BLOCKCHAIN TECHNOLOGY

What Is It Good for?

INDUSTRY'S DREAMS AND FEARS FOR THIS NEW TECHNOLOGY

SCOTT RUOTI, BEN KAISER, ARKADY YERUKHIMOVICH, JEREMY CLARK, AND ROBERT CUNNINGHAM

In 2008, an author using the pseudonym Satoshi Nakamoto wrote a white paper describing Bitcoin, a new decentralized cryptocurrency.[8] Unlike past attempts at forming a cryptocurrency—attempts that relied on preestablished trusted entities for the system to operate correctly—Bitcoin's design runs on the open Internet, with no one in charge, while maintaining tight security. While the building blocks of Bitcoin were not novel, the composition of these properties into a single system was a meaningful contribution,[9] and Bitcoin became the first cryptocurrency to achieve widespread attention.

In response to Bitcoin's success, the technology was quickly dissected to understand how it works and what is new about it. Its most innovative component has been labeled *blockchain technology*, a decentralized mechanism for participants to agree upon data and computation.

Technology news commonly leaves the cheery impression that blockchain technology reduces or even completely eliminates the need for trust. The use cases of such an innovation stretch the imagination. Occasionally, there is a contrarian take.[12]

The truth is, trust is complicated. Blockchain technology does eliminate specific, narrow reliances on trust, but it also requires new assumptions that might be better or worse for specific use cases. Thus, there are not many single-sentence talking points that will be accurate about blockchain technology's efficiency, security, cost, etc.

It is clear that this technology requires a more nuanced discussion. Business executives, government leaders, investors, and researchers frequently ask the following three questions: (1) What exactly is blockchain technology? (2) What capabilities does it provide? (3) What are good applications?

The goal of this article is to answer these questions thoroughly, provide a holistic overview of blockchain technology that separates hype from reality, and propose a useful lexicon for discussing the specifics of blockchain technology in the future.

METHODOLOGY

The discussion in this article is based on a rigorous textual analysis of nonacademic sources (hereafter referred to as industry white papers), including but not limited to the technology, financial, and health care sectors—from startups to SMEs (small and medium-sized enterprises) to Fortune 500 corporations. Academics have already systematized deep technical aspects of blockchain technology. Our analysis systematizes a distinct set of knowledge—the institutional knowledge in industry—which helps complete the picture. What industry might lack in technical knowledge, it makes up for in understanding market needs, the true costs of deployment, the intricacies of existing and legacy systems, stakeholders and their competing interests, and the regulatory landscape.

Grounded theory limits the impact of researcher bias, ensuring that the themes and processes are derived from the data and not from the researchers' preconceived notions of what the data says.

While there is valuable information to be learned from industry, analyzing these sources also brings challenges, including (1) imprecise terminology and errors in knowledge; (2) inclusion of hype; and (3) researcher bias.

The well-established research method known as *grounded theory*[3,15] was used to rigorously analyze the data in a way that directly addresses each of these three limitations. Grounded theory helps researchers identify high-level themes and processes within qualitative data sources generated by humans and filled with imprecise terminology and descriptions. Additionally, grounded theory limits the impact of researcher bias, ensuring that the themes and processes are derived from the data and not from the researchers' preconceived notions of what the data says.

Materials

The following methods were used to gather materials:

- Following RSS feeds that track news and publications related to blockchain technology.

- Downloading materials published by blockchain consortia (e.g., Hyperledger, the Decentralized Identity Foundation).
- Reviewing documents from major accounting firms, banks, and tech companies.
- Browsing news articles and blog posts related to blockchain technology.
- Reviewing submissions to the ONC (Office of the National Coordinator of Health Information Technology) for the *Blockchain in Health Care Challenge*.

In reviewing these materials, we also followed references and included those documents if relevant. In total, 132 documents were collected and split into three categories:

- **High-level overviews.** Often prepared by investment firms, these overviews of blockchain technology provided an enumeration of efforts at using blockchain technology in practice.
- **System designs.** These papers proposed ways blockchain technology could be used in a specific system (or, less frequently, reported on a pilot study).
- **Commentaries.** These generally shorter documents discussed specific facets of blockchain technology in greater depth than seen in other documents.

