FEDERAL RESERVE BANK *of* MINNEAPOLIS
February 2019

Ten troublesome blockchain terms: What's accurate? What's not?

The terminology used to describe blockchain technology poses challenges for regulators and business leaders. Determining the facts, understanding the variants, and effectively communicating the capabilities of the technology prove problematic when terms are misleading or used out of context. This could lead to regulatory inconsistencies across jurisdictions, inaccurate assessment of risk, policy or legislative actions counter to intended outcomes, technology selection mistakes, and wasted time and resources.

In August 2018, a group of Federal Reserve System staff with business and technology backgrounds met to challenge assumptions about the terms used to describe the functions and features of distributed ledger technology (DLT) and blockchain systems.

Here's what we concluded: Most of the terms used to describe blockchain technology are misleading. These terms often suggest that the "natural" design of blockchain delivers capabilities achievable only through specific design choices or with the addition of other systems or technologies.

The views expressed in this document are those of the workshop participants shown below and do not represent the opinions of the Federal Reserve System or its components.

Contributors in alphabetical order: Todd Albers, Guy Berg, Jim Cunha, Andy Frank, Angela Lawson, Matthew McHugh, David Negrin, CJ Obermaier, Danny Oursbourn, Skyler Pinna, Peter Purcell, Tinku Thompson, Lillian Villarroel, Michael Warner, Ken White

How and why we got here

Various sources offer conflicting views of the current state of blockchain and other DLTs in the private sector.[1] McKinsey points to large investments in blockchain by venture capital firms and technology players like IBM.[2] Chief information officers, however, appear cautious of it at this point, according to research by Forrester.[3] Many of the pilots begun over the past few years have either been abandoned or will be abandoned soon, states a 2017 article by Gartner. Put simply, there are many misunderstandings about blockchain.[4] In the Gartner article, Ray Valdes, former vice president at Gartner and a Gartner Fellow notes, "A primary cause of failure is a fundamental lack of understanding around the basic concept of blockchain technology, which results in a misalignment of its capabilities with the business problem that the enterprise is seeking to solve."

The challenges in the private sector have led various stakeholder groups, including standards organizations and banking and payments industry groups, to question what is real and what is not when it comes to emerging technologies like blockchain. Unfortunately, with no shortage of hyperbole about the benefits and capabilities of blockchain, the Federal Reserve System is subject to the same information challenges as the private sector. This dearth of objective material led Angela Walch, associate professor at St. Mary's University School of Law, to caution regulators in her 2017 paper, The Path of the Blockchain Lexicon (and the Law). "It is essential," she writes, "that regulators do not simply accept what they read or hear at face value; rather, they must adopt a critical point of view and act strategically to uncover the facts beneath the muddle of inconsistent terminology, misinformation and hype."[5]

So a group of Federal Reserve System colleagues convened and employed a simple methodology. We debated 10 common terms about blockchain and asked if the technology delivers the implied results the terms suggest.

We know that blockchain is an emerging technology. Much can and will change as will our understanding of it. As such, our analysis should be considered representative of both a point in time and specific to the perspectives and diverse expertise of the participants involved, rather than definitive.

For now, here's what we believe about the accuracy of the following common terms.

1 Security

Is it accurate to say blockchain provides security?

Yes, but limited to security against manipulation of data on the chain. Other security capabilities are dependent on the system design and supporting technology subsystems.

The use of "security" as a feature is misleading. Security can be defined in a number of ways. For example, a "secure system" may suggest that it provides data integrity, access control, confidentiality, and authentication. Our findings indicate that while blockchain provides security relative to the unmanipulated integrity of the data recorded on a blockchain, the blockchain alone, without additional technologies or systems, cannot protect against unauthorized access, such as a data breach.[6] If a system that feeds an update to the blockchain has a security vulnerability, the blockchain may be adversely affected. The blockchain itself also does not provide authentication.[7] While public key certificate technology authenticates the entry point to the chain, not all implementations have a certificate authority that manages the generation and legitimacy of the keys. Blockchain alone does not have the ability to identify if a key, or access credential, has been compromised, which would enable fraudulent information to be added to the chain.

Takeaway

— Design Matters

Many, if not most, of the purported features and capabilities of blockchain are design- and implementation-specific. Assumptions should not be made that because one design implementation includes a particular feature (privacy, transparency, strong user authentication, and so on) that others will share that feature.

