017)* (pp. 1:1–1:16). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. https://doi.org/10.4230/LIPIcs.DISC.2017.1

Chaum, D., Fiat, A., & Naor, M. (1988). Untraceable Electronic Cash. In S. Goldwasser (Ed.), *Advances in Cryptology—CRYPTO' 88* (pp. 319–327). Springer. https://doi.org/10.1007/0-387-34799-2_25

Cheah, E. T., & Fry, J. (2015). Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. *Economics Letters*, *130*, 32–36. https://doi.org/10.1016/j.econlet.2 015.02.029

Chu, J., Chan, S., Nadarajah, S., & Osterrieder, J. (2017). GARCH modelling of cryptocurrencies. *Journal of Risk and Financial Management*, *10*(4), 17. https://doi.org/10.3390/jrfm10040017

Clark, J., Demirag, D., & Moosavi, S. (2020). Demystifying Stablecoins: Cryptography meets monetary policy. *Queue*, *18*(1), 39–60. https://doi.org/10.1145/3387945.3388781

Davis, J. (2011, October 3). The crypto-currency. *The New Yorker*, *87*. https://www.newyorker.com/ma

gazine/2011/10/10/the-crypto-currency

De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Cambridge, Massachusetts: Harvard University Press. https://doi.org/10.2307/j.ctv2867sp

Diem. (n.d.). Retrieved 3 May 2021, from https://www.diem.com/en-us/

Eyal, I. (2017). Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities. *Computer*, *50*(9), 38-49.https://doi.org/10.1109/MC.2017.3571042

Ferrari, V. (2020). The regulation of crypto-assets in the EU – investment and payment tokens under the radar. *Maastricht Journal of European and Comparative Law*, *27*(3), 325–342. https://doi.org/10.1177/1023263X20911538

Genkin, D., Papadopoulos, D., & Papamanthou, C. (2018). Privacy in Decentralized Cryptocurrencies. *Communications of the ACM*, *61*(6), 78–88. https://doi.org/10.1145/3132696

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., & Siering, M. (2014, June 7). Bitcoin-asset or currency? Revealing users' hidden intentions. *ECIS 2014 Proceedings*. European Conference on Information Systems. https://aisel.aisnet.org/ecis2014/proceedings/track10/15

Hacker, P. (2019). Corporate Governance for Complex Cryptocurrencies?: A Framework for Stability and Decision Making in Blockchain-Based Organizations. In P. Hacker, *Regulating Blockchain* (pp. 140–166). Oxford University Press. https://doi.org/10.1093/oso/9780198842187.003.0008

Härdle, W. K., Harvey, C. R., & Reule, R. C. G. (2020). Understanding Cryptocurrencies. *Journal of Financial Econometrics*, *18*(2), 181–208. https://doi.org/10.1093/jjfinec/nbz033

Hileman, G., & Rauchs, M. (2017). *Global cryptocurrency benchmarking study* [Report]. Cambridge Centre for Alternative Finance, University of Cambridge. https://ideas.repec.org/b/jbs/altfin/201704-gcbs.html

HXN [в^{3}ʌʀ]. (2009, September 24). This is really interesting: Bitcoin, the p2p cryptocurrency. Http://bitcoin.sourceforge.net/ [Tweet]. @*hxn*. https://twitter.com/hxn/status/4334116324

Lansky, J. (2018). Possible state approaches to cryptocurrencies. *Journal of Systems Integration*, *9*(1), 19–31. https://doi.org/10.20470/jsi.v9i1.335

Ludlow, P. (Ed.). (2001). *Crypto anarchy, cyberstates, and pirate utopias*. Cambridge, Massachusetts: MIT Press. https://doi.org/10.7551/mitpress/2229.001.0001

Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, *35*(8), 2337-2354. https://doi.org/10.1016/j.tele.2018.10.004

Moin, A., Sekniqi, K., & Sirer, E. G. (2020). SoK: A Classification Framework for Stablecoin Designs. In J. Bonneau & N. Heninger (Eds.), *Financial Cryptography and Data Security* (pp. 174–197). Springer International Publishing. https://doi.org/10.1007/978-3-030-51280-4_11

Monero. (n.d.). *Monero Research Lab*. Monero. https://web.getmonero.org/resources/research-lab/

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system* [White Paper]. https://bitcoin.org/bitcoin.pdf

Nakamoto, S. (2009, February 11). *Bitcoin open source implementation of P2P currency* [Forum post]. P2P Foundation Post. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source

Peters, G. W., & Panayi, E. (2016). Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. In P. Tasca, T. Aste, L. Pelizzon, & N. Perony (Eds.), *Banking Beyond Banks and Money: A Guide to Banking Services in the Twenty-First Century* (pp. 239–278). Springer International Publishing. https://doi.org/10.1007/978-3-319-42448-4_13

Pernice, I. G., Henningsen, S., Proskalovich, R., Florian, M., Elendner, H., & Scheuermann, B. (2019, June). Monetary stabilization in cryptocurrencies–design approaches and open questions. In *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 47-59). IEEE. https://doi.org/10.1109/CVCBT.2019.00011

Popper, N., & Isaac, M. (2020, April 16). Facebook-Backed Libra Cryptocurrency Project Is Scaled Back. *The New York Times*. https://www.nytimes.com/2020/04/16/technology/facebook-libra-cryptocurrency.html

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, *18*(3), 2084-2123. https://doi.org/10.1109/COMST.2016.2535718

Sidorenko, E. L. (2019). Stablecoin as a New Financial Instrument. In S. I. Ashmarina, M. Vochozka, & V. V. Mantulenko (Eds.), *Digital Age: Chances, Challenges and Future* (pp. 630–638). Springer International Publishing. https://doi.org/10.1007/978-3-030-27015-5_75

Sovbetov, Y. (2018). Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litcoin, and Monero. *Journal of Economics and Financial Analysis*, *2*(2), 1–27. https://mpra.ub.uni-muenchen.de/85036/

Tziakouris, G. (2018). Cryptocurrencies—A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective. *IEEE Security & Privacy*, *16*(4), 92–94. https://doi.org/10.1109/msp.2018.3111243

White, L. H. (2015). The Market for Cryptocurrencies. *Cato Journal*, *35*(2), 383–402. https://ideas.repec.org/a/cto/journl/v35y2015i2p383-402.html

Yermack, D. (2015). Is Bitcoin a Real Currency? An Economic Appraisal. In D. Lee Kuo Chen (Ed.), *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (pp. 31–43). Academic Press. http://doi.org/10.1016/b978-0-12-802117-0.00002-3

Zcash. (n.d.). *How it works*. Zcash. https://z.cash/technology/

Ziolkowski, R., Miscione, G., & Schwabe, G. (2020). Decision problems in blockchain governance: Old wine in new bottles or walking in someone else's shoes? *Journal of Management Information Systems*, *37*(2), 316-348.

https://doi.org/10.1080/07421222.2020.1759974