Analysis

Four members of our group participated in the analysis of collected documents. We continued gathering and reviewing documents until each felt that the last three to five documents read revealed no new information; this is a commonly accepted stopping criterion in grounded theory that ensures that all core (i.e., not one-off) ideas have been identified. A technical companion to this paper contains the complete mythological details: the type of coding used at each stage and theory generation.[11]

Results

The analysis revealed a set of 75 interconnected concepts that define blockchain technology. These concepts are grouped into five broad categories:

- Technical properties—the components that make up blockchain technology. Examples include decentralized governance, a consensus protocol, and an append-only transaction ledger.
- Capabilities—the high-level features provided by the technical properties. Examples include automatic executions of code (i.e., smart contracts), internal auditability, and access control.
- Technical primitives—the building blocks used to construct the technical properties and capabilities of blockchain technology. Examples include timestamps, hash chains, and peer-to-peer communication.
- Use cases—classes of systems that the literature identified as applications of blockchain technology. Examples include cryptocurrencies, supply-chain management, and identity management.
- Normative properties—representative of what people hope to achieve using blockchain technology. Importantly, these properties are not provided by the use of blockchain technology, as the technical properties and capabilities are. In general, normative properties relate strongly to

the hype surrounding blockchain technology. Examples include public participation, trustlessness, and censorship resistance.`

While the concepts defining blockchain technology are divided into these five categories, individual concepts are highly interconnected, both inter- and intra-category. This lends credence to the notion that blockchain technology is a cohesive whole, with each of its component concepts serving a purpose in the overall technology. This article focuses on some interesting and useful highlights from the full analysis, while interested readers are directed to the technical companion article and data files for the rest.[11]

Blockchain technology is primarily defined by three sets of technical properties: shared governance and operation, verifiable state, and resilience to data loss.

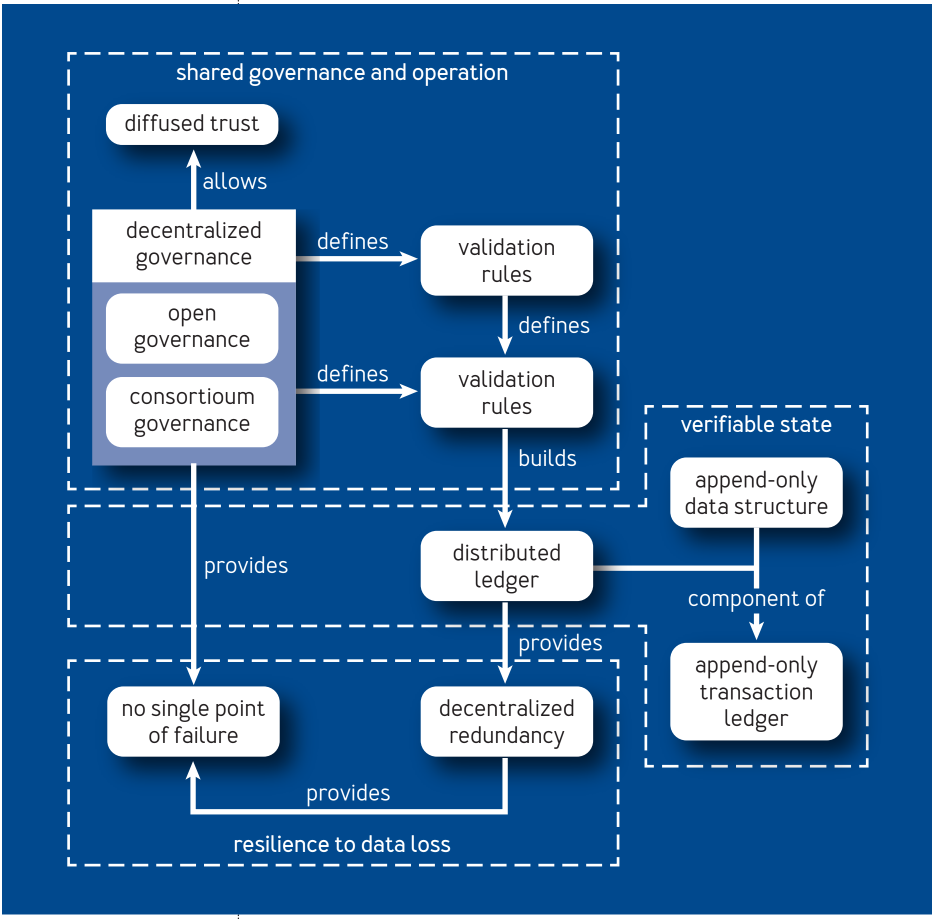
TECHNICAL PROPERTIES

The first broad category of blockchain technology concepts is technical properties, subdivided into three key groups: shared governance and operation, verifiable state, and resilience to data loss. Figure 1 shows the relationships among them.

