A Blockchain Buyer's Playbook Part 2

Compliments of

SEPTEMBER 21, 2019

Caplock Security LLC

Tuan Phan, CISSP, CBSP, PMP, Security+, SSBB

Introduction

In Part 1 of the Playbook, we discussed that blockchain solutions seek will likely displace traditional services across a variety of industries through efficiency and lower costs. For the financial institutions, we highlighted several specific use cases where blockchain technology has started to reshape the way financial services are structured, provisioned and consumed. We provided patterns to assist organizations to better understanding if blockchain technology may be a good fit for a proposed application or project.

We covered key concepts of blockchain in details to provide the minimum background understanding required in applying the technology. While blockchain technology may be complex and technical to implement, it potentially offers significant improvements to existing processes and methods. In other words, blockchain technology can and have created new business models and corresponding opportunities. However, blockchain technology is not a panacea to solve or improve existing processes, and therefore, organizations need to understand what their true needs are before embarking on the adoption of blockchain technology.

In Part 2 of the Playbook we will dive in the constraints and limitation of blockchain technology and how to avoid the pitfalls of blockchain implementation.

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.

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 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; and
- 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 are 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.

Regulatory Perspective. Domestically, in 2018 regulatory focus on blockchain technology has been limited to its promise as enabler for more efficient and optimal ways of doing things and less on the regulatory roadmap in contrast to countries such as Singapore, Switzerland, etc. Positive trends are noted with the rapid forming of industry groups from financial services, healthcare and supply chain management to education and academia and others, as well as federal and state government working groups such as the Congressional Blockchain Caucus, Government Blockchain Association (GBA), Delaware Blockchain Initiative and Illinois Blockchain Initiative. 2018 was the year of

promoting blockchain adoption as indicated by the 2018 Joint Economic Report released by the U.S. Congress with 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."

In 2019, the regulatory landscape shifts to concerns of money laundering using cryptocurrencies with the introduction of several congressional bills related to blockchain and cryptocurrencies to protect against money laundering (BSA, AML), counterfeit, terrorist financing (CTF) and tax evasion (KYC). These bills include:

- Illicit Cash Act
- The Virtual Currency Consumer Protection Act of 2019
- U.S. Virtual Currency Market and Regulatory Competitiveness Act of 2019
- Fight Illicit Networks and Detect Trafficking Act ("FIND Trafficking Act")
- Homeland Security Assessment of Terrorists' Use of Virtual Currencies Act
- FinCEN Improvement Act of 2019
- The Financial Technology Protection Act
- Blockchain Regulatory Certainty Act

As of September 2019, most bills have passed the US House of Representatives and are pending before the US Senate.

Internationally, the recent quarter of 2019 saw jurisdictions compete for crypto business based upon regulatory vision and completeness of implementation. The charts below show the widely varying levels of maturity and sophistication in AML/CTF regimes around the globe. The gaps in these regulations present risky avenues that can be exploited by money launderers and terrorist organizations. Specifically, the money laundering potential of crypto-to-crypto exchanges and privacy coins are not well addressed by lawmakers attempting to regulate digital assets based on the physics of fiat currency.