Further, an essential feature often attributed to a blockchain is the transparency it provides, suggesting visibility to some information and transactions interacting with the chain.[8] Transparency of data may or may not be a security feature depending on the identified threat. For example, in a digital currency system, transparency may be an asset. However, in other applications such as settlement or clearing for financial institutions where confidentiality may be a key component of security, system data transparency is a security risk. Additionally, where transparency is present but confidentiality is needed, either encryption of the data on the chain or strong authentication access is required.[9] Confidentiality and access control can be built into a blockchain, but are not inherent attributes.

2 Data Integrity

Is it accurate to say blockchain provides data integrity?

Yes, but much depends on the design and effectiveness of the implementation.

Blockchain ensures that the rules of the system have been followed. It can identify and resist attempts to modify data on the chain through the hashing, chaining, distribution, consensus process, and rules implementation.

It does not assure accuracy of the data entered on the chain, but it does support integrity in that it provides strong protection from the manipulation of data once it is entered and confirmed through the consensus process. Where the blockchain is the initial source of information—for example, when transactions are recording the activity of a native token, like Bitcoin or other cryptocurrency, on the blockchain system—the data can be verified. However, in a supply chain implementation where information such as tracking data or weights and measures is external to the system, the data cannot be verified by the blockchain alone.

Takeaway

— A larger system is at play

Blockchain could be, in most cases, a core component within a larger system and work in conjunction with other technologies. For example, identity validation tools like iris scanners, RFID tags for supply chain tracking to achieve data integrity, external databases for query functions, or cryptography to encrypt confidential data may be employed to supplement the capabilities of the blockchain itself and to produce results as required by the specific business case. These types of additional technologies are a required component of the data entry into the blockchain system to achieve the data accuracy or integrity often (incorrectly) described as a feature of blockchain.

3 Authentication

Is it accurate to say blockchain provides authentication?

Yes, when defined only as providing proof that a certain key was used. If defined otherwise, then no.

From a security standpoint, blockchain does not authenticate or ensure the identity of the end user/actor. The term "authentication" is problematic for several reasons. Some may assume it refers to the accuracy of the data from an external source and subsequently recorded on the chain. Others may think it means that the human user's identity has been authenticated through the use of the private key. In fact, neither is a core capability of blockchain.

Blockchain does, however, provide transaction validation or validation of the updated state of the ledger by recording that an event took place, that it conformed to the rules of the network at the time of entry, and that it was confirmed via a consensus mechanism. For example, a document or a reference to a document containing the description of an asset such as a home or a diamond could be added to a blockchain. The fact that the document was added or was transferred from one party or another could be authenticated. But whether the description of the real-world asset is accurate, or that the asset exists, is outside of the core capability of a blockchain system.

In addition, blockchain ensures that a particular key was used to sign a transaction or enter data onto the record, thereby validating the transaction as submitted by the private key with the authority to transact. Authority is conferred through the private key. But blockchain does not provide new capabilities to perform authentication of the individual interacting with a chain. If authentication of a user is desired, additional technologies such as an iris scanner or other biometric device could be incorporated to provide two-factor authentication along with the usage of a private key.

4 Central Authority

Is it accurate to say blockchain eliminates the need for a central authority?

No, Blockchain does not inherently eliminate central authorities; rather, it substitutes one type of authority or trust model for another.

Instead of placing trust in a central authority such as a broker to facilitate an exchange, participants must trust in the system design and technology, and the network rules. It does not eliminate the need for some form of governance authority to establish, implement, and enforce the rules and to respond to unexpected system challenges and exceptions. While members of such a governance body may be distributed or decentralized, a point of governance is still needed to address operational issues.

Takeaway

— Value depends on the sum of its parts

Much of the value proposition of blockchain appears to rely on emergent properties created by the combination of distributed copies, cryptographic linkage of transactions, digital signatures, decentralized processing with consensus agreement, and supporting system technologies. For example, the claims nearest to accuracy—"Blockchain provides data integrity," "Blockchain provides resiliency," and "Blockchain provides transparency"—all require most of the elements above in combination to provide the expected benefit.

5 Immutability

Is it accurate to say blockchain provides immutability?

No, but it offers a reasonable expectation of immutability if a transaction has been added, a valid and effective consensus process has been employed, and finality as defined within the system has been reached.

A blockchain is intended to reject tampering with the history, but much is dependent on the implementation of the system and the dynamics, including the incentives and technology, within the participating network. The word "immutable" literally means the record cannot be changed. Relying on this as indisputable fact without assessing vulnerabilities to attack or the potential for mutation of existing data increases risk. Such reliance could lead to neglect of due diligence necessary to protect against unforeseen attacks or attacks that may have a low probability of success. A governance body, majority decision in a decentralized community, or the orchestration of attacks such as the "51% attack" could render the data mutable.[10] The overall system design, including the participation rules, consensus protocols, and participation demographics, has an impact on the potential vulnerabilities of the system to tampering; therefore, immutability should not be automatically assumed. For example, a fork in the chain, where two (or more) versions of a record of transactions may exist, causes potential confusion as to which chain records the accurate, authoritative, and accepted version of events. A software update that effectively rewrites the "official" record is possible.[11]

6 Resiliency

Is it accurate to say blockchain provides resiliency?