Shared governance and operation

Blockchain technology addresses the scenario in which a collection of entities (for example, individuals or companies) want to participate in a communal system but do not trust each other or any third party to operate the system single-handedly. By deciding on the system details (governance) and then deploying networked devices (referred to as *miners*) to run the system, each entity can be assured of correct operation. If a small number of the miners become compromised (within bounds that are highly nuanced), the uncompromised miners can reject

FIGURE 1: **TECHNICAL PROPERTIES FOR BLOCKCHAIN TECHNOLOGY**



the malicious actions taken by the compromised miners and preserve the correct operation of the system. In this regard, blockchain technology provides *diffused trust,* in which the collective of miners is trusted. This is often given the misnomer *trustlessness*—trust still exists but has been diffused.

Shared operation is enabled by *consensus protocols,* which are used by the miners to agree upon which operations—known as *transactions*—will be executed by the system. A transaction is sometimes what it sounds like, a financial transaction that moves a unit of value from one account to another, but more generally it is a request that a certain function (which itself may be stored in the blockchain system) be executed on a set of inputs given in the transaction. Shared governance exists over what valid transactions look like (e.g., the transaction is digitally signed by the sender) and how the system functions (e.g., the size and number of operations in a transaction are less than a certain bound). Shared operation means every miner validates transactions, and consensus among miners is used to ensure that only correct outputs of valid transactions are written to the blockchain system (invalid or incorrectly executed transactions can be proposed but will be rejected by the miners).

Blockchain systems can be categorized based on who is allowed to act as a miner:

➡ ***Open governance (i.e., permissionless blockchain systems).*** Any party that is willing to participate in the consensus protocol is allowed to do so, regardless of their identity. To prevent a Sybil attack, in which an attacker creates multiple identities in order to influence the results of the consensus protocol, open governance system rely on consensus protocols where miners prove ownership and/or expenditure of some costly, finite resource. Proof of work (demonstrating ownership of computing resources) and proof of stake (staking digital assets owned on the blockchain system) are two common methods.[2,5]

- ***Consortium governance (i.e., permissioned blockchain systems).*** Participation in the consensus protocol is limited to miners approved on a whitelist defined at system initialization. If this set never changes, it is known as a *static consortium*. Alternatively, in an *agile consortium* miners change over time, either based on the rules of the system (e.g., random selection) or through consensus by the existing miners. Because each miner in a consortium is mapped to a known identity, a traditional byzantine fault-tolerant protocol (from distributed systems) can be used. This sidesteps the wasteful resource expenditure of Sybil-resistant protocols such as proof of work.[2,5]

For each type of governance, there is a need to reward correct participant behavior. The first type of incentive is *intrinsic*—i.e., miners maintain the system faithfully because they derive value from using it. Next, *on-chain incentives* exist when the blockchain system provides direct benefits to miners for faithful execution (e.g., minting currency and giving it to the miners). Finally, *off-chain incentives* are those not managed by the blockchain system—for example, contractual obligations or individual reputation. Importantly, off-chain incentives apply only to consortium governance, as they inherently rely on knowing the identity of the miners.

Verifiable State

Entities adopt blockchain technology because they want their trust to be rooted in the system (i.e., that the current state of the system accurately reflects the transactions that the consensus protocol allowed to execute in the past). To enable this trust, miners write all transactions to a cryptographically verified append-only ledger,[14] providing full system provenance and allowing miners (or outside parties) to audit the system's current state and past operations.

In many systems, including Bitcoin, this ledger is colloquially referred to as the *blockchain* (we avoid using this term for the ledger to avoid confusion with holistic references to blockchain technology). In the ledger, all transactions are strictly ordered, and after consensus is reached (and as long as it is maintained) this ordering never changes and transactions are never removed. Thus, all miners who begin at the first entry (called the *genesis block*) will process all the transactions in the same order and reach the same current state for the entire system.

Resilience to data loss

If the ledger were stored in a single location, deletion or modification of data could be detected by all parties, but there would be no guarantee that the data could be restored. With blockchain technology, the content of the ledger is replicated among all miners to address this single point of failure. When data does need to be restored—for example, if an individual miner's ledger is corrupted or a new miner joins—the replicated data can be verified to ensure that it correctly represents the system state.

Some blockchain systems try to limit the amount of data any given miner needs to replicate by segmenting the data and assigning miners to handle governance and operations for only a subset of the system. This is known as *sharding*, with individual segments of the data called *shards*. Sharding can drastically reduce the amount of data that miners need to store, while also increasing the performance of the consensus protocol, which often scales based on the number of miners. Still, sharding adds complexity to auditing the system as a whole. Additionally, by reducing the number of miners responsible for any given transaction, sharding reduces the number of miners an adversary would need in order to deceive an end client about a transaction's existence.

