The International Journal of Digital Accounting Research
Vol. 19, 2019, pp. 103-144
ISSN: 2340-5058

# A Cybersecurity Control Framework for Blockchain Ecosystems

**Jesús Canelón,** California State University San Bernardino, USA jesus.canelon@csusb.edu

**Esperanza Huerta,** San José State University, USA esperanza.huerta@sjsu.edu

**José Incera,** Instituto Tecnológico Autónomo de México, Mexico jincera@itam.mx

**Terry Ryan,** Claremont Graduate University, USA terry.ryan@cgu.edu

**Abstract.** This paper proposes a cybersecurity control framework for blockchain ecosystems, drawing from risks identified in the practitioner and academic literature. The framework identifies thirteen risks for blockchain implementations, ten common to other information systems and three risks specific to blockchains: centralization of computing power, transaction malleability, and flawed or malicious smart contracts. It also proposes controls to mitigate the risks identified; some were identified in the literature and some are new. Controls that apply to all types of information systems are adapted to the different components of the blockchain ecosystem.

Keywords: blockchain, cybersecurity, internal controls

## 1. INTRODUCTION

In this paper, we develop a framework for cybersecurity controls for blockchain ecosystems. The ability of blockchains to store immutable records has made them

DOI: 10.4192/1577-8517-v19_5

*Submitted May 2019*
*Accepted November 2019*

attractive for many business applications. Although heralded as an ecosystem with tamper-proof mechanisms, disclosed cyberattacks on blockchains have made evident that, as is true for any other system, blockchains should implement internal controls to ensure the security of the information they hold. Among the many controls for blockchains, given their decentralized and multiuser nature, cybersecurity controls are of the utmost importance.

Although cybersecurity controls in blockchains are relevant to many professionals—from information technology managers to software developers—accountants have a primary role in understanding, implementing, and assessing the strength of those controls. Accountants are responsible for ensuring the reliability of the information reported in financial statements; the interactions between blockchains and accounting information systems make accountants responsible for overseeing blockchain controls. Similarly, auditors are responsible for evaluating blockchain controls to the extent that blockchains are integrated with financial reporting. Although standards and guidance are lacking, external auditors are already offering attestation services for independent evaluations of blockchain controls (Rapoport, 2018).

Control frameworks are purposely broad because they intend to apply to any type of information system. As a result, there is little guidance on controls specifically designed for blockchains. To the best of our knowledge, only ISACA (2019) has issued formal guidelines on the audit of blockchains. One of the reasons for this lack of guidance for blockchain controls is that most controls apply to any type of information systems. For instance, access controls should be implemented and enforced regardless of the type of application. Another reason for the lack of guidance for blockchain controls is the fast pace at which the blockchain industry is developing. Although blockchains share some of the cybersecurity controls required for any information systems, blockchains have unique characteristics that warrant special consideration of cybersecurity controls specifically designed for the blockchain ecosystem.

To develop our framework, we first conducted a comprehensive review of the practitioner literature to identify publicly disclosed attacks on blockchains. We supplemented this review with an examination of academic articles to identify the vulnerabilities of blockchains. These assessments served as a starting point for identifying risks to the different components of the blockchain ecosystem. The

framework includes different components of the ecosystem, such as oracles and arbitrators because, although they are external to the core blockchain technology, the information they provide impacts the reliability of the information stored in the blockchain.

The framework emphasizes risks and controls rather than the technology behind blockchains; however, we provide an appendix describing cybersecurity threats. The appendix is intended to facilitate the understanding of cyber threats for accountants and accounting students with limited technical knowledge. This framework can be used to develop standards for blockchain audits, to foster academic research in blockchain cybersecurity controls, to introduce students and faculty to the blockchain ecosystem, and to guide updates in the accounting curriculum. In addition, this framework contributes to prescriptive knowledge by identifying risks and proposing associated controls that can inform design science research in blockchain. Prescriptive knowledge, as the name implies, gives instructions and recommendations on how to accomplish a goal (Gregor and Hevner, 2013). Design science research can use this framework when designing real world blockchain applications.

This paper is organized as follows. The first section provides a brief explanation of the different components of the blockchain ecosystem. This section aims to provide the necessary background for understanding the interaction among blockchain components. The literature review section describes the review of the practitioner literature reporting cybersecurity attacks on blockchains. We present a comprehensive list of known blockchain security events, including attacks on blockchain instances, in Appendix 2. The risks and controls section describes cybersecurity risks to blockchain ecosystems and propose controls to mitigate the risks. We summarize the controls in a cybersecurity control framework. Finally, we discuss the limitations and potential areas for research.

