

December 23, 2020

Tokens and accounts in the context of digital currencies

Alexander Lee, Brendan Malone, and Paul Wong¹

Introduction

Several years ago, innovation in financial markets began to generate discussion of digital tokens and tokenization of financial assets. When these ideas first entered the public discourse, they were used to help illustrate a possible future state where financial instruments could be turned into digital objects and transferred in real time across the globe without financial intermediaries.² Established financial institutions proposed to tokenize securities to speed up settlement and enhance collateral mobilization. Technology startups proposed digital tokens tied to fiat currencies and other assets (for example, gold, diamonds, and other commodities). As work in these areas progressed from speculative ideation to concrete technology development, central banks began actively researching digital tokens through distributed ledger technology (DLT) experiments.

Despite the prevalence of the terms "token" and "tokenization," their meanings are still confusing to most. What is a token from a technical perspective, and from a conceptual or functional perspective? Many people use "token" as if its meaning were self-evident. References to tokens in the economics literature, computer science publications, technology blog posts, and general newspapers are inconsistent, as different people use the term to describe different (but related) things. Is a token a physical object, a digital object, something defined by a smart contract, or something else entirely? This lack of consistency has arguably led to further confusion and miscommunication.

Understanding the context in which tokens are referred to is important to understanding digital currencies. The goal of this note is not to propose new terminology or definitions, but rather to provide guidance that can help prevent potential confusion or miscommunication in the use of the terms "token" and "account".

The first section of this note explains how the cryptocurrency community has approached the concepts of tokens and tokenization. The second section looks at the domains of payment economics and central banks, and discusses tokens in the context of CBDC. The note concludes by highlighting some issues with the "tokens vs. accounts" dichotomy and the potential challenges that could arise as a result of the continued use of these ambiguous terms.

Tokens and the cryptocurrency community

Terminology regarding tokens in the cryptocurrency community has evolved, with no sole authority on exact definitions. Current concepts of tokens and tokenization likely originate from their usage in the context of Ethereum, a large public blockchain that offers a robust programming capability in the form of so-called smart contracts. An early use case for this flexible programmability was the definition of custom assets, and the Ethereum community proposed a standard for fungible units of value termed "tokens" shortly after its public launch. The adopted standard, widely known by its proposal identifier ERC-20, is arguably the primary reference point for the concept of tokens on Ethereum and other public blockchains today.

Ethereum, smart contracts, and the ERC-20 token standard

The public Ethereum blockchain, launched in 2015, was inspired by the core design of Bitcoin as a distributed ledger that does not require a central authority to coordinate agreement on its contents.³ Beyond this fundamental decentralized recordkeeping functionality, Ethereum introduced additional programming capability for interacting with the ledger contents. While Bitcoin does allow for the programming of spending conditions applicable to certain discrete amounts of bitcoin, Ethereum's design allows for the creation of generalized computer programs known as smart contracts, which are executable code stored on the Ethereum blockchain.⁴ A smart contract may be as simple as a calculator or as complicated as The DAO, an early experiment that was essentially a decentralized investment fund.⁵ The public functions of these smart contracts can be executed by any user of the Ethereum system and by other smart contracts.

An early use case for smart contracts was the programmatic definition of assets (or representations thereof) on a blockchain.⁶ The Ethereum community termed these assets "tokens". The general idea was that a smart contract could define its own ledger for tracking user balances of a token (essentially a sub-ledger of Ethereum, specific to that particular smart contract) and allowing users to transact in the asset represented by that token. Given the flexibility of

smart contracts programming on Ethereum, there are a great many ways to implement such a system; thus, in order to allow for more consistent interoperability of tokens, a standard interface for fungible tokens was proposed and adopted shortly after Ethereum's launch. This standard is known by its proposal number, ERC-20. Tokens issued by smart contracts that adhere to this standard are referred to as ERC-20 tokens.⁷ The standard interface allows for various functionality, including sending tokens from address to address on the blockchain, delegating them to a third party as an "allowance," and assigning them an identifier akin to a ticker symbol.

The widespread adoption of the ERC-20 standard has likely helped shape the notion of a "cryptocurrency token" as a custom asset issued on top of a blockchain through the use of smart contracts. Other blockchain platforms which have followed Ethereum's lead in offering flexible programming capability, such as Eos, Cardano, Tezos, and Stellar, all allow for the issuance of custom assets that the cryptocurrency community terms tokens.⁸

How do tokens on the Ethereum network differ from ether?

Ethereum has a native cryptocurrency, "ether", that is used to pay for all transactions processed by the network. Ether itself, however, is not an ERC-20 token; rather, it is an intrinsic part of the blockchain platform which predates the existence of any ERC-20 tokens.⁹ An Ethereum transaction may consist of a simple transfer of ether itself from one user to another, or it may be a call to a particular smart contract's function.¹⁰ Depending on the amount of computation that the Ethereum network must perform in order to execute the transaction, a corresponding fee will be charged in ether. A simple user-to-user transfer of ether may incur a low fee, while a call to a smart contract function that performs a large amount of mathematical computation may incur a high fee. This fee-for-computation policy means that the functions for interacting with ERC-20 smart contracts as described above, such as sending ERC-20 tokens from one user to another, incur their own transaction fees denominated in ether. Thus, while it is possible to transact value denominated in ether without the need for any other payment instrument, the same is not true of ERC-20 tokens: in order to transact in the latter, a user must also maintain a balance of ether for paying network transaction fees.

How are ERC-20 tokens recorded and transferred on the blockchain?

Chief among Ethereum's functionalities is electronic recordkeeping. Unlike Bitcoin, which handles recordkeeping using a format known as "unspent transaction outputs" (also referred to as UTXO), Ethereum records information via account addresses.¹¹ These account addresses are conceptually similar to user accounts in traditional finance.¹² However, in Ethereum, these accounts and associated balances on any ERC-20 sub-ledger are distributed across a decentralized network of participating computational nodes; thus, the only place where (balances of) ERC-20 tokens exist is on this network. While software for controlling user balances of these tokens has come to be known as a "cryptocurrency wallet", such wallets do not hold anything with a unit of value (as the name might suggest). Rather, a cryptocurrency wallet holds a private key that allows its holder to authorize transactions on a blockchain platform, in a manner loosely akin to placing one's signature on a check. While tokens may be viewed or controlled via wallet software, to the extent that they "exist," it is only in the replicated databases maintained by a blockchain platform's computational nodes and in the form of an account balance, not as a digital "object" in the wallet software itself.

Once a person controls tokens on the network, they can transfer control of those tokens to others. The sender and recipient of the tokens do not need to have a relationship with the token issuer; they simply need an Ethereum address for which they control the private key. The sender initiates the transfer by cryptographically signing and submitting to the Ethereum network a message that will deduct tokens from their balance and add them to the balance of the recipient's account. After the sender has used their private key to authorize the reassignment of control of some quantity of their tokens to someone else, that recipient now has the ability to use their own private key to transfer the tokens from their account balance in the same manner. Importantly, no unique digital information owned by the sender is transferred to the recipient's cryptocurrency wallet.

Other types of crypto tokens

Since Ethereum launched, a number of other blockchain projects have appeared that also offer the capability to issue tokens. While Ethereum remains the most common platform, other platforms reported by industry data aggregator CoinMarketCap with tokens in the top 100 by market capitalization include Binance Coin, TRON, Rootstock, Omni, and Stellar.¹³ Other newer platforms that are designed for token issuance, both existing and proposed, include Algorand, Avalanche, and Libra. Despite differences in the technology underlying these platforms, the conceptualization of tokens as programmatically-defined units of value that can be transacted on those platforms and tracked via account balances, remains a common feature.