Yes. Resiliency can refer to both downtime of the available system and resistance to attacks such as replay or denial of service.

The core design pattern of blockchain potentially provides more resiliency features than traditional distributed databases with the application of appropriate rules and inclusion of a consensus mechanism and integrated system incentives or disincentives for behavior among participants in the network. However, to achieve greater resiliency than traditional systems, no clear rule exists for how many nodes may be required. In a design where anyone can write to the blockchain, a method or practice is needed to discourage malicious behavior. In addition, it is still open to debate whether a blockchain architecture can achieve resiliency more cost effectively.

Takeaway

— Resiliency is a core capability

The statement "Blockchain provides resiliency" was one of the few accurate statements and one of the only features that could be achieved by the core capabilities of a blockchain system without additional technology.

7 Transparency

Is it accurate to say blockchain provides transparency?

Yes, though transparency is dependent on the design pattern, related to the business rules, and subject to the requirements of the use case.

For example, a blockchain system could be designed for privacy and confidentiality rather than data transparency to meet specific business requirements. In a public blockchain implementation like Bitcoin, transparency is connected to read/write participation, does not apply to the identity of the transacting parties, and is a business requirement. This de facto case may cause the erroneous belief that this type of transparency applies to every design implementation. While the basic blockchain components do not include data encryption, encryption technology can be added based on the business need. Additionally, where blockchain systems are developed in open source environments, there is transparency in the code base, but the applications built on top may not be transparent and could depend on implementation and privacy requirements.

8 State of Truth

Is it accurate to say blockchain provides a shared state of truth?

No. However, it does provide a mutually agreed upon, shared record that may or may not represent accurate data.

Blockchain preserves the record as agreed upon by the participants in the network at a point in time and based on the rules of the system. But it cannot assess, without additional technologies or processes, whether the input data are factually accurate. If data added to the chain originated on the chain itself, as in payments applications like Bitcoin, the accuracy of the data can be validated against the transaction history. However, where external information, such as the provenance of a shipment of mangoes, is entered into the system, the accuracy of this information cannot be validated by the blockchain itself. For example, a blockchain system can be used to record product information as it moves through a supply chain with the addition of external technologies like electronic scales and radio frequency identification readers (RFIDs). A box of mangoes could be weighed and a barcode identifying the product could be scanned at each leg in its journey to market, thereby adding the data to the blockchain system. However, assessing whether those mangoes were stolen from a neighboring farm before packaging, or if the mangos were actually rocks of the same weight, is outside the blockchain system and therefore cannot be affirmed within the system itself.

Takeaway

— Shorthand can be dangerous

The shorthand used to speak about blockchain can result in false impressions and must be challenged to enable greater understanding. If we found so much to debate, others are likely to have similar questions and issues. Continued discussion to deconstruct and challenge the true capabilities delivered by blockchain is warranted.

9 Confidentiality

Is it accurate to say blockchain provides confidentiality?

No. Confidentiality is not inherent to the design pattern of blockchain, but is a design implementation option. A system can be designed to encrypt data on the chain to provide confidentiality, but that is not a baseline function or a new capability delivered by blockchain technology.

10 Non-repudiation

Is it accurate to say blockchain provides non-repudiation of transactions/data?

Yes, specific to two aspects: (1) that a certain key was used to initiate a transaction and (2) that the transaction and data conformed to the rules of the system. But it does not provide identity assurance of the user or accuracy of any external data entered into the system.

The use of a particular key is sometimes incorrectly assumed to be linked to a computer or device used by a person. The use of this key does not, in and of itself, imply that a certain individual was in control of the device or the key at the time of the transaction. A malicious actor could compromise the access credentials that would enable an illegitimate transaction, which could result in repudiation if dispute is allowed based on the agreed-upon rules among the system participants. However, a transaction's success at following the rules as described in the blockchain system cannot be repudiated.

More to think about blockchain and potential next steps

Our findings indicate that most of the shorthand references common in describing blockchain capability are not accurate and require greater scrutiny. We believe that bringing more certainty to the definitions of key terms used to describe blockchain prevents costly mistakes and wasted resources. Doing this exercise brought greater clarity for the participants. However, more work is needed. We hope to share these insights more broadly for continued development.