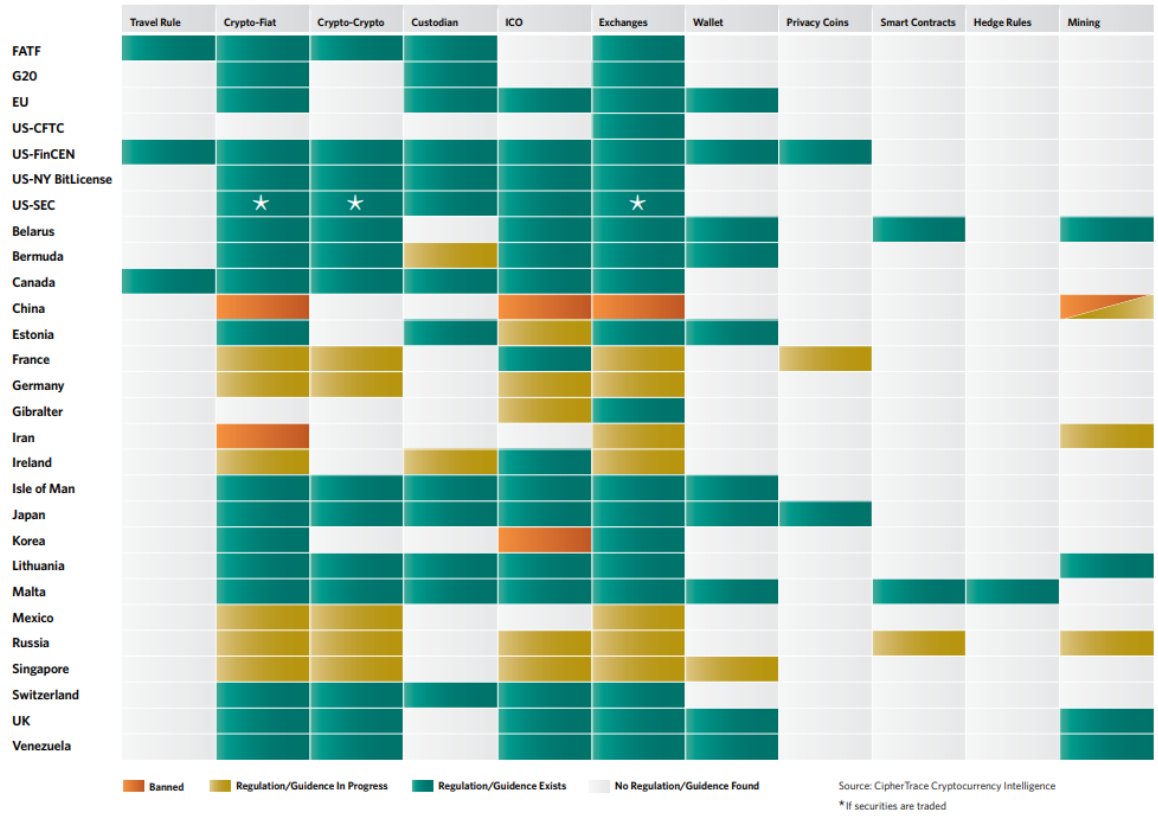

Figure 1 – Global Implementation of AML/CTF

Expertise. The adoption of the blockchain technology and usage of smart contracts across businesses will require new talents with specialized skillsets. According to a recent study conducted by ZipRecruiter.com, blockchain jobs pay at a medium of $146,183 per year similar to salary ranges reported by many technical job search sites. Freelance developers are also doing well, due to the lack of general availability of blockchain-specific experience, with billing rates exceed $150 per hour.

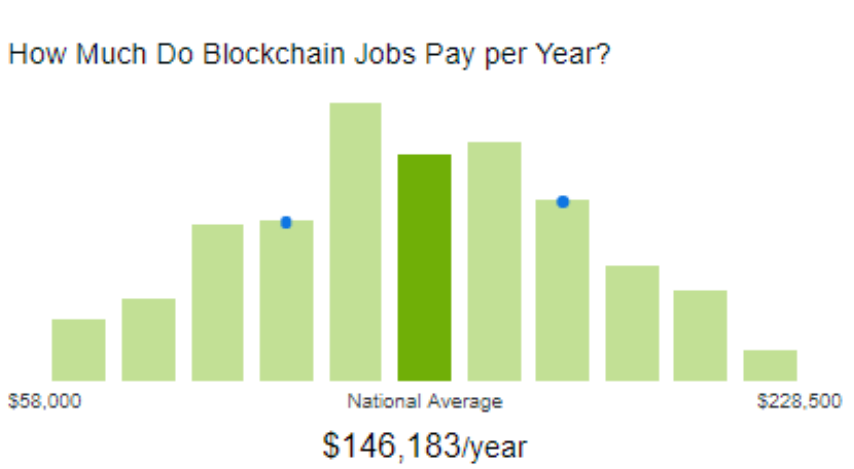

Figure 2 – 2019 Salary Survey of Blockchain Professionals (ZipRecruiter.com)