In addition to fungible tokens (which have been described above in detail through explanation of the ERC-20 standard), blockchain platforms may also support non-fungible tokens.¹⁴ On Ethereum, there is an adopted standard for such tokens, commonly known by its proposal number ERC-721.¹⁵ Whereas fungible tokens can be used to represent "homogenous" assets such as a unit of currency or ownership of a specific quantity of gold, non-fungible tokens can be used to represent unique assets, such as a work of art or a property deed (for example, CryptoKitties).

Any blockchain platform offering sufficiently flexible programming typically has the capability of implementing functionality for non-fungible tokens.

Tokens and the central banking community

The use of tokens in money and banking date back several centuries. Traditionally, the term "token" has been used to describe physical objects representing value, such as precious metals or official coinage that acted as symbolic representations of value and could be used to make payments. Ownership of these early tokens was determined solely by physical possession. The most common way a person could come to own a monetary token was by trading for it with goods or services. In any such trade, transfers happened bilaterally between individuals. Crucially, physical monetary systems relied heavily on the assumption that such a token was difficult to replicate. If it could be copied easily, users could effectively create their own money at will, thereby debasing its value.

The exchange of tokens between individuals eventually led to the use of "accounts" to record asset ownership more easily and to facilitate more-complex trading and financial transactions. When combined with specialized institutions and processes, accounts allow for easy transfers between participants. Instead of carrying coins or precious metals (or any other tradeable goods, for that matter), merchants could keep accounts with a third party, such as a bank. For example, a bank in Renaissance-era Venice might have kept accounts for merchants on a paper ledger and allowed account holders to transfer balances from one person to another without any physical exchange of assets between the transacting parties. If the merchants needed physical money, they could clear out some or all of their bank account balances in exchange for an equal value in physical tokens.

Cash and central bank accounts

Although this idea – of money existing either as physical objects or as records in a ledger – predates the creation of fiat currency by states, it has obvious parallels to the central banking world. Central banks have historically issued money in two forms: cash and deposits. Cash is a physical form of money. It is widely available to the general public for a variety of uses, and it can be transferred from person to person anonymously. In addition, cash has built-in security features to make physical money easy to authenticate but difficult to counterfeit. For these reasons, cash, as we use it today, is analogous to the historical notion of a monetary token. Deposits, such as reserve and settlement balances, are an electronic form of money represented using accounts. They are typically only available to a limited set of entities, certain financial institutions and the official sector, for specific purposes.

In recent years, new formulations and categorization of money have arisen. In 2009, Kahn and Roberds wrote a seminal paper on payments economics that formalized the distinction between what the authors describe as "account-based" payment systems and "store-of-value" payment systems.¹⁶ In their description, the essence of the dichotomy boils down to the type of verification required by each system, "Verification of identity is central to accounts systems, just as counterfeit protection is central to store-of-value systems." Their formulation of money suggests that identity verification is a core distinction between an account-based payment system, such as bank deposits, and a "store-of-value" payment system, such as cash. In their formulation, the traditional concept of a "token" can be viewed as embodying the "store-of-value" systems.

Evolution of tokens and central bank digital currency

As conversations evolved within the central banking community on CBDC, the verification-based distinction between "accounts" and "store of value" (or "tokens") proposed by Kahn and Roberds was extended to CBDC.¹⁷ A 2018 report by the Committee on Payments and Market Infrastructures and the Markets Committee, for example, described token-based systems as reliant on the ability of the users of the system to verify that the digital object (that is, a token) is genuine and not a counterfeit.¹⁸ The report contrasted this with the notion of account-based systems as being reliant on someone – usually the asset issuer or other third party – to verify a user's ability to transfer an account balance by confirming the user's identity. These definitions are agnostic to any technology.¹⁹

Many central bank reports and speeches, as well as economics papers, have taken a similar approach by categorizing tokens as distinct from accounts, and by focusing on the object of verification (that is, verification of the token's authenticity or the user's identity) as a key determinant of CBDC classification.²⁰ This view presents tokens and accounts as strict foils, as described in another recent report that described digital tokens as "digital representations of value that are not recorded in accounts."²¹ Some reports, speeches, and papers offer a more nuanced view by acknowledging that value can be transferred from an account using information-based verification as well as identity-based verification.²² But, to a large extent, many CBDC reports, speeches, and papers focus on the known-identity concept as a key difference between tokens and accounts.

Taken as a whole, this central banking view of tokens and accounts is the byproduct of a desire to be both general (technology-agnostic) and categorical (tokens are distinct from accounts). The tokens concept is used, in some sense, as a short-hand for digital units of value that can be transferred anonymously, and offers a generic description for how that might happen (authenticating an "object"). As a practical matter, however, central banks often shy away from

describing how, exactly, tokens are recorded using a digital recordkeeping system – except to avoid suggesting they are tracked in an account-like structure or using accounting entries. Accounts, from this CBDC perspective, are understood mainly as a shorthand for "traditional" bank accounts maintained by entities in centralized or hub-and-spoke systems.

CBDC and the tokens and accounts dichotomy

The tokens and accounts dichotomy for CBDC may be confusing because the cryptocurrency and central banking communities use the terms in different ways. While tokens in the cryptocurrency community are generally understood as programmatically defined assets on a blockchain, the central bank view of a CBDC token in the tradition of Kahn and Roberds' dichotomy refers only to a notional "object" that is never strictly defined. What the cryptocurrency community calls tokens can be tracked in a form that central bankers might recognize as accounts, whereas in the central banking community, tokens and accounts refer to distinct potential designs for a CBDC. These different uses for the same terms may have led to misunderstanding regarding how CBDCs could and should be designed. Recently, several researchers have come to similar conclusions regarding the challenges caused by the ambiguity and lack of consistency in the tokens and accounts terminology.²³

The token and accounts dichotomy raises a few important issues. The first issue is that making tokens and accounts an "either/or" choice may not be useful; in some cases, it may be counterproductive. Attempting to create a distinction between the two may obscure or even misrepresent what is happening from a technical perspective. As noted above, tokens can operate within the context of accounts in the cryptocurrency community – this is true for many such digital currency systems.²⁴ With traditional money and banking, not all accounts rely on identity verification. For example, accessing a bank account in some jurisdictions, such as those jurisdictions with weak anti-money laundering requirements, may involve knowing a secret piece of information, rather than having an identity verified. Accounts need identifiers, but those are not the same as identities.²⁵ The distinctions between tokens and accounts may make sense in the respective cryptocurrency and central banking communities, but not in the common vernacular.

The second issue is the concept of a "digital object" form of money that can be stored locally. The metaphor of a coin, object, or bearer instrument living in a wallet or locally on someone's machine raises significant questions regarding technological feasibility, safety, and security.²⁶ Unlike traditional money, tokens in the cryptocurrency space are not stored locally but rather on a blockchain. What can be stored locally is a private key that allows for the transfer of the tokens on the blockchain. Importantly, what is stored or possessed by the end user has consequences for how we think about bearer instruments in the digital world: Is a private key that allows for the transfer of tokens on a blockchain a bearer instrument? Should a private key be treated as a legal equivalent to physically holding the token or asset? Systems that feature true local storage of the asset itself, coupled with offline peer-to-peer transfer capabilities, have value as a conceptual tool for analysis, but there remain questions about their development, secure operation, and widespread distribution. In the meantime, calling these systems and blockchain-based systems "token-based," further obscures the diverse technological underpinnings of each form of electronic recordkeeping.