Further, though we evaluated 10 common terms and descriptions, many more exist. Future discussions can both update the work done by this group and address other feature descriptors of blockchain systems such as "trustless" or "decentralized." The group also identified an opportunity to address the developing "permissioned" blockchain market segment. Because the claims to some feature functionality likely originated with a permissionless and public model in mind, a permissioned and private blockchain design may be assumed by many to be similar. Additional work could address how the terms and their meanings differ specific to the implementation.

In addition, organizations with interest in this technology may benefit from this brief paper in developing business cases or requirements for pilot testing or hands-on development for learning about if and how a blockchain can be used as a tool to improve efficiency or drive results.

As Walch points out, the questions of law and the importance of preciseness in language are key. If laws or regulations take for granted some features of blockchain that are design-dependent—as many are—challenges may arise in litigation that are difficult to unwind. For those within the legal community, continued study and engagement both with these results and in future discussions could add value. Much of the discussion around smart contracts could benefit from legal, business, and technical expertise in collaboration as well.[12]

Lastly, because the impetus for convening this session began with questions from standards groups and business associations, our research—sourced collaboratively across the many business and technological experts within the Federal Reserve System with interest in this space—can contribute clarity to these national and international efforts where appropriate.

By seeking to clarify the terms used to describe a technology, we believe it's accurate to say that we can reduce regulatory inconsistencies, improve communication, and contribute to the accurate assessment of risk.

[1] We use "blockchain" throughout this brief for simplicity, though we note that a blockchain structure is thought to be a subset of what is referred to more generally as "distributed ledger technologies."For a simple explanation of blockchain see: Murray, Maryanne. "Blockchain Explained." Reuters. June 15, 2018.https://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

[2] Carson, Brant; Romanelli, Giulio; Walsh, Patricia; and Zhumaev, Askhat. "Blockchain beyond the hype: What is the strategic business value?" McKinsey & Company, June 2018. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value

[3] Bennet, Martha. https://go.forrester.com/blogs/predictions-2018-the-blockchain-revolution-will-have-to-wait-a-little-longer/ Forrester, November 2017.

[4] Pettey, Christy. "7 Strategies to Gain Value from a Doomed Blockchain Project." Gartner, April 5, 2017. https://www.gartner.com/smarterwithgartner/7-strategies-to-gain-value-from-a-doomed-blockchain-project/

[5] For a discussion of the pitfalls of the shifting blockchain lexicon, see: Walch, Angela. The Path of the Blockchain Lexicon (and the Law) (March 24, 2017). 36 Review of Banking & Financial Law 713 (2017). Available at SSRN: https://ssrn.com/abstract=2940335

[6] See number 2: Does blockchain provide data integrity?

[7] See number 3: Does blockchain provide authentication?

[8] See number 7: Does blockchain provide transparency?

[9] See number 9: Does blockchain provide confidentiality?

[10] Benchimol, Menajem, "51% Attack Occurs in Bitcoin Golds Blockchain Stealing Millions in the Meantime." Ebitnews.com May 25, 2018. https://ebitnews.com/2018/05/25/51-attack-occurs-in-bitcoin-golds-blockchain-stealing-millions-in-the-meantime/

[11] The hard fork in July 2015 was criticized by some as a "rollback" of the Ethereum code and therefore a violation of the "unchangeable" nature a blockchain is expected to have. Because of a bug in the code of an entity called the DOA, the Ethereum community largely voted to institute a change in the software that made it possible for those affected by the bug and the subsequent loss of ether (the native token of Ethereum) to recoup their funds. Those in the community, who did not agree to fork the code, maintain the original chain and the original token termed "Ethereum Classic." The "Classic" chain is incompatible with the forked code that addressed the bug.

[12] In addition to the statements we evaluated, the group also briefly discussed the term "smart contract." We characterize it this way: A smart contract is a means of automating an action initiated by one or more agents and recorded on a ledger. However, the current use of the term is very misleading. A "smart contract" is not a contract in the legal sense, nor is it an autonomous actor capable of judgment. It is not "intelligent" as in artificial intelligence. These automated actions may, however, be the expression of a legal contract in software form where the conditions of the contract are written and committed to the blockchain, through the consensus process, where the results of the executed code, once conditions are met, are also committed to the chain and confirmed. The consensus process, though, does not affirm or validate the real-world results of any exogenous transfer of goods or services. In addition, bugs in the code will be introduced. The effectiveness of the contract will only be as good as the code it was written in.