What's the RUSH?

Is your company considering adopting the technology this year? Then let's be sure you understand what it is, what it isn't and what it means for security and privacy.

BY TUAN PHAN, CISSP

WHEN BITCOIN topped $19,000 per coin across the various crypto-exchanges around the world in 2017, cryptocurrencies drew worldwide attention beyond that of technology enthusiasts and crypto miners/traders. As a result, blockchain technology, which made Bitcoin possible, also entered the mainstream in a big way. Suddenly, everyone from product marketers to cyber pundits touted blockchain's potential to improve business processes, from recordkeeping and transaction tracking to many other back-office activities like asset management, procurement, inventory, financial reporting and tax preparation.

ILLUSTRATION BY JEFF MANGIAT

While supply chain applications are obvious, security ones are not. That hasn't stopped vendors from claiming the blockchain is the Next Big Thing. Is blockchain technology viable beyond cryptocurrency? What are the possible use cases and their drawbacks? Is blockchain ready for prime time? Can blockchain be the solution to the world's biggest problems? These are the questions that this article seeks to answer in defining and then identifying and assessing opportunities and obstacles for blockchain applications.

WHAT IS BLOCKCHAIN?

In *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World* (Portfolio, 2016), authors Don and Alex Tapscott describe the technology as "an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value." Specifically, in the blockchain technology stack, applications shift from centralized servers to transparent, secure and user-centric decentralized networks.

In essence, blockchain technology is a new operations paradigm that shifts trust from central bodies to codes and protocols using a one-stop technology platform.

In addition, blockchain technology incorporates architecture designs such as peer-to-peer computing (e.g., distributed networking) to provide high availability and resilience to lower the transaction costs for the blockchain network. It also provides cryptographical techniques to provide identification, authentication and authorization of transactions, as well as the immutability of the digital ledger.

To lower transaction costs and eliminate the need for a central authority, blockchain employs smart contracts (e.g., program codes or logic that run on the blockchain platform) and a consensus model that allows the distributed nodes to verify transactions and maintain the valid transactions in an immutable ledger.

In essence, blockchain technology is a new operations paradigm that shifts trust from central bodies to codes and protocols using a one-stop technology platform. This accelerates operational processing; reduces transaction costs; provides automation and standardization; and offers disintermediation or the elimination of the middlemen.

BLOCKCHAIN TECHNOLOGY AT WORK

It is difficult to disagree that blockchain technology is appropriate for managing cryptocurrencies, especially given there were more than 2,000 cryptocurrencies in existence as of September 2018. Cryptocurrencies thrive in untrusted environments like the internet and in the absence of central authorities, such as the country of the fiat currency or network operator.

However, for blockchain technology to become more widely accepted, its uses must extend beyond cryptocurrencies. Accordingly, drawing from the cryptocurrency space, three possible generic use cases for blockchain applications emerge.

Proof of ownership

The broadest use case for blockchain is proof of ownership. This encompasses all transactions that represent the lifecycle from acquisition to transfer of the ownership. Possible applications include real estate properties, financial instruments, loans, patents and trademarks. Proof-of-ownership applications should only be utilized for situations where ownership may be acquired (e.g., purchased), transferred (e.g., sold) and disputed (e.g., liened) and, accordingly, ownership information must exist or be available in a public forum.

Proof of chronology

The second popular use case is proof of chronology, which incorporates time and order with the proof of ownership to track transactions over time. Possible applications include the following:

- Regulatory reporting and compliance
- Accounting and auditing
- Financial management and procurement
- Federal personnel workforce data and appropriated funds
- Federal assistance and foreign aid delivery
- Clearance/background investigations
- Professional certifications
- Marriage certificates
- Auction/bid processes
- Clearing and settlement
- Escrow services
- Tracking of payments and deliveries
- Other goods and services in which time plays a key role in the fulfillment of the transactions (e.g., food spoilage)

Proof of existence (and identity)

The third generic use case is proof of existence, which does not consider the time aspect and simply demonstrates the existence of something, regardless of its lifecycle, to offer

integrity and assurance of legitimacy. Proof of existence can apply to internet domains, email addresses and corporation/brand names and, conversely, to records such as criminal convictions, debarments, fines and complaints.