The third issue is that digital tokens are fundamentally just pieces of information in both cryptocurrency and central banking. When talking about tokens in cryptocurrency, we may not necessarily associate a value with them – in a public system such as Ethereum, for example, anyone wishing to do so can deploy a new smart contract defining tokens that may have no explicit use and, consequently, have no transactional value. Certain tokens may even be specifically designed and deployed without any payments or financial use case in mind.²⁷ In central banking, tokens have historically referred only to physical assets that represent value. This notion, however, has changed in recent years with discussions on the tokenization, which typically refers to the digitization of an asset representing value (often via issuance of a token on a blockchain which represents a claim to the asset), such as cash and securities.²⁸ The evolving use case of tokenizing securities and other assets is similar to the prominent use of tokens representing value in the cryptocurrency community. In order to analyze the implications of these tokenized digital financial markets, it will be important to understand what people are referring to when they talk about tokenization.

Finally, many CBDC reports focus on either conceptual, policy topics or technical issues. However, the intersection of analytical concepts and technical implementation is necessary to avoid further confusion over what is a token, what can it do, how it can support a digital currency, and what it means in the context of a CBDC. Clarity on the terms can help further the conversation on digital currencies, including CBDCs. This shared understanding is particularly important as some jurisdictions race to the design and implementation of a CBDC—some of which are based on "tokens," others based on "accounts," and yet others using a combination of the two. As jurisdictions consider legal frameworks and oversight regimes around the issuance and use of digital currencies, the need for clear use of words and clear definitions becomes even more important.


Concluding thoughts

By highlighting how the terms "tokens" and "accounts" are used by the cryptocurrency community and the central banking community, this note seeks to inventory the subtly and sometimes obviously different ways these common

terms are being used by different people to reference different concepts. Acknowledgement of how these terms are being used in different communities may help identify areas where misalignment could create issues for legal frameworks and oversight regimes for digital currencies and so-called tokenized financial markets. Central banks researching CBDC will need to engage numerous stakeholders in the debate around its design and, ultimately, whether it should be pursued. Those stakeholders include the general public, legislative bodies, the private sector, and other central banks and the official sector. For these conversations to be successful, it is imperative that everyone speaks the same language, or, at the very least, enters the conversation with a common understanding of each perspective.

1. The views expressed in this paper are solely those of the authors and should not be interpreted as reflecting the views of the Board of Governors or the staff of the Federal Reserve System. The authors would like to thank Jillian Buttecali, Jacqueline Cremos, Melissa Leistra, Mark Manuszak, David Mills, Zach Proom, and Sarah Wright of the Federal Reserve Board; Jesse Leigh Maniff of the Federal Reserve Bank of Kansas City; and Antoine Martin and Joey Patel of the Federal Reserve Bank of New York for their contributions and assistance towards this note. [Return to text](#)

2. This use of "tokenization" is distinct from the way the term is used in the context of payment card security, which is out of scope for this note. [Return to text](#)





3. See Mills, David C., Kathy Wang, Brendan Malone, Anjana Ravi, Jeff Marquardt, Clinton Chen, Anton Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kargenian, Max Ellithorpe, Wendy Ng, and Maria Baird, "Distributed ledger technology in payments, clearing, and settlement," Finance and Economics Discussion Series 2016-095, Washington: Board of Governors of the Federal Reserve System, <https://doi.org/10.17016/FEDS.2016.095>  . [Return to text](#)

4. Despite the implications of the name, a "smart contract" need not encode anything like a legal agreement. On Ethereum, a smart contract is best understood simply as a term for a computer program. [Return to text](#)

5. While the example of a calculator is certainly feasible from a technological perspective, such a smart contract would unlikely be deployed in practice. The reason for this is that every transaction made on Ethereum is charged a fee. For functionality such as handling tokens or other units of value, paying a fee may be reasonable. However, paying a fee to call the "add" functionality of a calculator smart contract, when one could simply use a pocket calculator to add two numbers, would not be reasonable. Thus, many smart contracts deployed in practice either handle value themselves or aim to provide a functionality that cannot be replicated more cheaply outside of the blockchain (as a calculator smart contract could). [Return to text](#)

6. These assets are understood in the cryptocurrency community to be additional assets beyond any "native" cryptocurrency which is an intrinsic part of the blockchain software. Ether and bitcoin are the native assets of the Ethereum and Bitcoin blockchains, respectively. [Return to text](#)

7. See <https://eips.ethereum.org/EIPS/eip-20>  for the original proposal, which eventually became the ERC-20 standard. [Return to text](#)

8. For references to this terminology in the official documentation of all of these projects, see, respectively: <https://developers.eos.io/welcome/latest/getting-started/smart-contract-development/deploy-issue-and-transfer-tokens> , <https://docs.cardano.org/en/latest/explore-cardano/glossary.html> , <https://assets.tqtezos.com/docs/intro/#token-contracts> , and <https://developers.stellar.org/docs/issuing-assets/>  . [Return to text](#)

9. As an intrinsic part of the platform, ether is a resource which any smart contract can use, without the need to rely on any external smart contracts. The same is not true of ERC-20 tokens: in order to design a smart contract that can interact with a particular ERC-20 token, the new smart contract needs to interact with the smart contract defining that particular ERC-20 token. [Return to text](#)

10. Ether is similar to ERC-20 tokens in the sense that both are fungible units and may hold some market value either inside or outside the scope of the Ethereum platform. As of September 10, 2020, one ether was valued at more than \$300. [Return to text](#)


11. UTXOs are a format for recording balances where the value recorded for each "output" is a discrete amount that resulted from a prior transaction. A transaction may generate one or more UTXOs; for example, a single transaction may generate payments to two separate parties (two UTXOs), with a third UTXO being a "change" output sent back to the originator of the transaction. Ownership of UTXOs is defined by possession of the private key that enables a particular output's balance to be spent, rather than ownership of an "account" that has the balance tied to it. An individual user of a system that uses the UTXO model for recording balances may have the ability to spend an arbitrary number of UTXOs. In a pseudonymous system such as Bitcoin, which originated the UTXO model, there is no intrinsic way for a third party to roll up a user balance for a given user of the system. In Ethereum, by contrast, a user's ether balance may be observed publicly at their Ethereum user address. (Of course, an Ethereum user may create many such pseudonymous addresses and corresponding account balances if they wish.) It should be noted that the cryptocurrency community does in fact think of a dichotomy between the UTXO model and account model of accounting in blockchains, but the difference is distinct from the central banking community's notion of tokens vs. accounts. The conflation of these two dichotomies by central bankers may add to confusion regarding the matter of defining a "token." [Return to text](#)


12. The ether balance of an account address on Ethereum is publicly visible, a pronounced difference from traditional financial accounts. The address itself, however, is pseudonymous, unlike an account identifier in traditional finance which is associated with a known real-world entity. [Return to text](#)



13. At the time of this writing; see <https://coinmarketcap.com/tokens/>  for current information. [Return to text](#)

14. The difference between fungible and non-fungible tokens hinges on a simple technical inversion of an ownership mapping: a fungible token smart contract typically maps owner IDs to respective token balances, whereas a non-fungible token smart contract typically maps a

unique token identifier to the owner's ID for each specific token. [Return to text](#)

15. See <http://erc721.org/>  for further information on this standard. [Return to text](#)


16. See, Kahn, Charles M., and William Roberds, "Why pay? An introduction to payments economics," *Journal of Financial Intermediation*, Volume 18(1), January 2009, <https://www.sciencedirect.com/science/article/pii/S1042957308000533> . [Return to text](#)