## 2. BRIEF DESCRIPTION OF THE BLOCKCHAIN ECOSYSTEM

Control frameworks organize and categorize internal controls to reasonably ensure that financial reporting is reliable and that operations are effective, efficient, and in compliance with laws and regulations. The cybersecurity control framework we propose, includes the blockchain itself and additional components of the blockchain ecosystem. A blockchain stores data (typically, transactions) in a set of

blocks linked together by commonly agreed rules. For the blockchain to be of any use, there are many other components (such as the users or transaction stakeholders, the validating rules and consensus mechanisms, the interfaces with the physical world) that must interact together as a system. In this paper, we refer to such a set of interacting components as a blockchain ecosystem. We provide below a brief description of the typical components in a blockchain ecosystem. The first public application of a blockchain, Bitcoin, initially included only two components, nodes and wallets. Wallets are the means for owners to keep and transfer their tokens, and nodes are the bookkeepers. Nodes make up the backbone of a blockchain, as each node keeps a copy of the ledger; that is the reason why a blockchain is described as a distributed ledger. As blockchains have evolved to support different transactions, additional components have been added to the ecosystem. Table 1 describes the tasks performed by the components of the ecosystem.

| Component | Tasks |
|---|---|
| Node | Receives transaction from wallets or other nodes. Validates transactions. Groups transactions into blocks. Appends blocks to the chain. Keeps a copy of the entire blockchain. |
| Wallets | Sends or receives tokens through simple transactions or transactions embedded in smart contracts. |
| Smart contract | Executes a transaction when the conditions programmed are met. |
| Oracles | Provides information to the blockchain about events in the real world. |
| Arbitrators | Referees disputes in transactions. |
| Web exchanges | Executes transactions on behalf of wallet owners. |

Table 1. Components and tasks in a blockchain ecosystem

The sequence of recording transactions in a typical blockchain starts when a sender transfers tokens to a receiver. The wallet of the owner broadcasts the transaction to several nodes, which in turn rebroadcast the transaction to other nodes; as a consequence, nodes do not receive transactions at the same time. Nodes validate the transactions received by verifying, among other things, that the sender owns enough tokens to transfer to the receiver. In addition to validating transactions, nodes group transactions into new blocks. Because there can be delays in propagating the information, the transactions grouped by each node can

be different. Figure 1 provides a broad overview of the actions of wallets and nodes in a basic blockchain.

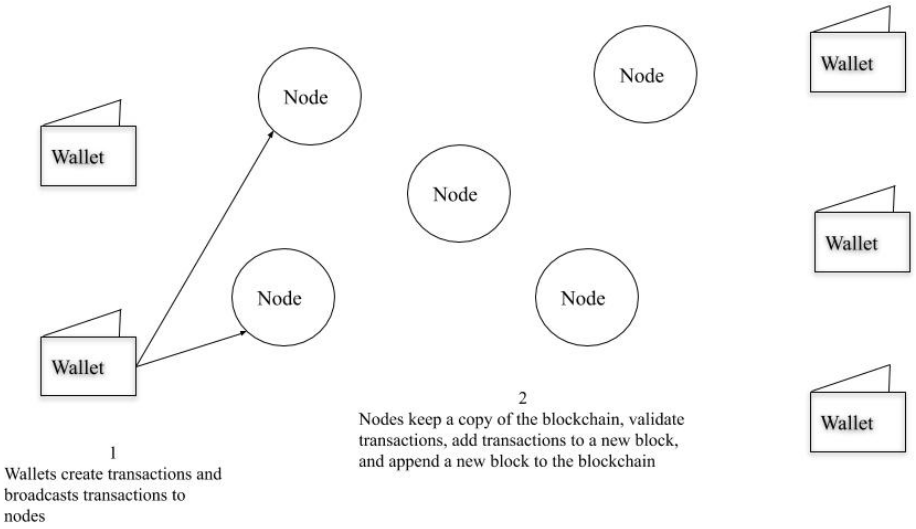


Figure 1. Actions of wallets and nodes

A node appends a newly created block (N+1) to the last validated block (N), creating a chain of blocks from which blockchain gets its name. When block N+1 is added to the blockchain by a node, other nodes verify that all the transactions in the block are valid, and if so, append the new block to their local copy of the blockchain. If the block has invalid transactions, the nodes reject the proposal to append block N+1 to the blockchain, keeping N as the latest block in the chain.