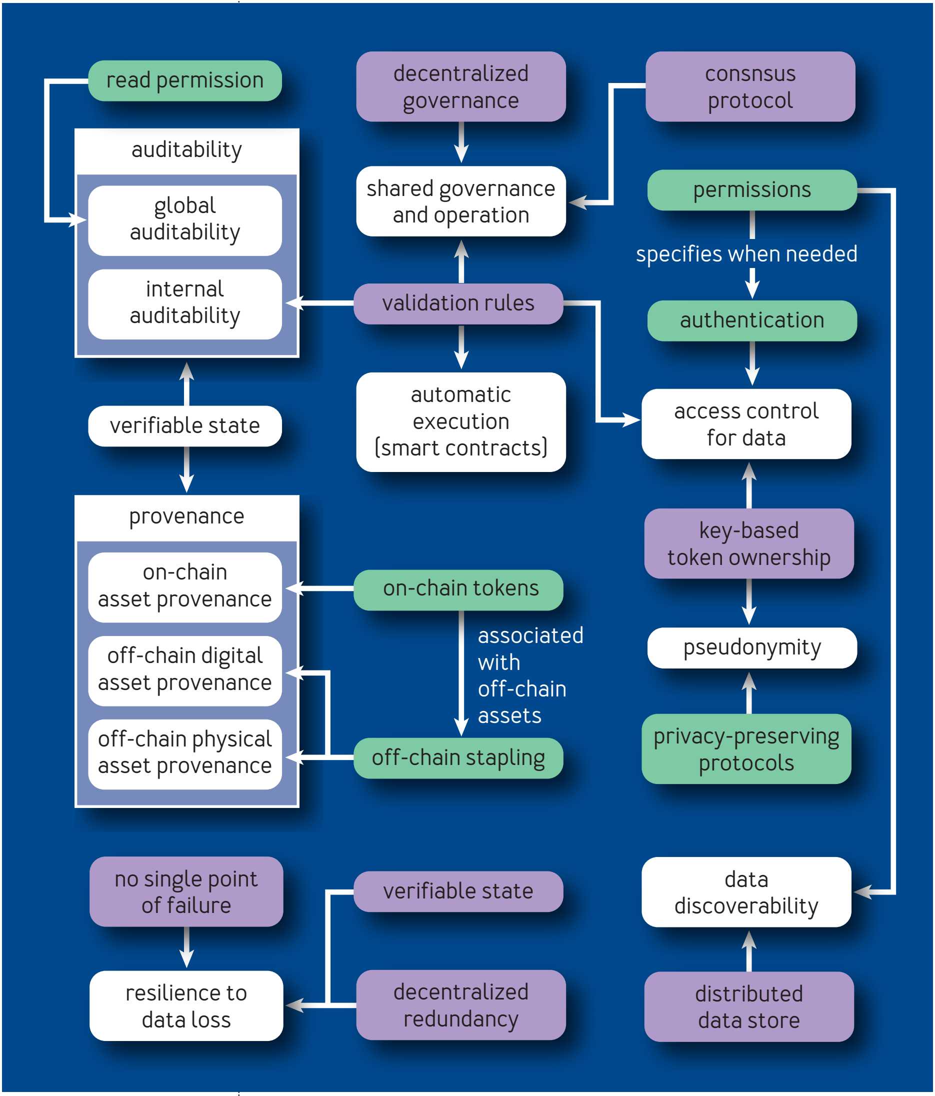
CAPABILITIES

Capabilities define the high-level functionality that can be achieved by using blockchain technology in a system's design. Blockchain technology's three core capabilities were described in the preceding section: (1) shared governance and operation;, (2) verifiable state, and (3) resilience to data loss. In coding, we identified 11 additional capabilities. (In figure 2 these capabilities are color coded: purple represents capabilities; blue, technical properties; and green, technical primitives. Arrows indicate that the destination depends on the source.)

Provenance and auditability

Blockchain systems provide a complete history of all transactions that were approved by the consensus process (i.e., full-system provenance). This information can be used by the miners to audit the system and ensure that it has always followed the appropriate rules. Additionally, this information can be used by nonminers to verify that the system is being governed and operated correctly.

FIGURE 2: **CAPABILITIES FOR BLOCKCHAIN TECHNOLOGY**



If transactions are used to store information regarding digital or real-world resources, then the resources must be *stapled* to on-chain identifiers. The provenance information for the blockchain system can also be used to provide audit information for those resources. This can be used to track physical off-chain assets (e.g., for supply-chain management), digital off-chain assets (e.g., copyrighted digital media), or digital on-chain assets (e.g., cryptocurrencies or data files).