The adoption of the blockchain technology and usage of smart contracts may need to be certified to meet the requirements of regulatory bodies and ongoing audits and certifications. This demand requires the upskilling of the workforce impacting the employees, auditors and the consultants, to gain a deep understanding of inner working functions of specific blockchain technologies (e.g., Ethereum, HyperLedger, etc.) and technical programming language for the smart contracts. For quality assurance and internal/external audits, the auditing process may become more automated, and less a burden on the entity's staff as auditors can deploy automation to the blockchain to extract information and analyze transactions in real-time. Accordingly, the blockchain technology does not likely to displace current audit professionals but will likely transform the way in which auditors extract, test and analyze data supporting financial and/or internal control attestation. At the minimum, blockchain technology will upskill professionals in the audit and information technology security areas.

Interoperability and System Integration. Integration with legacy financial systems running on several different platforms such as mainframes, web servers, database services, and more recently, web services or microservices remains to be an ongoing challenge, specifically with key management and the handling/integration of hardware modules (HSMs) for key storage and generation and security infrastructure such as VPNs. Typically, data integration and exchange to legacy systems are handled through the implementation of a secure web interface such as APIs using programming languages such as JavaScript, .NET, or Python, however, the implementation, in most

cases, requires some custom coding which can impact ongoing interoperability as systems are updated.

Security Considerations. From a security perspective, blockchain technology is not well understood by most professionals due to the complexity of the components and infancy of the technology. Attacks on blockchain networks typically target on four key components, and are dependent on the type of the blockchain network:

- The Infrastructure (network itself)
- The Nodes
- The Users
- The Smart Contracts

As blockchain solutions rely on more complex supporting infrastructures such as multifactor authentication and API, the attack and exploitation may not be in the blockchain solutions themselves as highlighted by the hack that took place at the world's number-one cryptocurrency exchange, Binance. The hackers stole over 7,000 bitcoins (worth US$40 million at the time). From what is known by researchers, hackers employed a variety of techniques, including phishing, viruses and other multi-pronged attacks to obtain API keys, two-factor authentication codes, and other personal information from a large number of users, including "very high net worth accounts." The hackers structured the transactions in a way that passed Binance's existing security checks. By the time Binance was able to suspend withdrawals, the hackers had already gotten away with the millions in cryptocurrency.

Similar exploits were also carried against GateHub and resulted in a loss of US$10 million. According a statement by GateHub, hackers penetrated the wallets after gaining access to a database that contained valid customer access tokens. These credentials essentially tell a server who the users are and keep them logged in. When a user logs out, the access token is destroyed, and the user must log back in to receive a new one. Broken authentication such as compromised access tokens is number two on the OWASP's top 10 attack vectors.

These two cases highlight the importance of the design of the network architecture and access control plays a crucial role in reducing both insider and outsider threats to the network.

Node management also plays a crucial role in securing the blockchain network. Eclipse attacks, where the attacker seeks to isolate to launch attack against a specific user, can be thwarted by requiring a minimum number of participants or nodes (between 8 to 13 nodes) to be properly connected.