Blocks have two distinct parts: the body that contains the transactions and the header that contains information about the current block and the previous block. The immutability of records in a blockchain is achieved by using unique identifiers calculated with mathematical functions (called hash functions) applied to the content of the blocks. Block N stores in its header a unique identifier of the content of its own body. The header of block N also includes a unique identifier of the entire content (body and header) of block N-1. The unique identifier can only

be calculated based on the given content and not with any other content; even a change in a single bit results in a different unique identifier. The immutability of the records in a blockchain is achieved because identifiers can be recalculated and compared with the original identifier stored in the header of blocks at any time. When the original and recalculated identifiers match, the content has not been altered; when the identifiers do not match, the content has been altered. Figure 2 depicts the structure of blocks and the unique identifiers based on the contents.

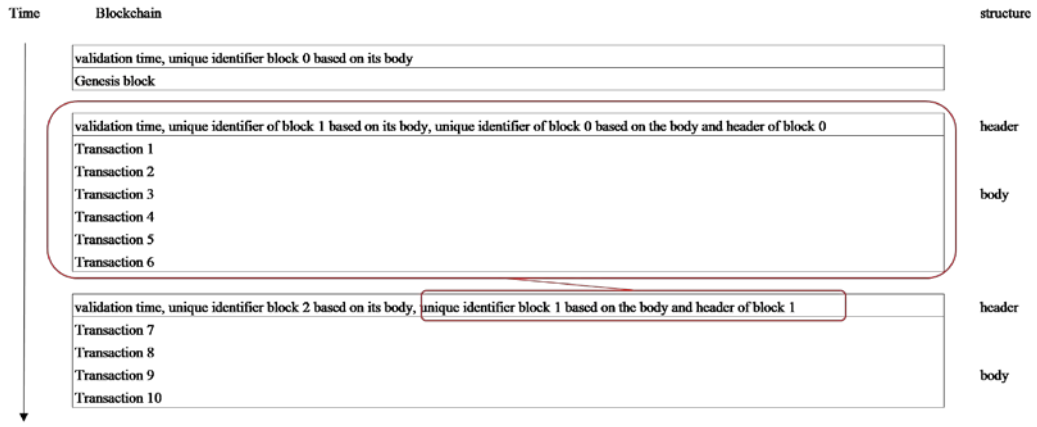


Figure 2. Structure of blocks and unique identifiers

In blockchains, tokens are unique; the transfer of tokens from one owner to another is managed by validating the ownership of the tokens with the digital signature of the owner. Tokens may represent digital cryptocurrencies, such as Bitcoin's BTC, Ethereum's Ether or Ripple's XRP. More generally, tokens are digital assets that may represent tangible assets such as diamonds, real estate, food and goods in a supply chain or kilowatts of energy. Tokens might also represent intangible assets, such as copyrights, software licenses, voting rights, identity management and academic credit validation. When a person receives tokens, the tokens are “locked” with the digital signature of the receiver, making the receiver the owner of the tokens. The tokens can only be redeemed (“unlocked”) with the owner’s digital signature (Antonopoulos, 2017). When a sender creates a transaction, the sender unlocks the tokens with his/her digital signature and transfers the ownership of the tokens to the receiver.

When tokens represent assets related to the physical world, the blockchain system needs a mechanism to interact and retrieve information from the physical world. For instance, if a blockchain tracks the supply chain of electronics components, it

may require access to the systems of the manufacturers, transportation companies, customs, and any other intermediary, until the electronic components reach their final destination. Oracles are the blockchain component tasked with providing a blockchain with information about the physical world.

Private, permissioned blockchains, may add a component known as a Membership Service Provider (MSP) to validate the identity of the members, as well as to manage access and permissions. For instance, an MSP manages which members can access read-only, validate transactions, and create and append blocks.

## 3. LITERATURE REVIEW

We started our inquiry by conducting a comprehensive literature review to identify publicly disclosed attacks on blockchains. A search was conducted of both academic and practitioner literature to identify publications concerning various combinations of the terms "blockchain" and synonyms for "attack." Several databases, including ProQuest, were searched, as was Google Scholar. Although hundreds of publications mentioning blockchain and some notion of attack were found, most of these concerned how blockchain could be used to deter attacks, rather than how blockchain instances have been attacked. A final set of 66 publications, scholarly articles, blog postings, practitioner white papers, and web

pages, discussing a total of 36 events, were thoroughly analyzed to appreciate what is known publicly concerning attacks on blockchain. Of course, as is true with any analysis of attacks on business firms, it may be true that some (or even most) of the actual attacks that have occurred have not been publicized. This literature review can inform design science research by identifying one of the problems that blockchains need to solve, namely protecting the integrity of the data.