17. See, for example, Mersch, Yves, "Digital Base Money: an assessment from the ECB's perspective," Farewell ceremony for Pentti Hakkarainen, Deputy Governor of Suomen Pankki – Finland's Bank, 16 January 2017, <https://www.ecb.europa.eu/press/key/date/2017/html/sp170116.en.html> . See also, Bech, Morten, and Rodney Garratt, "Central Bank Cryptocurrencies," *BIS Quarterly Review*, 16 September 2017, https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf . [Return to text](#)

18. See Committee on Payments and Market Infrastructures, "Central bank digital currencies," March 2018, <https://www.bis.org/cpmi/publ/d174.pdf> . [Return to text](#)


19. While cryptocurrencies reintroduced the term token into our modern lexicon, a token-based CBDC does not have to be implemented using blockchain or DLT, as long as the "digital object" is what is verified. Many "token-based" CBDCs currently proposed or envisioned, however, rely on blockchain or DLT. [Return to text](#)

20. See, for example, Auer, Raphael, and Rainer Böhme, "The technology of retail central bank digital currency," *BIS Quarterly Review*, 1 March 2020, https://www.bis.org/publ/qtrpdf/r_qt2003j.htm . See also, Mersch, Yves, "An ECB digital currency – a flight of fancy?" Consensus 2020 Virtual Conference, 11 May 2020, <https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200511~01209cb324.en.html> . See also, The Digital Dollar Project, *Exploring a US CBDC*, May 2020, https://static1.squarespace.com/static/5e16627eb901b656f2c174ca/t/5ee11f91d21ce15f2953bed7/1591811994197/Digital-Dollar-Project-Whitepaper_vF_6_10_20.pdf . See also, Kahn, Charles M., Francisco Rivasdeneyra, and Tsz-Nga Wong, "Should the Central Bank Issue E-money?" Bank of Canada Staff Working Paper 2018-58, December 2018, <https://www.bankofcanada.ca/wp-content/uploads/2018/12/swp2018-58.pdf> . [Return to text](#)




21. See, Bech, Morten, Jenny Hancock, Tara Rice, and Amber Wadsworth, "On the future of securities settlement," *BIS Quarterly Review*, 1 March 2020, https://www.bis.org/publ/qtrpdf/r_qt2003i.htm . [Return to text](#)

22. See, Bank of England, *Central Bank Digital Currency: Opportunity, challenges and design*, March 2020, <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593> . [Return to text](#)

23. See, for example, Milne, Alistair, "Argument by False Analogy: The Mistaken Classification of Bitcoin as Token Money," Loughborough University – School of Business and Economics, 25 November 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290325 ; Shah, Dinesh, Rakesh Arora, Han Du, Sriram Darbha, John Miedema, and Cyrus Minwalla, "Technology Approach for a CBDC," Bank of Canada: Staff Analytical Note 2020-6, February 2020, <https://www.bankofcanada.ca/2020/02/staff-analytical-note-2020-6/> ; Kiff, John, Jihad Alwazir, Sonja Davidovic, Aquiles Farrias, Ashraf Khan, Tanai Khiaonarong, Majid Malaika, Hunter Monro, Nobu Sugimoto, Hervé Tourpe, and Peter Zhou, "A Survey of Research on Retail Central Bank Digital Currency," IMF Working Paper, June 2020, <https://www.imf.org/en/Publications/WP/Issues/2020/06/26/A-Survey-of-Research-on-Retail-Central-Bank-Digital-Currency-49517> ; Sveriges Riksbank, "Second special issue on the e-krona 2020:2," Sveriges Riksbank Economic Review, June 2020, <https://www.riksbank.se/globalassets/media/rapporter/pov/engelska/2020/economic-review-2-2020.pdf> ; and Garratt, Rod et al., "Token-or Account-Based? A Digital Currency Can Be Both," Liberty Street Economics blog, August 12, 2020, <https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both.html> . [Return to text](#)

24. See, for example, Grym, Aleks, "The great illusion of digital currencies," *BoF Economics Review*, Bank of Finland, 21 June 2018, https://helda.helsinki.fi/bof/bitstream/handle/123456789/15564/BoFER_1_2018.pdf?sequence=1&isAllowed=y . [Return to text](#)

25. The difference emphasized here between identifiers and identities points to a challenge with using the concept of "identity" in the context of finance and computing: identity has multiple meanings. On one hand, it is related to privacy and anonymity (e.g., do you know something about who I am?). At the same time, particularly in the context of computing systems, it can refer to access control (e.g., within a given system, am I authorized as a user with certain permissions?). [Return to text](#)

26. The fundamental technological issue with such a design relates to the non-uniqueness of information, particularly in a digital context. Unlike atoms, which cannot be "copy-and-pasted" and thus allow for things like the creation of a singular instance of an authentic currency note with a specific serial number, bits representing information in a computer can be copied without any intrinsic way to distinguish any particular copy as "authentic." Certain systems such as the Handle System (<https://www.handle.net/> ) attempt to solve this problem by allowing authorized parties to maintain a registry of links to the "authentic" copy of any particular piece of digital information, but this approach requires network connectivity for use of the system and active maintenance of the links by administrators. Attempting to maintain a singular or "authentic" copy of a particular piece of digital information via secure hardware is risky because these secure hardware systems are repeatedly compromised (see, for example, <https://arstechnica.com/information-technology/2020/06/new-exploits-plunder-crypto-keys-and-more-from-intels-ultrasecure-sgx/> ) , and has been discouraged in at least one report looking specifically at CBDCs that was co-authored by a number of computer scientists specifically researching digital payments technologies (see Allen, Sarah et al., "Design Choices for Central Bank Digital Currency: Policy and technical considerations," Brookings: Global Economy & Development Working Paper 140, July 2020, https://www.brookings.edu/wp-content/uploads/2020/07/Design-Choices-for-CBDC_Final-for-web.pdf ) , particularly Section 8 – Secure Hardware). [Return to text](#)

27. For example, CryptoKitties (<https://www.cryptokitties.co/> ) uses non-fungible tokens on Ethereum to represent virtual pets rather than a financial asset. [Return to text](#)

28. Assets do not have to start in physical form in order to be tokenized. For example, dematerialized securities could be tokenized and represented on a blockchain. [Return to text](#)

Please cite this note as:

Lee, Alexander, Brendan Malone, and Paul Wong (2020). "Tokens and accounts in the context of digital currencies," FEDS Notes. Washington: Board of Governors of the Federal Reserve System, December 23, 2020, <https://doi.org/10.17016/2380-7172.2822>.