Proof of existence can streamline and reduce the friction between multiple systems (e.g., reduction of paperwork burdens, prevention of data errors, reconciliation of transactions) by acting as a microservice to handle the finality of transactions among those systems.

Proof of identity may also be viewed as a special case of proof of existence as it leverages identification and authentication to prove identities. Practical applications of proof of identity include:

- Single sign-on services to websites
- Digital signatures
- Birth certificates
- Drivers' licenses
- Passports
- Visas
- Health benefit cards
- Other identity-related documentation

IMPACT OF BLOCKCHAIN TECHNOLOGY

One way to measure blockchain's potential impact is to consider the technology's integrity, scalability and, of course, security and privacy implications.

Integrity consideration

Integrity affects public and private blockchain environments differently. The public blockchain network exists in a permissionless environment where anyone can conduct transactions on the network with the appropriate software. Furthermore, the network is not controlled by a central authority, and the participants, both the users conducting the transactions and the nodes that verify the transactions, are not trusted.

Accordingly, user and node identities rely on the user/node public addresses and authentication is accomplished using the corresponding private key. Timestamped transaction data is shared node to node to ensure network concurrency.

To verify the validity of the transactions, each node races to examine its collection of transaction data, craft a new block for the transaction data needing processing and present that block to the peers.

The network selects and rewards the winning node to publish the block (e.g., making those transactions permanent by incorporating the valid block to each node's version of the ledger) from those that provide the fastest response time to the new block with the highest quality meeting a set of predetermined validation rules.

Meeting the fastest response time and the highest quality requirements are collectively known as proof of work (PoW), and this consensus model ensures that the integrity is maintained for the network through the consumption of computational resources (e.g., computer hardware, electricity). PoW provides strong integrity guarantees and tolerates up to a threshold of attacks (i.e., requiring attackers to gain at least 51 percent of the network's total hashrate in order to impact the network—what is called a "51 percent attack"). However, this type of attack actually needs at least 75 percent of the total nodes to work, to be honest.

Other than identification and authentication mechanisms and an immutable ledger, there is little similarity between public and private blockchain environments.

Other than identification and authentication mechanisms and an immutable ledger, there is little similarity between public and private blockchain environments.

A private blockchain network runs in a private, permissioned environment, typically with a designated network operator, where the participants are known to the operator and other participants. A private blockchain is costlier to operate and does not reward nodes (i.e., tokenless) as decisions are made using a voting scheme, typically the Byzantine Fault Tolerance (BFT) consensus model, where a set number of nodes agrees to the validity of a block of transactions.

BFT offers a greater degree of adversarial tolerance of up to 33 percent of the total nodes as malicious vs. 25 percent from PoW. A private blockchain also places stricter controls on privacy and access to the transaction data for the nodes, but it eliminates the computation and environmental impacts associated with PoW. This mechanism is necessary to provide transaction privacy for the participants, such as those in a network of buyers/consumers and suppliers/providers.

For example, a buyer using the same network may source the same product from multiple suppliers using different unit pricing based on the quantity and other intangibles uniquely negotiated between the buyer and the supplier (and, of course, kept private from other suppliers). In addition, instead of producing their own product for the buyer, the suppliers may choose to be the buyer themselves and resell the product using their own set of pricing and

other intangibles over the same network.

The integrity of the blockchain equates to the degree of trust. PoW requires transaction data to prove transaction history and binds that degree of trust to expending computing resources. The more resources consumed and transactions examined, the more trustworthy and, accordingly, the higher the integrity given to the blockchain.

By replacing the PoW with BFT, the nodes do not have any real consequence to submitting invalid blocks; therefore, they are more likely to yield inconsistent outcomes at the cost of availability. Accordingly, BFT may be unacceptable in scenarios where integrity in the transactions must be kept high.

The detraction from decentralization also impacts the integrity of a private blockchain. Nodes must still be compensated for providing the infrastructure that processes the transactions and this typically comes in the form of fiat currency provided by the network operator. As the payment does not make use of a utility token of the network, the integrity of the network may suffer since consequences for submitting invalid blocks are not considered. When coupled with the smaller number of nodes available, the network operator may exert more influence on the network than intended, requiring more trust to the network from the participants. This weakens the network's value proposition.

All of these factors may impact the network's availability and generate fraudulent or third-party interference, which may lead to censorship.

The immutability of the ledger can also be influenced by the selected environments.