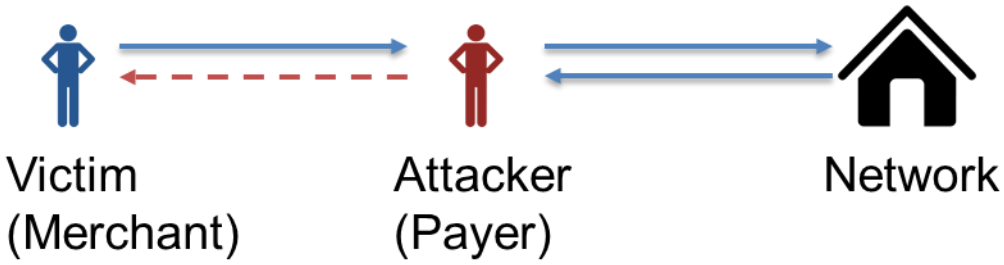

Figure 3 – Eclipse Attack

Additional controls may include designating authorized nodes (e.g., whitelisting of nodes) for participating in a federated or private blockchain consensus process, increase the number of connections, randomize the node selection process especially those participate in consensus, and limit the number of nodes per IP/machine.

Public blockchains are prone to 51% attack, where the attacker seeks to take advantage of the PoW consensus algorithm to achieve a double-spend condition. Therefore, care should be taken to ensure the network has enough nodes that are geographically dispersed to prevent any collusion from any one entity or any specific nation. In other words, for a public blockchain, the size and security of the network is directly correlated to its network hashrate, and conversely, one can infer from the network hashrate the maturity and the adoption of the blockchain technology. Other mitigation for 51% attack includes the usage of checkpointing (i.e., by storing a block in the history of the blockchain at intervals and refusing to accept divergent blockchains without these blocks), prevent the use of ASIC miners (e.g., Bitmain miners), and increase the number of block confirmations before locking in the finality of transactions.

Patching of security flaws on private blockchains follows best practices similar to other enterprise applications and, and for 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 which may result in the creation of a second blockchain. Hard fork does not guarantee the adoption of the change as the roll back may correct previous blocks/transactions that were previously deemed invalid as valid. These issues were highlighted in the infamous Decentralized Autonomous Organization (DAO) hack that resulted in the loss of $50 million of ethers and the subsequent hard fork that split into Ethereum and Ethereum Classic.

Nodes supporting blockchain network are also prone to attacks and vulnerabilities. Cryptojacking attacks, where the attacker leverages phishing to load cryptomining code onto mining nodes or user computers. These malware exploits known or misconfiguration in browsers. Real world examples include Remote Manager Exploit, BadShell and CoinHive. Standard mitigations are available including conducting security audits and security awareness training with focus on phishing prevention, installing ad-blocking or anti-cryptomining extension into browsers, and usage of endpoint protection and web filtering tool.

Attacks on the users uses common attack methods such as phishing and malware to steal the private keys and/or user credentials. The possession of the private key proves 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 composes of an integer between 1 and 1077. While it does not seem like much, for practical purposes, the keyspace is essentially infinite. As the private keys contain many digits, Wallet Import Format (WIF) is utilized to reduce the private key into a sequence of characters and numbers shown below:

5GK67bPQuYpm884wtkJNzQGaCErckhHJBGFsvd3VymHfqcXj3hS

Figure 4 – Notional Bitcoin Address

Given their importance, extreme caution must be taken whenever storing or transmitting private keys and the selection of the software wallets as not all wallets are

equally secured. Most software wallets provide user-friendly PINs, passwords or passphrases further to encrypt and decrypt the private keys stored within and keep the encrypted wallet on the main hard drive of the user computer.