***Disclaimer:** FEDS Notes are articles in which Board staff offer their own views and present analysis on a range of topics in economics and finance. These articles are shorter and less technically oriented than FEDS Working Papers and IFDP papers.*

Last Update: January 06, 2021

2020年12月23日

数字货币环境中的代币和账户

亚历山大·李, 布兰丹·马龙和保罗·王¹

介绍

几年前, 金融市场的创新开始引起人们对数字代币和金融资产代币化的讨论。当这些想法首次进入公众讨论时, 它们被用来帮助说明未来的可能状态, 在这种情况下, 金融工具可以转换为数字对象, 并在没有金融中介的情况下在全球范围内实时传输。²已建立的金融机构建议对证券进行令牌化, 以加快结算速度并加强抵押物动员。科技初创公司提出了与法定货币和其他资产(例如, 黄金, 钻石和其他商品)绑定的数字令牌。随着这些领域的工作从投机概念发展到具体技术发展, 中央银行开始通过分布式账本技术(DLT)实验积极研究数字令牌。

尽管普遍存在“令牌”和“令牌化”两个术语, 但它们的含义仍使大多数人感到困惑。从技术角度以及从概念或功能角度来看, 令牌是什么? 许多人使用“令牌”就好像其含义不言而喻。经济学文献, 计算机科学出版物, 技术博客文章和一般报纸中对令牌的引用不一致, 因为不同的人使用该术语来描述不同的(但相关的)事物。令牌是物理对象, 数字对象, 由智能合约定义的东西, 还是完全其他的东西? 缺乏一致性可以说导致了进一步的混乱和误解。

了解令牌被引用的上下文对于理解数字货币很重要。本注释的目的不是提出新的术语或定义, 而是提供指导, 以帮助防止在使用“令牌”和“帐户”时出现潜在的混淆或误解。

本说明的第一部分介绍了加密货币社区如何处理令牌和令牌化的概念。第二部分着眼于支付经济学和中央银行的领域, 并在CBDC的背景下讨论了代币。本文的结尾部分着重强调了“令牌与帐户”二分法的一些问题以及由于继续使用这些歧义性术语而可能引起的潜在挑战。

代币和加密货币社区

加密货币社区中有关令牌的术语已经发展, 没有确切定义的唯一授权。令牌和令牌化的当前概念很可能源于以太坊环境中的使用, 以太坊是一种大型的公共区块链, 以所谓的智能合约的形式提供了强大的编程能力。这种灵活的可编程性的早期用例是自定义资产的定义, 以太坊社区在其公开发布后不久就提出了可替代价值单元的标准, 称为“代币”。通过的提议标识符ERC-20广为采用的标准可以说是当今以太坊和其他公共区块链上令牌概念的主要参考点。

以太坊, 智能合约和ERC-20令牌标准

以太坊公开区块链于2015年启动, 其灵感来自比特币的核心设计, 即分布式账本, 不需要中央机构来协调其内容的协议。³除了基本的分散式记录保存功能之外, 以太坊还引入了额外的编程功能, 可与分类帐内容进行交互。虽然比特币确实允许对适用于某些离散量比特币的支出条件进行编程, 但以太坊的设计允许创建称为智能合约的通用计算机程序, 这些程序是存储在以太坊区块链上的可执行代码。⁴智能合约可能像计算器一样简单, 也可能像DAO一样复杂, DAO是一项早期实验, 本质上是分散投资基金。⁵这些智能合约的公共功能可以由以太坊系统的任何用户和其他智能合约执行。

智能合约的早期用例是区块链上资产(或其表示)的程序化定义。⁶以太坊社区将这些资产称为“令牌”。总体思路是, 智能合约可以定义其自己的分类账, 以跟踪代币的用户余额(本质上是以太坊的子分类账, 特定于该特定智能合约), 并允许用户以该代币表示的资产进行交易。鉴于以太坊上智能合约编程的灵活性, 有很多方法可以实现这种系统。因此, 为了允许令牌具有更一致的互操作性, 在以太坊启动后不久, 提出并采用了可替代令牌的标准接口。该标准的建议号为ERC-20。遵循此标准的智能合约发行的令牌称为ERC-20令牌。⁷标准接口允许各种功能, 包括在区块链上从一个地址到另一个地址发送令牌, 将它们作为“津贴”委派给第三方, 以及为它们分配类似于股票代码的标识符。

ERC-20标准的广泛采用可能有助于通过使用智能合约将“加密货币令牌”的概念塑造为在区块链顶部发行的自定义资产。跟随以太坊(Ethereum)领先的其他区块链平台提供了灵活的编程功能, 例如Eos, Cardano, Tezos和Stellar, 都允许发行由加密货币社区称为令牌的自定义资产。⁸

以太坊网络上的代币与以太币有何不同?

以太坊有一个本地的加密货币“ether”, 用于支付网络处理的所有交易。然而, 以太本身并不是ERC-20代币; 相反, 它是区块链平台的固有部分, 早于任何ERC-20代币的存在。⁹以太坊交易可能包括以太本身从一个用户到另一个用户的简单转移, 或者可能是对特定智能合约功能的调用。¹⁰根据以太坊网络为执行交易必须执行的计算量, 将以太币收取相应的费用。简单的用户到用户的以太币传输可能会产生较低的费用, 而调用执行大量数学计算的智能合约功能可能会产生较高的费用。这种按计算收费的策略意味着, 如上所述与ERC-20智能合约进行交互的功能(例如, 将ERC-20令牌从一个用户发送到另一个用户)会产生他们自己的以太币计的交易费用。因此, 虽然无需任何其他支付工具就可以交易

以太币计价的价值，但ERC-20代币并非如此：为了在后者中进行交易，用户还必须保持以太币的余额，以便支付网络交易费。

如何在区块链上记录和转移ERC-20代币？

以太坊功能中的主要功能是电子记录。与比特币使用称为“未用交易输出”（也称为UTXO）的格式处理记录保存不同，以太坊通过账户地址记录信息。¹¹这些帐户地址在概念上类似于传统金融中的用户帐户。¹²但是，在以太坊中，任何ERC-20子分类账上的这些账户和相关余额都分布在参与计算节点的分散网络中；因此，存在（余额）ERC-20令牌的唯一位置是此网络上。虽然用于控制这些令牌的用户余额的软件已被称为“加密货币钱包”，但此类钱包不包含任何带有单位价值的东西（顾名思义，这是事实）。相反，一个加密货币钱包持有一个私钥，允许其持有者以类似于将人的签名放在支票上的方式在区块链平台上授权交易。虽然可以通过钱包软件查看或控制令牌，但只要它们“存在”，它就只能存在于由区块链平台维护的复制数据库中。

一旦一个人控制了网络上的令牌，他们就可以将这些令牌的控制权转移给其他人。令牌的发送者和接收者不需要与令牌发行者有关系；他们只需要一个以太坊地址来控制私钥。发送者通过加密签名并向以太坊网络提交一条消息来启动传输，该消息将从其余额中扣除令牌并将其添加到接收者账户的余额中。在发送方使用其私钥授权将其某些数量的令牌的控制权重新分配给其他人之后，该接收者现在可以使用自己的私钥以相同的方式从其帐户余额中转移令牌。重要的是，不会将发送者拥有的唯一数字信息传输到接收者的

其他类型的加密代币

自以太坊启动以来，出现了许多其他的区块链项目，这些项目也提供了发行代币的功能。虽然以太坊仍然是最常见的平台，但行业数据聚合商CoinMarketCap报告的其他平台中，以市值排名前100的代币包括Binance Coin，TRON，Rootstock，Omni和Stellar。¹³现有的和提议的其他专门用于令牌发行的较新平台包括Algorand，Avalanche和Libra。尽管这些平台背后的技术存在差异，但令牌的概念化仍然是一个常见功能，即以编程方式定义的价值单位可以在这些平台上进行交易并通过帐户余额进行跟踪。

除了可替代令牌（以上已通过对ERC-20标准的解释进行了详细描述）之外，区块链平台还可能支持不可替代令牌。¹⁴在以太坊上，有一种针对此类令牌的采用标准，通常以其提案号ERC-721闻名。¹⁵替代性代币可用于代表“同质”资产，例如货币单位或特定数量的黄金的所有权，而不可替代性代币可用于代表独特的资产，例如艺术品或财产契约（例如CryptoKitties）。任何提供足够灵活编程的区块链平台通常都具有实现不可替代令牌的功能。