Access control and pseudonymity

Data stored in a blockchain system may have limitations on which users can use it as an input to a transaction or modify it as part of the transaction. For example, a financial asset should be a valid input to a transaction only if the owner of that asset approves its use. One approach to providing this functionality is storing access control lists (ACLs) in the ledger and having the appropriate users prove their identity to the miners (e.g., using Kerberos or OAuth 2.0) as part of the transaction validation process.

More commonly, access control in a blockchain system is implemented cryptographically: data is associated with a public key when it is created, and the ability to use or modify this data as part of a transaction is granted only to users who can prove knowledge of the corresponding private key (e.g., by generating a signature that validates with the public key attached to the data). Ownership of the data can be expanded or transferred by associating it with a new public key.

Key-based (as opposed to ACL-based) ownership of data has another advantage: It allows for pseudonymous ownership and use of data. Still, this requires careful attention in the system design to use appropriate cryptographic techniques (e.g., zero-knowledge proofs, mix networks, or secure multiparty computation) to avoid linking real-world individuals to their keys and actions. This remains an open problem.

Automatic execution (smart contracts)

In a general-purpose blockchain system, a smart contract or decentralized application (DApp) can be deployed using a transaction that stores the code for a set of functions and the initial state of the contract. These functions can then be called in subsequent transactions. The functions themselves are executed by the miners, and outputs are verified through the consensus protocol. Any entity can execute any function, but the function might be programmed to fail if the conditions under which it is called are not what the designer intended. The computational power of the scripting language that can be used to specify a function varies from system to system and there are many nuances to ensure functions can be executed by each miner deterministically in a timely fashion. Bitcoin is known for its limited scripting language that enables little beyond financial transactions, while Ethereum strives for highly verbose code capable of general computation.

Data discoverability

If users are allowed to read any record stored in a blockchain system, then it is possible to search for records of interest. This capability is nothing more than what is provided by having a read-only data lake, but it was still discussed frequently in the reviewed literature.

CHALLENGES AND LIMITATIONS

Our analysis reveals several challenges that need to be considered when developing systems that use blockchain technology.

Scalability and performance

Decentralized governance and operation incur three forms of overhead: (1) the need to run a consensus protocol before state can be updated, (2) the need to store the full system provenance, and (3) the need for each miner to store the ledger in its entirety. Furthermore, most of today's open governance blockchain systems are based on proof of work, which brings additional challenges. Users must acquire hardware and expend electricity to participate in consensus, the real-world cost of which can be tremendous. For example, it was estimated that as of April 2018 the energy consumed by Bitcoin miners alone was equivalent to the power usage of almost 5.5 million U.S. households.[4]

On-chain correctness

All executable code is subject to bugs, and smart contracts are no exception. The immutability of a blockchain's ledger exacerbates this challenge by impeding rollback of state changes, even those that are clearly malicious. Failure to act can be costly (e.g., the DAO attack[13]), but so too can reversing transactions. If miners decide to roll back the ledger to erase a mistaken transaction, confidence in the blockchain system may be lost. The rollback system must be designed carefully, or there is risk of further exploitation.[1] Alternatively, if miners can't agree on what to do about errant transactions, it could lead to a *fork*: the creation of two competing blockchain system.

Off-chain stapling

Many blockchain systems manage off-chain assets by representing them on-chain using digital identifiers, or *tokens*. A major challenge for these applications is ensuring consistency between on-chain state and the off-chain reality it represents. When dealing with digital assets, consistency can be maintained by code; for example, a smart contract can track transference of ownership for a digital media license. For physical assets, real-world processes must be employed to ensure consistency. These processes are an obvious point of failure, as they rely on correct execution by trusted parties (something that blockchain systems are often deployed to remove). The end users must also be trusted, as they may be able to separate a token and sell it while keeping the asset, causing the token to be attached to an invalid asset (e.g., fake goods in luxury markets).

Similar challenges arise when blockchain systems must track real-world events and information (e.g., sports scores, web requests). While such information can be provided by *off-chain oracles*, these are trusted entities that are difficult to audit.

Security

Because of their decentralized nature, blockchain systems are potentially vulnerable to a number of security threats.

Coordinated attacks by a majority (or, often, even a large minority) of the miners can reorder, remove, and change transactions on the ledger. Additionally, blockchain systems are vulnerable to traditional network attacks such as denial of service or partitioning. Such attacks aim to lower the number of participating miners or fracture the network of miners to prevent consensus, lower the bar for attacks, or create an inconsistent state.