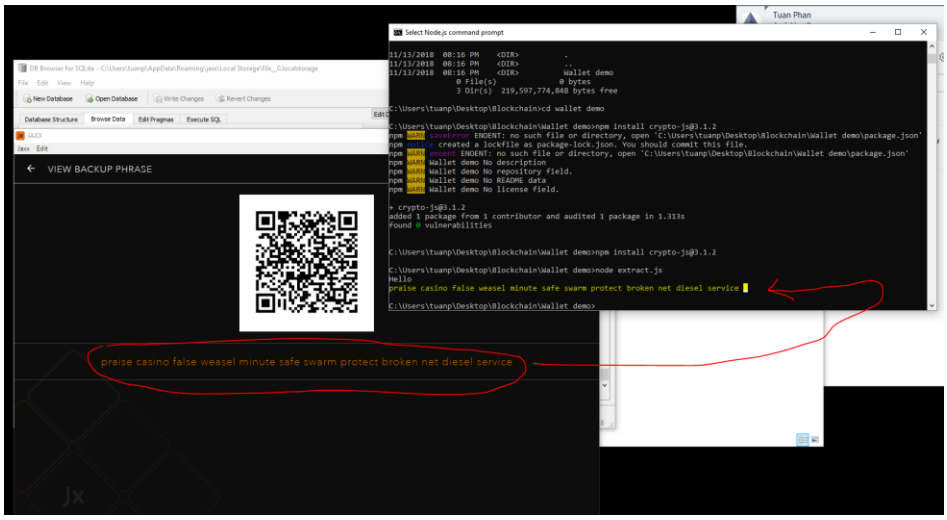

Figure 5 – Extracted Seed Words from an 'Encrypted' JAXX Wallet

However, the keyspace for the wallet's PIN, passwords or passphrase must be sufficiently large to prevent the extraction of sensitive data such as wallet seed words (as demonstrated by the author above) using either decryption cracker or rainbow tables particularly if the hash algorithm is known such as documented by JAXX's usage of SHA256 hash algorithm of the four-digit PIN utilized for user authentication.

As most blockchain technology is open-sourced, available documentation may be not be up to date and formal training on specific blockchain platforms may also be limited. As the result, most developers are likely to be self-taught through trial and error and therefore will likely make significant mistakes, which can lead to the presence of buggy codes. In addition, the developers may not be aware of coding best practices pertaining to these nascent smart contracts. This lack of awareness makes smart contracts one of the most significant sources of weaknesses for blockchain security, as attackers seek to exploit one or more of the following vulnerabilities in smart contracts:

Access Control	Timestamp Manipulation
Default Visibility	Bad Randomness
Reentrancy	Front Running

Integer Over/Underflow	Denial of Services
Unchecked Return	Short Address

Table 1 – Common Vulnerabilities in Smart Contracts

For example, a review of Ethereum smart contracts indicated bugs per line of code exceeds 100 per 1000 lines, or between 2X to 6X the industry average depending on the coding techniques. The top two categories of issues related to:

a. Security flaws that resulted in the loss of money or control for users or owners.
b. Doesn't do what it claims either in the description or code comments.

In another study published in 2018, "Finding the Greedy, Prodigal and Suicidal Contracts at Scale" by Ivica Nikolic, et. al., the authors analyzed nearly one million smart contracts on Ethereum and found 34,200 (or 3%) had some form of trace vulnerabilities based on the MAIAN tool as follows:

- Greedy – Contracts that either lock funds indefinitely
- Prodigal – Contracts that leak funds carelessly to arbitrary users
- Suicidal – Contracts that can be killed by anyone

Case in point, MAIAN analysis described in previously, properly identified the Parity Technology's Smart Contract multi-signature library as suicidal which caused a lock to the Parity wallet resulting in the freezing of a $150M of Ethereum tokens when the contract was accidently exploited by an inexperience developer.

The most effective mitigation for vulnerabilities relating to smart contracts is the use of formal verification of secure coding practice through security audits, peer code reviews, formal testing and code regression maintenance would have been averted these trace vulnerabilities. In addition, publicly released security audits, such as those shown below, give greater confident to general end-users that the smart contracts have been vetted by security professionals, and are likely to have a lower risk profile compared to unvalidated smart contracts.