代币和中央银行界

在货币和银行业务中使用代币的历史可以追溯到几个世纪前。传统上，“令牌”一词用于描述代表价值的实物，例如贵金属或官方造币，它们充当价值的象征性代表并可以用来付款。这些早期代币的所有权仅通过实际拥有来确定。一个人拥有货币代币的最常见方式是与服务或商品进行交易。在任何此类交易中，转移都是在个人之间进行的。至关重要的一点是，实物货币系统严重依赖于这样的令牌难以复制的假设。如果可以轻松地复制它，则用户可以有效地随意创建自己的货币，从而贬低其价值。

个人之间代币的交换最终导致使用“帐户”来更轻松地记录资产所有权并促进更复杂的交易和金融交易。与专业机构和流程结合使用时，帐户可以使参与者之间轻松转移。商人可以携带硬币或贵金属（或其他任何可买卖的商品），而不是第三方，例如银行。例如，在文艺复兴时期的威尼斯，一家银行可能已经在纸制账本上保留了商户的帐户，并允许帐户持有人将余额从一个人转移到另一个人，而交易双方之间没有任何实际资产交换。如果商人需要实物钱，

现金和中央银行账户

尽管这种想法-将货币作为实物或作为分类帐中的记录存在-在国家创建法定货币之前就已经存在，但它与中央银行界存在明显的相似之处。中央银行历来以两种形式发行货币：现金和存款。现金是金钱的有形形式。它广泛地为公众提供了多种用途，并且可以匿名地在人与人之间转移。此外，现金具有内置的安全保护功能，可以使实物货币易于验证，但难以伪造。由于这些原因，今天使用的现金类似于货币代币的历史概念。存款（例如准备金和结算余额）是使用帐户表示的电子货币形式。它们通常仅适用于有限的一组实体，

近年来，出现了新的公式和货币分类。2009年，卡恩（Kahn）和罗伯兹（Roberds）撰写了一篇有关支付经济学的开创性论文，正式确立了作者所说的“基于帐户的”支付系统与“价值存储”支付系统之间的区别。¹⁶在他们的描述中，二分法的本质归结为每个系统所需的验证类型：“身份验证对于帐户系统至关重要，就像防伪保护对于价值存储系统至关重要。”他们的货币公式表明，身份验证是基于帐户的支付系统（例如银行存款）和“价值存储”支付系统（例如现金）之间的核心区别。在其表述中，“代币”的传统概念可以看作体现了“价值存储”系统。

代币和中央银行数字货币的演变

随着CBDC在中央银行界内部对话的发展，由Kahn和Roberds提出的“帐户”和“价值存储”（或“令牌”）之间基于验证的区别也扩展到了CBDC。¹⁷例如，支付与市场基础设施委员会和市场委员会在2018年的一份报告中将基于令牌的系统描述为依赖于系统用户验证数字对象（即令牌）是否真实的能力。而不是假冒产品。¹⁸该报告将此与基于帐户的系统的概念进行了对比，该系统依赖于某人（通常是资产发行人或其他第三方）来通过确认用户的身份来验证用户转移帐户余额的能力。这些定义与任何技术无关。¹⁹

许多中央银行的报告和讲话以及经济学论文都采用了类似的方法，将代币分类为与账户不同，并将关注对象（即，对代币的真实性或用户身份的确认）作为关注对象。CBDC分类的关键决定因素。²⁰这种观点将令牌和帐户显示为严格的标签，如另一份最近的报告中所述，该报告将数字令牌描述为“未记录在帐户中的价值的数字表示形式”。²¹通过确认可以使用基于信息的验证以及基于身份的验证从帐户中转移价值，一些报告，演讲和论文提供了更为细微的看法。²²但是，在很大程度上，许多CBDC的报告，演讲和论文都将重点放在已知身份概念上，这是令牌和帐户之间的主要区别。

总体而言，这种中央银行对代币和账户的看法是对通用（技术不可知）和分类（代币与账户不同）的渴望的副产品。从某种意义上说，令牌的概念是可以匿名转让的有价数字单位的简写，并为可能发生的方式提供了通用的描述（验证“对象”）。然而，实际上，中央银行通常会回避描述使用数字记录保存系统准确记录令牌的方式-避免建议以类账户结构或使用会计分录来跟踪令牌。从CBDC的角度来看，帐户主要被理解为由集中式或中心辐射型系统中的实体维护的“传统”银行帐户的简写。

CBDC与令牌和帐户二分法

CBDC的代币和帐户二分法可能会令人困惑，因为加密货币和中央银行界以不同的方式使用这些术语。虽然通常将加密货币社区中的令牌理解为区块链上以程序方式定义的资产，但按照卡恩（Kahn）和罗伯兹（Roberds）二分法的传统，中央银行对CBDC令牌的看法仅指从未严格定义的概念“对象”。可以以中央银行可以识别为帐户的形式跟踪加密货币社区所谓的令牌，而在中央银行社区中，令牌和帐户指的是CBDC的不同潜在设计。相同术语的这些不同用法可能导致对CBDC如何设计和应该设计的误解。最近，²³

令牌和帐户二分法提出了一些重要问题。第一个问题是使令牌和帐户成为“要么/或者”选择可能没有用。在某些情况下，它可能适得其反。从技术的角度来看，试图在两者之间建立区分可能会掩盖甚至误解正在发生的事情。如上所述，令牌可以在加密货币社区的帐户环境中操作-这对于许多此类数字货币系统都是如此。²⁴使用传统的货币和银行业务，并非所有帐户都依赖身份验证。例如，访问某些辖区（例如反洗钱要求不高的辖区）中的银行帐户可能涉及知道一条秘密信息，而不是对身份进行验证。帐户需要标识符，但是标识符与标识符不同。²⁵令牌和帐户之间的区别在各自的加密货币和中央银行社区中可能是有意义的，但在普通语言中则没有意义。

第二个问题是可以本地存储的“数字对象”形式的货币的概念。比喻说，生活在钱包中或某人机器上的硬币，物品或承载工具的隐喻引起了有关技术可行性，安全性和安全性的重大问题。²⁶与传统货币不同，加密货币空间中的令牌不是存储在本地而是存储在区块链上。可以在本地存储的是一个私钥，该私钥允许在区块链上传输令牌。重要的是，最终用户存储或拥有的东西会影响我们对数字世界中的承载工具的看法：允许在区块链上传输令牌的私钥是否是承载工具？是否应将私钥视为等同于实际持有令牌或资产的合法等同物？具有资产本身真正本地存储功能以及脱机对等传输功能的系统具有作为分析的概念工具的价值，但仍存在有关其开发，安全操作和广泛分发的问题。同时，

第三个问题是，数字令牌从根本上来说只是加密货币和中央银行中的一部分信息。当谈论加密货币的代币时，我们不一定与它们关联一个值-例如，在以太坊这样的公共系统中，任何希望这样做的人都可以部署一个新的智能合约来定义可能没有明确使用的代币，因此，没有交易价值。某些令牌甚至可以专门设计和部署，而无需考虑任何付款或财务用例。²⁷在中央银行中，代币历史上仅指代表价值的实物资产。但是，近年来，随着关于令牌化的讨论，这一概念发生了变化，令牌化通常是指代表价值的资产的数字化（通常是通过在代表资产要求的区块链上发行令牌），例如现金和现金证券。²⁸代币化证券和其他资产的不发展的用例类似于代表代币在社区中价值的代币的显著使用。为了分析这些标记化数字金融市场的含义，重要的是要了解人们在谈论标记化时所指的是什么。