Privacy and anonymity

Data in a blockchain ledger is public (at least to all miners) in order to enable verification, meaning that sensitive data is inherently nonprivate. Confidentiality can be provided using a reference monitor that limits access (for nonminers) to data stored in a blockchain system based on access-control lists stored in the ledger, but this introduces a trusted entity (the reference monitor). Alternatively, the data can be encrypted using advanced cryptographic techniques that allow miners to verify the correctness of encrypted transactions (e.g., zero-knowledge proofs, secure multiparty computation, and functional encryption),[7] though encrypting data limits auditability and the ability to have meaningful shared governance.

Extreme care must be taken when trying to build an anonymous blockchain system. While many existing blockchain systems provide a notion of *pseudonymity* in which users are identified by their cryptographic keys instead of by their real-world names, this does not provide true anonymity, as attacks that correlate transactions by the same pseudonyms together with other data external to the blockchain system can effectively deanonymize users.[6]

Usability

The availability of user-friendly developer tools varies significantly depending on the maturity of the blockchain platform. Some projects such as Ethereum have mature tools, while others have very little support. Many blockchain platforms are geared toward expert users and lack the experience-focused tools needed for easier use by nonexperts. A related challenge is that some blockchain systems require users to store, manage, and secure cryptographic keys; this requirement is known to be a significant impediment for most users.[10]

Legality and regulation

Some benefits claimed by blockchain systems cannot be attributed to the underlying technology, but rather to sidestepping the regulation and oversight that slows existing systems (for example, international payments or raising capital by selling virtual assets to investors). As regulators catch up, compliance is given priority. Blockchain technology is not directly regulated; firms are regulated based on how they use it. The most discussed areas of regulation are taxation, audited financial statements, transaction reporting (know-your-customer/anti-money laundering/anti-terrorist financing), securities law, banking, and custodianship. An extreme case of regulation is prohibition of cryptocurrencies or blockchain assets. At the time of writing, the largest country to ban Bitcoin is Pakistan, and the largest country to prohibit wide categories of cryptocurrency use is China.

USE CASES

Industry and government can apply blockchain technology in a number of use cases that require shared governance, verifiable state, and/or resilience to data loss.

Financial use cases

Electronic currencies and payments

It is well known that blockchain technology can be used to build cryptocurrencies; Bitcoin is a working example of this. Blockchain technology enables electronic transactions that are resilient even when large amounts of money are at stake. Bitcoin has notable drawbacks that include low scalability, high energy consumption, and merely moderate privacy protections. A payment system using consortium governance can address the first two key challenges.

Asset trading

Financial markets allow the exchange of assets. They tend to involve intermediaries such as exchanges, brokers and dealers, depositories and custodians, and clearing and settlement entities. Blockchain-based assets—which are either intrinsically valuable or are claims on off-chain assets (material or digital)—can be transacted directly between participants, governed by smart contracts that can provide custodianship, and require less financial market infrastructure. Two key challenges are: (1) stapling for tokens that represent something off-chain (e.g., equity in a firm or a debt instrument); and (2) government oversight and regulatory compliance.

Markets and auctions

A central component of asset trading is the market itself—the coordination point for buyers and sellers to find each other, exchange assets, and provide price information to observers. Auctions are a common mechanism for setting a fair price; this includes double-sided auctions such as the order books in common use by financial exchanges. The key challenge for a decentralized market is that transactions are broadcast to the consensus protocol and thus nonconfidential, hindering privacy and enabling front-running.

Insurance and futures

Transactions can be arranged that are contingent on future times or events. Examples include a purchase of assets at a future time for a locked-in price, an insurance payout for a fire, or action on a loan default. The key challenges are: (1) determining trustworthy oracles to report relevant off-chain events such as fires, exchange rates, etc. (or limiting the contracts to on-chain events); and (2) choosing between a design that locks up so much collateral it can settle all possible eventualities, or a leaner design where the counterparty promises to fulfill its obligations but there is the *counterparty risk* that it will not.

Penalties, remedies, and sanctions

Legal contracts anticipate potential future breaches and specify a set of penalties or remedies. With blockchain technology, remedies for likely outcomes could be programmed (these could be later overturned through traditional litigation). As with insurance and futures, oracles and counterparty risk are key challenges.

Data storage and sharing use cases

Asset tracking

Blockchain technology can be used to track material assets that are globally distributed and valuable, and whose provenance is of interest. This includes standalone items such as artwork and diamonds, certified goods such as food and luxury items, dispersed items such as fleets of vehicles, and packages being shipped over long distances, which will change hands many times in the process. It also includes the individual components of complex assembled devices, where the parts originate from different firms. For heavily regulated industries such as airlines, and for military/intelligence applications, it is important to establish the source of each part that has been used, as well as a maintenance history (i.e., its provenance). Blockchain technology provides a common environment where no single firm has the elevated power and control of running the database that tracks this information. Key challenges are the reliable stapling of data, confidentiality, and onboarding all the necessary firms onto the same blockchain system.