Verified transactions are aggregated into a block and incorporated into the ledger based on an append-only approach on the time-order basis using the hashes of the transactions and the hash of the block header of the prior block. Accordingly, the chaining of the current block to previous blocks and so forth makes any attempt at altering past transactions extremely difficult and prevents tampering with the transactions after they have been accepted as valid. Any transactions not documented as part of the history are regarded as nonexistent.

However, if transactions were faultily recorded, possibly due to faulty underlying infrastructure design errors or incorrectly programmed smart contracts, how can they be corrected? For public blockchains the short answer is: They can't. Faulty transactions cannot be corrected and are generally accepted as is. For significant issues, major changes are accomplished through a major code update (e.g., a hard fork), which involves a complete ledger revamp across all impacted transactions to address the issue identified. Hard forks contradict the guiding principle of ledger immutability and are often contentious discussions within the blockchain community.

In the world of cryptocurrencies, hard fork debates have led to the creation of competing solutions such as Ethereum from Ethereum Classic and Bitcoin Cash from Bitcoin. By contrast, corrections of faulty transactions in private blockchains are trivial in nature as the design allows for such corrections to be facilitated by the network operator, an implied trusted central authority.

Scalability

One known limitation of current blockchain technology is the limited throughput, measured as transactions processed per seconds. On average, Bitcoin processes about seven transactions per second, compared to Ethereum (15 transactions per second) and Ripple (the fastest major cryptocurrency, at 1,500 transactions per second). For comparison purpose, the Visa network does around 24,000 transactions per second. The consequences of a slow transaction rate often result in a longer wait for individual transaction confirmation. Subsequently, there's less finality on the transactions due to a possible transaction rollback and, as a result, higher transaction fees.

Solutions to scaling include:

- Increasing the block size
- Separating signature from transaction data (e.g., Segregated Witness method)
- "Sharding" transactions
- Off-chaining transactions

Increasing block size makes nodes more expensive to operate, reduces the number of nodes and leads to more powerful centralized entities. Block size changes are more difficult on a public blockchain, requiring hard fork and often contested by the user community.

Sharding effectively breaks the blockchain into partitions of smaller chunks with their own independent piece of state and transaction history, allowing the throughput of transactions processed in total across all shards to be much higher than having a single shard do all the work as in a main blockchain.

Off-chaining allows for transactions to be processed off the main network and added to it later. Off-chaining violates decentralization, as the nodes performing such tasks must be explicitly trusted. While these technologies are promising in solving the scaling obstacles, they should be considered experimental at best.

SECURITY AND PRIVACY CONSIDERATIONS

From a security and privacy perspective, blockchain technology is not well understood due to the complexity of the components and infancy of the technology.

The design of the network architecture and access con-

trol plays a crucial role in reducing insider threats to the network. Requiring a minimum number of nodes to be properly connected, designated and authorized for participating in a federated or private blockchain consensus process is a good start to strengthening the security of blockchain technology. The minimum number should be at least large enough to provide adversarial protection that matches the degree of integrity required for the network. Since public blockchains are prone to the aforementioned 51 percent attack, care should be taken to ensure the network has enough geographically dispersed nodes to prevent any collusion from any one entity, any specific country or specific region of the world.

While it does not seem like much, for practical purposes, the keyspace is essentially infinite.

The possession of the private key proves both ownership and the assigned rights to execute certain transactions. Accordingly, security depends on choosing and protecting the private key. For example, Bitcoin's security model rests on a private key that composes an integer between 1 and 10^{77}. While it does not seem like much, for practical purposes, the keyspace is essentially infinite. As the private keys contain many digits, using the Wallet Import Format (WIF) reduces the private key into a sequence of characters and numbers shown below:

5GK67bPQuYpm884wtkJNzQGaCErckhHJBGFsvd3VymHfqcXj3hS

Or, most blockchain wallets can generate a series of words as backup (e.g., *body decision painful space bloom sunlight grown father sky third mirror jump*). Given their importance, take extreme caution whenever storing or transmitting private keys or safeguarding the backup words. Most software wallets provide user-friendly PINs, passwords or passphrases to encrypt and decrypt stored private keys and keep the encrypted wallet on the main hard drive of the user's computer. However, the keyspace for the wallet's PIN, password or passphrase must be sufficiently large to prevent being reversed using rainbow tables, particularly if the hash algorithm is known—such as documented by JAXX's known weakness for using the SHA256 hash algorithm for the four-digit PIN utilized for user authentication.