最后，许多CBDC报告都集中在概念，政策主题或技术问题上。但是，必须将分析概念和技术实现相结合，以避免在代币是什么，它能做什么，它如何支持数字货币以及在CBDC上下文中意味着什么方面造成进一步的混淆。明确术语可以帮助进一步讨论包括CBDC在内的数字货币。这种共同的理解尤其重要，因为某些管辖区竞相设计和实施CBDC，其中一些管辖区基于“令牌”，其他管辖区基于“帐户”，而另一些则使用两者的组合。当司法管辖区考虑围绕数字货币发行和使用的法律框架和监督制度时，

结论思想

通过重点介绍加密货币社区和中央银行社区如何使用“令牌”和“帐户”一词，本注释旨在细微地盘点，有时显然是不同人使用这些通用术语来引用不同概念的方式。承认这些术语在不同社区中的使用方式可能有助于确定哪些地方可能出现偏差，从而给数字货币和所谓的代币化金融市场的法律框架和监督制度带来问题。研究CBDC的中央银行将需要使众多利益相关者参与有关其设计以及最终是否应继续进行的辩论。这些利益相关者包括公众，立法机构，私营部门以及其他中央银行和官方部门。

1.本文表达的观点仅是作者的观点，不应解释为反映理事会或美联储系统工作人员的观点。作者要感谢美联储（Federal Reserve Board）的Jillian Buttecali, Jacqueline Cremos, Melissa Leistra, Mark Manuszak, David Mills, Zach Proom和Sarah Wright。堪萨斯城联邦储备银行的Jesse Leigh Maniff；纽约联邦储备银行的Antoine Martin和Joey Patel对此作出了贡献和协助。[返回文字](#)

2.“令牌化”的使用不同于在支付卡安全性中使用该术语的方式，该术语不在本注释的范围之内。[返回文字](#)

3.见米尔斯，戴维·C，王凯西，布伦丹·马龙，安妮娜·拉维，杰夫·马夸特，克林顿·陈，安东·巴德夫，蒂莫西·布雷津斯基，琳达·法西，金伯利·廖，凡妮莎·卡格尼安，马克斯·埃利索普，吴文迪和玛丽亚·贝尔德。“支付，清算和结算中的分布式分类帐技术”，《金融与经济讨论丛书2016-095》，华盛顿：美联储理事会，<https://doi.org/10.17016/FEDS.2016.095>。[返回文字](#)

4.尽管有名称的含义，但“智能合约”不需要编码法律协议之类的内容。在以太坊上，最好将智能合约简单地理解为计算机程序的术语。[返回文字](#)

5.虽然从技术角度来看，计算器的例子当然是可行的，但这样的智能合约在实践中不太可能部署。这样做的原因是，在以太坊上进行的每笔交易都要收费。对于诸如处理令牌或其他价值单位的功能，支付费用可能是合理的。但是，当人们可以简单地使用袖珍计算器将两个数字相加时，要花钱调用计算器智能合约的“加”功能是不合理的。因此，实践中部署的许多智能合约要么自己处理价值，要么旨在提供无法在区块链之外更便宜地复制的功能（就像计算器智能合约可以做到的那样）。[返回文字](#)

6.这些资产在加密货币社区中被理解为除作为区块链软件固有部分任何“本机”加密货币之外的其他资产。以太坊和比特币分别是以太坊和比特币区块链的原生资产。[返回文字](#)

7.有关原始提案，请参阅<https://eips.ethereum.org/EIPS/eip-20> [🔗](#)，该提案最终成为ERC-20标准。[返回文字](#)

8.有关所有这些项目的正式文档中对此术语的引用，请分别参见：<https://developers.eos.io/welcome/latest/getting-started/smart-contract-development/deploy-issue-and-transfer> [🔗](#)，<https://docs.cardano.org/en/latest/explore-cardano/glossary.html> [🔗](#)，<https://assets.tqtezos.com/docs/intro/#token-contracts> [🔗](#)，和[HTTPS://developers.stellar.org/docs/issuing-assets/](https://developers.stellar.org/docs/issuing-assets/) [🔗](#)。[返回文字](#)

9.作为平台的固有部分，以太坊是任何智能合约都可以使用的资源，而无需依赖任何外部智能合约。ERC-20令牌并非如此：为了设计可以与特定ERC-20令牌进行交互的智能合约，新的智能合约需要与定义该特定ERC-20令牌的智能合约进行交互。[返回文字](#)

10.以太类似于ERC-20代币，因为两者都是可互换的单位，并且可能在以太坊平台范围之内或之外具有一定的市场价值。截至2020年9月10日，一种以太的价值超过300美元。[返回文字](#)

11. UTXO是一种记录余额的格式，其中为每个“输出”记录的值是由先前交易产生的离散量。一笔交易可能会产生一个或多个UTXO；例如，单笔交易可能会向两个单独的交易方（两个UTXO）产生付款，而第三笔UTXO是发送回交易发起方的“更改”输出。UTXO的所有权是通过拥有使特定输出的余额可用的私钥来定义的，而不是拥有与之相关的余额的“帐户”的所有权。使用UTXO模型记录余额的系统的个人用户可以使用任意数量的UTXO。在起源于UTXO模型的假名系统（例如比特币）中，第三方没有固有的方式为系统的给定用户累积用户余额。相反，在以太坊中，可以在其以太坊用户地址上公开观察用户的以太余额。（当然，以太坊用户可以根据需要创建许多这样的假名地址和相应的账户余额。）应该指出的是，加密货币社区确实想到了UTXO模型与区块链中会计账户模型之间的二分法，但是区别与中央银行社区的代币和账户概念不同。央行行长将这两个二分法混为一谈可能会增加关于定义“令牌”的困惑。可以在以太坊用户地址公开查看以太余额。（当然，以太坊用户可以根据需要创建许多这样的假名地址和相应的账户余额。）应该指出的是，加密货币社区确实想到了UTXO模型与区块链中会计账户模型之间的二分法，但是区别与中央银行社区的代币和账户概念不同。央行行长将这两个二分法混为一谈可能会增加关于定义“令牌”的困惑。可以在以太坊用户地址公开查看以太余额。（当然，以太坊用户可以根据需要创建许多这样的假名地址和相应的账户余额。）应该指出的是，加密货币社区确实想到了UTXO模型与区块链中会计账户模型之间的二分法，但是区别与中央银行社区的代币和账户概念不同。央行行长将这两个二分法混为一谈可能会增加关于定义“令牌”的困惑。应当注意的是，加密货币社区实际上确实想到了UTXO模型与区块链中的账户模型之间的二分法，但是区别与中央银行社区的代币与账户概念不同。央行行长将这两个二分法混为一谈可能会增加关于定义“令牌”的困惑。应当注意的是，加密货币社区实际上确实想到了UTXO模型与区块链中的账户模型之间的二分法，但是区别与中央银行社区的代币与账户概念不同。央行行长将这两个二分法混为一谈可能会增加关于定义“令牌”的困惑。[返回文字](#)

12.以太坊上一个账户地址的以太余额是公开可见的，与传统金融账户有明显区别。但是，地址本身是假名，与传统金融中与已知现实世界实体相关联的帐户标识符不同。[返回文字](#)

13.在撰写本文时；有关最新信息，请参阅<https://coinmarketcap.com/tokens/> [🔗](#)。[返回文字](#)

14.可替代令牌和不可替代令牌之间的区别取决于所有权映射的简单技术反转：可替代令牌智能合约通常将所有者ID映射到各自的令牌余额，而不可替代令牌智能合约通常映射唯一的令牌标识符每个特定令牌的所有者ID。[返回文字](#)

15.有关此标准的更多信息，请参见<http://erc721.org/> [🔗](#)。[返回文字](#)