Identity and key management

Identities, along with cryptographic attestations about properties for those identities (e.g., over 18 years of age, has a driver’s license, owns a specific cryptographic key), can be maintained on a blockchain system. This is a special case of asset tracking, where the “asset” is a person. The key challenges are the same.

Tamper-resistant record storage

The append-only ledger of a blockchain system can be used to store documents, including the history of changes to these documents. This use case is best suited for records that are highly valuable (such as certificates and government licenses), have a small data size, and are publicly available (as they will be replicated by all miners). If large and/or confidential documents need to be stored, a blockchain system might store secure pointers (i.e., binding/hiding commitments) for the documents, while the documents themselves are stored in a different system.

Other use cases

Voting

Electronic voting is a challenging problem that is often asserted to benefit from blockchain technology's properties. Shared governance could be used to ensure that multiple parties (the government, nongovernmental organizations, international watchdogs) can work together to ensure that an election is legitimate. Auditability is important in providing evidence to the electorate that the election was fair. Finally, the resilience of blockchain technology is important in preventing cyberattacks against the voting system. Voting on a blockchain system, however, has many challenges to solve: (1) blockchain systems offer no inherent support for secret ballots; (2) electronic votes can be changed by the device from which they are submitted (undetectably if a secret ballot is achieved); (3) cryptographic keys could be sold to vote buyers; and (4) key recovery mechanisms would need to be established for lost keys.

Gambling and games

Gambling is already very popular on Bitcoin and Ethereum. Players can audit the contract code to ensure that execution is fair, and the contract can use cryptocurrency to handle the finances (including holding the money in escrow to prevent losing parties from aborting before paying). This use case is best suited for gambling games that do not require randomness, private state, or knowledge of off-chain events.

APPLICATION

Ultimately, blockchain technology is not a panacea, but it is a useful tool when the overhead is justified by the system's needs. A good place to start is by posing the following questions:

1. Does the system require shared governance?
2. Does the system require shared operation?

If both answers to these questions are no, the overhead of blockchain technology is unnecessary. If both answers are yes, there is a good fit. If only one of the answers is yes—if only shared governance or shared operation is needed but

Related articles

➡ Bitcoin's Academic Pedigree
The concept of cryptocurrencies is built from forgotten ideas in research literature.
Arvind Narayanan and Jeremy Clark
https://queue.acm.org/detail.cfm?id=3136559

➡ Research for Practice: Cryptocurrencies, Blockchains, and Smart Contracts
Arvind Narayanan and Andrew Miller
https://queue.acm.org/detail.cfm?id=3043967

➡ A Hitchhiker's Guide to the Blockchain Universe
Blockchain remains a mystery, despite its growing acceptance.
Jim Waldo
https://queue.acm.org/detail.cfm?id=3305265

not both—then two more questions should be considered:
3. Is it necessary to audit the system's provenance?
4. Is it necessary to prevent malicious data deletion?

If auditability and data replication are critical, blockchain technology should be considered. This is because meaningful shared governance *and* operation require miners to audit the operations of others and to be able to recover data that a malicious miner might try to delete.

Even though blockchain technology does not solve all the problems that its proponents claim it does, it is nonetheless a meaningful technology that will continue to be used in industry and is deserving of further research and experimentation.

The majority of this work was completed while the authors (other than Jeremy Clark) were working at MIT Lincoln Laboratory.

References

1. Avizheh, S., Safavi-Naini, R., Shahandashti, S. F. 2018. A new look at the refund mechanism in the Bitcoin payment protocol. *Financial Cryptography and Data Security (FC 2018)*; https://arxiv.org/abs/1807.01793.
2. Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., Danezis, G. 2019. SoK: Consensus in the age of blockchains. *ACM Advances in Financial Technology (AFT 2019)*; https://arxiv.org/pdf/1711.03936.pdf.
3. Corbin, J., Strauss, A. 1990. Grounded theory research: Procedures, canons and evaluative criteria. *Zeitschrift*

für Soziologie 19(6), 418–427.

