FEDS Notes

December 23, 2020

Tokens and accounts in the context of digital currencies

Alexander Lee, Brendan Malone, and Paul Wong[1]

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 Rivadeneyra, 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, Aleksi, "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