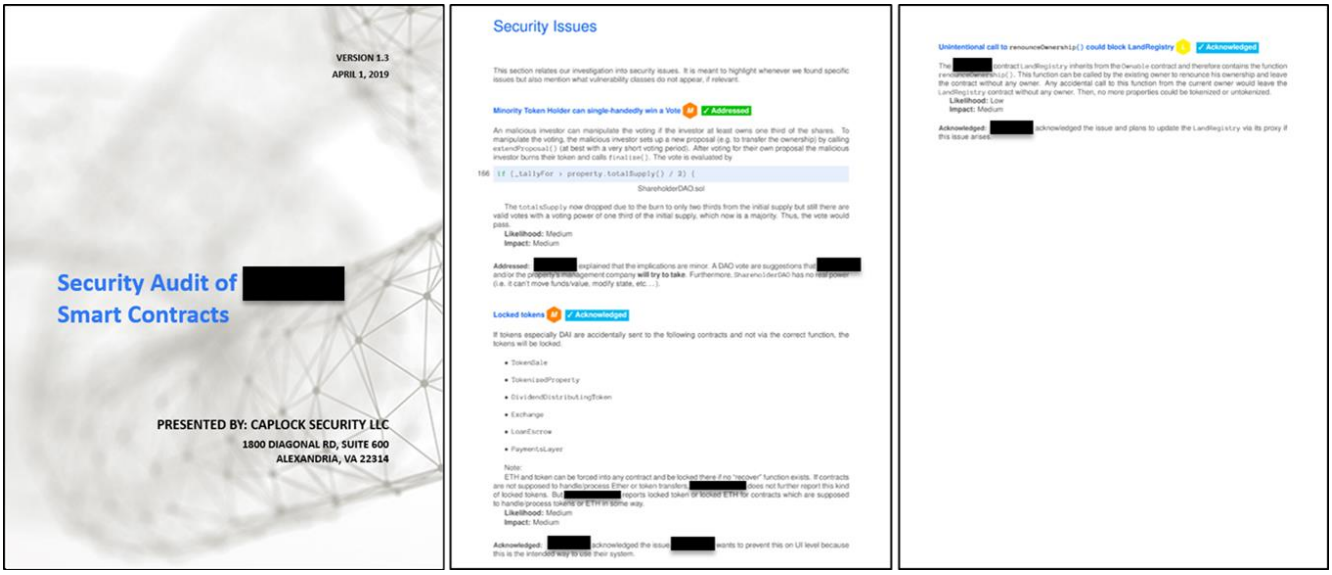

Figure 6 – Sample of Security Audit on a Smart Contract

Privacy Considerations. Unlike the public blockchains where the recovery of assets, user credentials or roll back of transactions is nearly impossible, private blockchains must provide mechanisms to facilitate these needs. Regulations such General Data Protection Regulation 2016/679 (GDPR) and the California Consumer Privacy Act (CCPA) stress the need for blockchain solution to provide data protection and privacy for all individual users of the solutions within EU and the state of California as an example. Accordingly, organizations must consider the tradeoff and plan for data accuracy and correction vs. immutability of information. Hard fork of codes may be more costly to implement post-events than pre-built transaction roll-back mechanisms to append transactions to the roll back state, particularly for systems that manage physical or financial asset.

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. Accordingly, instead of using actual data, better privacy implementation should use cryptographic hash for evidence on the chain. Other privacy implementation may be provided by the blockchain platform. For example, Hyperledger Fabric allows the use of channels for private information exchanges between selected members within a larger network as shown below:

Figure 7 – Channel within Hyperledger Fabric

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.

Summary

We discussed the limitations and constraints of blockchain solutions, particularly security and privacy concerns to the potentials for large-scale financial and data losses due to the large number of attack surfaces across the blockchain network, including the infrastructure, nodes, users and smart contracts. We stressed the importance of performing ongoing security audits on the blockchain network and its components using qualified security professionals.

We cautioned organizations to tread softly into the space as supporting blockchain technology requires specialized and hard-to-find expertise. This may require significant investments into infrastructure, the reengineering of existing processes, adding

specialized skill staff and enhancing the training and development of existing staff – which all add significant costs to the enterprise.

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 issues. 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.

Caplock Security and its partners thank you for your time and ongoing support. We welcome your feedbacks on our Blockchain Technology Playbook.

Tuan Phan, CISSP, CBSP, 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 202-780-5455 or tphan@caplocksecurity.com.