4. Digiconomist. 2019. Bitcoin energy consumption index; https://digiconomist.net/bitcoin-energy-consumption.
5. Garay J., Kiayias, A. 2018. SoK: a consensus taxonomy in the blockchain era. Cryptology ePrint Archive, Report 2018/754; https://eprint.iacr.org/2018/754.
6. Goldfeder, S., Kalodner, H. A., Reisman, D., Narayanan, A. 2018. When the cookie meets the blockchain: privacy risks of web payments via cryptocurrencies. *Privacy Enhancing Technologies (PETS 2018)* (4), 179-199; https://www.petsymposium.org/2018/files/papers/issue4/popets-2018-0038.pdf.
7. Kosba, A. E., Miller, A., Shi, E., Wen, A., Papamanthou, C. 2016. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In *IEEE Symposium on Security and Privacy,* 839–858; https://ieeexplore.ieee.org/document/7546538.
8. Nakamoto, S. 2008. Bitcoin: a peer-to-peer electronic cash system; https://bitcoin.org/bitcoin.pdf.
9. Narayanan, A., and Jeremy Clark, J. 2017. Bitcoin's academic pedigree. *acmqueue* 15(4); https://queue.acm.org/detail.cfm?id=3136559.
10. Ruoti, S., Andersen, J., Dickinson, L., Heidbrink, S., Monson, T., O'Neill, M., Reese, K., Spendlove, B., Vaziripour, E., Wu, J., Zappala, D., Seamons, K. 2019. A usability study of four secure email tools using paired participants. *ACM Transactions on Privacy and Security* 22(2), 13:1–13:33; https://dl.acm.org/citation.cfm?id=3313761&preflayout=tabs.
11. Ruoti, S., Kaiser, B., Yerukhimovich, A., Clark, J., Cunningham, R. 2019. SoK: Blockchain technology and

its potential use cases. Technical report. https://arxiv.org/abs/1909.12454

12. Schneier, B. 2019. There's no good reason to trust blockchain technology. *Wired*; https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/.
13. Siegel, D. 2017. Understanding the DAO hack. coindesk; https://www.coindesk.com/understanding-dao-hack-journalists.
14. Tamassia, R. 2003. Authenticated data structures. In *European Symposium on Algorithms*, 2–5. Springer; https://link.springer.com/chapter/10.1007/978-3-540-39658-1_2.
15. Wolfswinkel, J. F., Furtmueller, E., Wilderom, C. P. M. 2013. Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems* 22(1), 45–55; https://link.springer.com/article/10.1057/ejis.2011.51.

Scott Ruoti *is an assistant professor in the electrical computer and science department at the University of Tennessee in Knoxville. He obtained his Ph.D. from Brigham Young University, where his dissertation resulted in the creation of the first email encryption systems shown to be usable by the masses. His research interests include using blockchain technology to build and secure noncryptocurrency systems, improving the security and accessibility of password managers and two-factor authentication, and helping software developers create secure software. Contact him at ruoti@utk.edu.*

Ben Kaiser *is a Ph.D. student in the Center for Information Technology Policy at Princeton University. He obtained his B.S. and M.S. in computer science from Rensselaer Polytechnic Institute and worked at MIT Lincoln Laboratory on applied cryptography and secure computation. His current research agenda comprises interdisciplinary work with politics and sociology researchers examining how to detect disinformation websites, how news consumers perceive these sites, and how to best intervene to mitigate consumption and belief of disinformation.*

Arkady Yerukhimovich *is an assistant professor of computer science at George Washington University. Prior to joining the faculty there, he was a research staff member at the MIT Lincoln Laboratory working on applying cryptography to secure government computing systems. He received his Ph.D. from the University of Maryland, where his dissertation explored the fundamental limits of cryptographic constructions. His recent research is focused on developing cryptographic protocols for secure computation and database search, in particular on how these cryptographic tools can be used to secure large-scale systems such as cloud or blockchain systems.*

Jeremy Clark *is an associate professor at the Concordia Institute for Information Systems Engineering in Montreal. He obtained his Ph.D. from the University of Waterloo, where his gold-medal dissertation was on designing and deploying secure voting systems including Scantegrity, the first cryptographically verifiable system used in a public-sector* *election. He wrote one of the earliest academic papers on Bitcoin, completed several research projects in the area, and contributed to the first textbook. He has worked with several municipalities on voting technology and testified to both the Canadian Senate and House finance committees on Bitcoin. He has given more than 30 presentations on blockchain technology to government agencies, companies, investment funds, and other audiences. You can follow him on Twitter at @PulpSpy.*

Rob Cunningham *is the Associate Director for Cyber Assurance in the CERT division of the Software Engineering Institute, and an adjunct professor of cybersecurity at Carnegie Mellon University. Prior to joining CMU in 2018, he led a series of computer security groups at MIT Lincoln Laboratory. He received his Ph.D. in cognitive and neural systems from Boston University. He initially pursued research in machine learning, before turning to research measuring computer security, system security, and cryptographic protocols for secure storage and computation. Recently he has been exploring the implications of artificial intelligence on privacy and security. He regularly briefs the U.S. Government on technical matters related to computer security.*