As most blockchain technology is open sourced, available documentation may not be up to date and formal training on specific blockchain platforms may also be limited. As a result, most developers are likely to be self-taught through

SMART CONTRACTS: What's in That Code?

AN INDEPENDENT REVIEW of Ethereum smart contracts revealed more than 100 errors or bugs per 1,000 lines of code. That is between two and six times the industry average, depending on the coding techniques.

The top two categories of issues relate to:

- Security flaws that resulted in the loss of money or control for users or owners
- Poor performance based on the description or code comments

In a 2018 publication, *Finding the Greedy, Prodigal and Suicidal Contracts at Scale* by Ivica Nikolic, et al., the authors proposed the use of MAIAN, an automatic tool for finding three different types of trace vulnerabilities in Ethereum smart contracts:

- Greedy for contracts that lock funds indefinitely
- Prodigal for contracts that leak funds carelessly to arbitrary users
- Suicidal for contracts that can be killed by anyone

The authors analyzed nearly 1 million smart contracts on Ethereum and found 34,200 (or 3 percent) with some form of trace vulnerabilities. The authors were able to properly confirm Parity Technology's Smart Contract multi-signature library as suicidal, which locked the Parity wallet and ultimately froze $150 million in Ethereum tokens when the contract was unintentionally exploited by an inexperienced developer. The event was deemed accidental because the developer did not gain from the event.

Accordingly, a blockchain deployment should use formal verification of secure coding practices through peer code review, formal testing and code regression maintenance to improve the quality of the smart contract and reduce the likelihood of these trace vulnerabilities.

—T. Phan

trial and error and therefore will likely make significant mistakes, which can lead to the presence of buggy code.

This makes smart contracts one of the most significant sources of weaknesses for blockchain security.

OTHER SECURITY ISSUES TIED TO BLOCKCHAIN CREATION AND MANAGEMENT

Patching security flaws on private blockchains follows best practices similar to other enterprise applications and, for the most part, only lightly impacts an enterprise. On the other hand, patching of public blockchains represents a unique challenge as significant changes may require a hard fork, as previously discussed, which may result in the creating a second blockchain and subsequent costs from reprocessing affected transactions.

Unlike public blockchains where the recovery of assets, user credentials or rollback of transactions is nearly impossible, private blockchains can be designed to provide mechanisms to facilitate these needs. As such, the loss of identification credentials may be addressed with a robust key management program. Organizations must consider the tradeoff and plan for data accuracy and correction vs. immutability of information. Also, a hard fork of codes may be expensive to implement post-event; therefore, consider installing pre-built transaction rollback mechanisms to append transactions to the rollback state, particularly for systems that manage physical or financial assets.

Unlike public blockchains where the recovery of assets, user credentials or rollback of transactions is nearly impossible, private blockchains can be designed to provide mechanisms to facilitate these needs.

Due to its inherent distributed nature, blockchain implementation must consider the rights of individuals to protect and erase their private information, particularly financial and health information. Instead of using actual data, privacy experts recommend using cryptographic hash references to provide evidence on the chain while limiting access to transaction data.

Other implementation possibilities may include the obfuscation of transaction data, additional safeguards to limit access control for the nodes and the participants, or the use of zero-knowledge proofs or "succinct arguments of knowledge" (SNARKs). SNARKs offer the greatest possibility for safeguarding privacy as they programmatically verify hidden inputs known only to the user to derive public known output that affirms the user without revealing any other information.

KEEPING AN EYE ON REGULATIONS

In many countries, regulatory focus on blockchain technology has been limited, with more focus on its promise to enable more optimal ways of doing business. As its use grows, however, expect regulators to follow as is already happening in places like Singapore and Switzerland, among others.

Positive trends are happening. Industry groups from financial services, healthcare and supply chain management to education, academia and others are rapidly forming to access blockchain technology in a legal and regulatory contest. There also are U.S.-based federal and state government working groups such as the Congressional Blockchain Caucus, Government Blockchain Association (GBA), Delaware Blockchain Initiative and Illinois Blockchain Initiative.