16.参见Kahn, Charles M.和William Roberds, “为什么要支付？支付经济学导论”，《金融中介杂志》，第18（1）卷，2009年1月，<https://www.sciencedirect.com/science/article/pii/S1042957308000533> [🔗](#)。[返回文字](#)

17.例如，参见默夫·伊夫（Yves Mersch），“数字基础货币：欧洲央行的评估”，芬兰银行Suomen Pankki副行长Pentti Hakkarainen的告别仪式，2017年1月16日，<https://www.ecb.europa.eu/press/key/date/2017/html/sp170116.en.html> [🔗](#)。另请参阅Bech, Morten和Rodney Garratt, “中央银行加密货币”，BIS季度评论，2017年9月16日，https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf [🔗](#)。[返回文字](#)

18.参见支付和市场基础设施委员会，“中央银行数字货币”，2018年3月，<https://www.bis.org/cpmi/publ/d174.pdf> [🔗](#)。[返回文字](#)

19.虽然加密货币将令牌一词重新引入了我们的现代词典中，但只要使用“数字对象”进行了验证，就不必使用区块链或DLT来实现基于令牌的CBDC。但是，当前提出或设想的许多“基于令牌的”CBDC都依赖于区块链或DLT。[返回文字](#)

20.例如，参见Auer, Raphael和Rainer Böhme, “零售中央银行数字货币的技术”，《国际清算银行季刊》，2020年3月1日，https://www.bis.org/publ/qtrpdf/r_qt2003j.htm [🔗](#)。另请参见Yves Mersch, Yves, “一种欧洲央行数字货币—幻想中的飞行？” 共识2020虚拟会议，2020年5月11日，<https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200511~01209cb324.en.html> [🔗](#)。另请参阅《数字货币项目，探索美国CBDC》，2020年5月，https://static1.squarespace.com/static/5e16627eb901b656f2c174ca/t/5ee11f91d21ce15f2953bed7/1591811994197/Digital-Dollar-Project-Whitepaper_vF_6_10_20.pdf [🔗](#)。另请参见Kahn, Charles M., Francisco Rivasdeneyra和Tsz-Nga Wong, “中央银行是否应发行电子货币？” 加拿大银行职员工作文件2018-58，2018年12月，<https://www.bankofcanada.ca/wp-content/uploads/2018/12/swp2018-58.pdf>。[返回文字](#)

21.参见Bech, Morten, Jenny Hancock, Tara Rice和Amber Wadsworth, “关于证券结算的未来”，BIS季度评论，2020年3月1日，https://www.bis.org/publ/qtrpdf/r_qt2003i.htm [🔗](#)。[返回文字](#)

22.参见，英格兰银行，《中央银行数字货币：机遇，挑战与设计》，2020年3月，<https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la>

= zh-CN&hash = DFAD18646A77C00772AF1C5B18E63E71F68E4593 [🔗](#)。返回文字

23.例如，见米尔恩·阿利斯泰尔，“虚假类比的论点：比特币作为代币的误分类”，拉夫堡大学—商学院和经济学院，2018年11月25日，https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290325 [🔗](#)；Shah, Dinesh, Rakesh Arora, Han Du, Sriram Darbha, John Miedema和Cyrus Minwalla, “CBDC的技术方法”，加拿大银行：2020年6月员工分析笔记，2020年2月，<https://www.bankofcanada.ca/2020/02/staff-analytical-note-2020-6/> [🔗](#)；吉夫 (Kiff)，约翰 (John)，圣战阿瓦齐 (Jihad Alwazir)，桑娅·戴维多维奇 (Sonja Davidovic)，阿奎雷斯·法里亚斯 (Aquilés Farrias)，阿什拉夫·汗 (Afrat Khan)，塔奈·凯奥纳朗 (Tanai Khiaonarong)，马吉德·马拉凯 (Majid Malaika)，亨特·蒙罗 (Hunter Monro)，杉本伸夫，埃尔韦·图佩 (Hervé Tourpe) 和彼得·周 (Peter Zhou)，“零售中央银行数字货币研究概览”，IMF 工作论文，2020年6月，<https://www.imf.org/en/Publications/WP/Issues/2020/06/26/A-Survey-of-Research-on-Retail-Central-Bank-Digital-Currency-49517> [🔗](#)；Sveriges Riksbank，“关于电子货币2020的第二期特刊：2”，Sveriges Riksbank 经济评论，2020年6月，<https://www.riksbank.se/globalassets/media/rapporter/pov/engelska/2020/economic-review-2-2020.pdf> [🔗](#)；和 Garratt, Rod 等人，“基于令牌或基于帐户？数字货币可以同时存在”，《自由街经济学》博客，2020年8月12日，<https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-be-both.html> [🔗](#)。返回文字

24.例如，参见 Grym, Aleksi, “数字货币的巨大幻象”，《BoF 经济评论》，芬兰银行，2018年6月21日，https://helda.helsinki.fi/bof/bitstream/handle/123456789/15564/BoFER_1_2018.pdf?sequence=1&isAllowed=y [🔗](#) 返回文本

25.此处强调的标识符和身份之间的差异表明，在金融和计算领域中使用“身份”概念存在挑战：身份具有多种含义。一方面，它与隐私和匿名性有关（例如，您了解我的身份吗？）。同时，特别是在计算系统的上下文中，它可以指访问控制（例如，在给定的系统中，我是否被授权为具有某些权限的用户？）。返回文字

26.这种设计的基本技术问题涉及信息的非唯一性，特别是在数字环境中。不同于原子，原子不能被“复制并粘贴”，从而允许创建具有特定序列号的真实纸币的单个实例，而原子则可以被复制而无需任何内在方式来复制计算机中的信息。将任何特定的副本区分为“真实”。某些系统，例如处理系统（<https://www.handle.net/> [🔗](#)）试图通过允许授权方维护指向任何特定数字信息的“真实”副本的链接注册表来解决此问题，但是这种方法需要网络连接才能使用系统并由管理员主动维护链接。尝试通过安全硬件维护特定数字信息的单一或“真实”副本是有风险的，因为这些安全硬件系统反复遭到破坏（例如，请 [🔗](#) 参阅 <https://arstechnica.com/information-technology/2020/06/new-exploits-plunder-crypto-keys-and-more-from-intels-ultrasecure-sgx/> [🔗](#)），并且至少在一份专门研究CBDC的报告中受到阻挠，该报告由许多专门研究数字支付技术的计算机科学家合着（见 Allen, Sarah 等人，“中央银行数字货币的设计选择：政策”和技术方面的考虑”，《布鲁金斯：全球经济与发展工作文件140》，2020年7月，https://www.brookings.edu/wp-content/uploads/2020/07/Design-Choices-for-CBDC_Final-for-web.pdf [🔗](#)，特别是第8节-安全硬件）。返回文字

27.例如，CryptoKitties（<https://www.cryptokitties.co/> [🔗](#)）在以太坊上使用不可替代的令牌来代表虚拟宠物，而不是金融资产。返回文字

28.资产不必以物理形式开始就可以被标记化。例如，非物质证券可以被令牌化并在区块链上表示。返回文字

请将此注释引用为：

Lee, Alexander, Brendan Malone 和 Paul Wong (2020)。FEDS 注释：“数字货币环境中的代币和帐户”。华盛顿：美联储理事会，2020年12月23日，<https://doi.org/10.17016/2380-7172.2822>。

免责声明：FEDS 注释是一些文章，在这些文章中，董事会工作人员发表了自己的见解，并就一系列经济和金融主题进行了分析。与 FEDS 工作论文和 IFDP 文件相比，这些文章篇幅较短，技术性偏低。

最近更新：2021年1月6日