The 2018 Joint Economic Report released by the U.S. Congress makes the following recommendations:

- Policymakers and the public should become more familiar with the technology.
- Regulators should continue to coordinate to guarantee coherent policy frameworks, definitions and jurisdiction.
- Policymakers, regulators and entrepreneurs should continue to work together to ensure developers can deploy these new blockchain technologies quickly and in a manner that protects Americans from fraud, theft and abuse, while ensuring compliance with relevant regulations.

Several congressional bills related to blockchain and cryptocurrencies have also been proposed to protect against being leveraged for money laundering, counterfeiting, terrorist financing and tax evasion.

IS BLOCKCHAIN READY FOR PRIME TIME?

We are still at the beginning of a blockchain revolution.

The technology, while complex and technical to implement, potentially offers significant improvements to existing processes and methods. It creates new business models and corresponding opportunities.

However, blockchain technology is not a panacea to resolve issues with existing processes. Therefore, organizations need to understand their true needs prior to adopting blockchain technology.

Popular use patterns for evaluations

When considering use cases, organizations can apply the following use patterns in their evaluations. The absence of one or more of the patterns may indicate a poor fit for blockchain applications.

The most important use pattern for an ideal blockchain is the cost of trust currently performed by the "trusted" intermediaries. In the current transaction models, these are entities that operate, safeguard, oversee and ensure transactions for banks, insurance companies, lawyers, etc. Indirectly, they serve as a quasi-central authority to support the networks. However, their participation adds unnecessary transaction costs and controls on the network, both of which conflict with the blockchain's disintermediation and lack of authority value proposition.

The type of data and the methodology for their use also is central.

Decentralization must be chosen over centralization, as the latter requires implicit trust that contradicts blockchain's trustlessness value proposition. Accordingly, managed data must be sharable or be able to exist on a public forum.

The open access serves as notice for any disputes with the claimed ownership information. For example, in the U.S., real estate properties can be readily retrieved from states' departments of tax administration because that information is considered public record. In contrast, health, income tax and financial records do not exist in the public domain. In these instances, privacy takes precedence over transparency due to the limited sharing of information. Furthermore, a certain degree of trust must be placed on the network operator who becomes the custodian and facilitator of the sensitive data.

Also central to blockchain's value proposition is the ability to provide immutability and integrity to transactions in a logistic chain. Consequently, transaction data must be available so that the nodes can compute their version of the digital ledger and confirm the transaction history. By limiting access to the data, the certainty of the ledger is diminished. Although it may be overcome by new methods such as SNARKs, more thorough testing is still needed on a larger scale to demonstrate the viability of these approaches.

Blockchain technology still has critical obstacles to overcome, such as enhancing security without compromising network performance and honoring both transparency and privacy.

Organizations wanting to adopt blockchain technology should approach with caution as there are many hidden costs to consider, including mapping and reengineering existing processes to work in a blockchain scenario. Acquiring or training staff with the specialized skills to develop, implement and maintain the technology can add significant costs too.

Do your due diligence now so that everyone in the organization thoroughly understands how a blockchain application will work and how much time, talent and effort is required. That includes working through security and privacy issues before they become problems. Doing all of this not only will help determine blockchain's viability within an organization, it will also help ensure sensitive data cannot be compromised. That is one way to realize a strong return on investment for a technology still in its infancy. ■

TUAN PHAN, *CISSP, PMP, Security+, SSBB, is a partner with Caplock Security LLC, where he also serves the practice leader for blockchain technology. He is leading the development of several proofs of concept using Hyperledger Fabric and Ethereum private blockchains and implementing security audits of blockchain technology. Tuan can be reached at tphan@caplocksecurity.com.*

A RELATIVELY NEW INDUSTRY
Needs New Experts

THE ADOPTION OF BLOCKCHAIN technology and smart contracts will require specialized skillsets. According to a recent study conducted by Burning Glass Technologies, an analytics software company based in Boston, the demand for blockchain expertise grew by 115 percent in 2017, with similar gains reported by many technical job search sites.

Salaries are growing as well.

The freelance job website Upwork recently showed numerous positions for blockchain developers paying upwards of $150 per hour. Many blockchain startups are also offering a combination of equity, bonuses and other perks for onboarding and retaining qualified blockchain developers. Many of those rewards are reminiscent of incentives from the late 1990s, before the dot-com bubble burst.

—T. Phan