Appendix 2 summarizes the information obtained about publicly-acknowledged attacks on blockchain instances. Some sources that did not add significant information beyond those shown have been omitted. Table 2 summarizes the types of attacks publicly disclosed. Most of the incidents reported (eleven incidents) were attacks using centralization of computing power. Attacks on wallets included four incidents of corporate phishing, three incidents of loss or theft of private key, one incident of usurped public key, and three incidents of transaction malleability. Attacks on web exchanges included four incidents of loss

or theft of private key, one incident of usurped public key, and three incidents on distributed denial of service. There were two incidents reported on smart contracts with flawed or malicious code. Four reports did not provide detailed information about the nature of the attacks experienced.

| Component | Risk | Incident number | Total number of incidents |
|---|---|---|---|
| Nodes | Centralization of computing power | 2, 3, 9, 10, 26, 27, 28,29, 31, 33, 35 | 11 |
| Wallets | Corporate phishing | 14, 16, 24, 32 | 4 |
| | Loss or theft of private key | 12, 15, 25 | 3 |
| | Usurped public key | 13 | 1 |
| | Transaction malleability | 1, 11, 17 | 3 |
| Web exchanges | Loss or theft of private key | 19, 22, 23, 36 | 4 |
| | Usurped public keys | 18 | 1 |
| | Distributed denial of service | 4, 5, 7 | 3 |
| Smart contract | Flawed or malicious code | 8, 30 | 2 |
| Not disclosed | | 6, 20, 21, 34 | 4 |

Table 2. Types of Blockchain Attacks

From the academic literature, other types of attacks emerged. Li et al. (2017) identify the different risks related to blockchain as 51% vulnerability, private key security, double spending, transaction privacy leakage, criminal smart contracts and vulnerabilities in smart contracts. ISACA (2019) also provides guidance on the risks associated with blockchain implementations. Different from Li et al. (2017), who focus on attacks of blockchains that are already implemented, the ISACA guidelines (2019) for blockchain auditing consider the entire life cycle of a blockchain, including pre-implementation and governance. Although the ISACA guidelines are broader than those from Li et al. (2017), they both consider attacks

to the blockchain itself, rather than the blockchain ecosystem. The following sections expand on the attacks identified in the review of the practitioner and academic literature and are the building blocks of the proposed cybersecurity control framework.

## 4. RISK AND CONTROLS

### 4.1. Distributed denial of service attacks

A Denial of Service (DoS) attack attempts to make a targeted system unavailable to its end users. A Distributed Denial of Service (DDoS) attack uses many compromised computers in such an attempt (Saleh and Manaf, 2014). The compromised computers (laptops, desktops, Internet-of-Things devices) become "zombies" or "bots" that launch the attack upon the attacker's command (Rahmani et al., 2009). Consequences of a DDoS attack can be platform unreachability, loss of productivity, and reputation damage (Greevink, 2018).

Amazon Web Services (AWS, 2019) suggests four DDoS prevention controls: 1) Reduce attack surface area. This control limits the options for attackers by protecting information about ports, protocols and applications. 2) Define traffic baseline. This control refers to gathering information about normal and abnormal traffic. The pattern of normal traffic becomes the baseline and each incoming data packet is compared against it for classification. 3) Plan to scale. This control refers to the ability to scale bandwidth (transit) on demand to handle large volume of traffic and expand server capacity to increase or decrease the computation resources quickly. 4) Deploy sophisticated firewalls. This control refers to the installation of firewalls to protect against sophisticated application attacks such as SQL injection and cross-site request forgery. Prevention controls 3 (plan to scale) and 4 (firewalls) are useful not only in DDoS attacks; the ability to scale on demand can support peak operations and firewalls can filter phishing or virus attacks. Although a DDoS attack directed to a blockchain is unlikely, this attack can affect other components of the blockchain ecosystem, particularly oracles and exchanges.

Based on the risk of a distributed denial of service attacks, we propose cybersecurity control 1: *components of the blockchain should reduce the surface area of potential attacks and establish baselines on normal traffic.*

### 4.2. Ransomware attacks

Ransomware is software that takes control of the computer systems of its victims and demands that they pay ransoms to get control back. Ransomware usually infects computer systems through malware in email attachments or downloads from websites. There are two types of ransomware: 1) Locker-ransomware prevents its victims from accessing their computers, and 2) Crypto-ransomware encrypts the files of its victims, making the data unreadable (Sgandurra et al., 2016).

Blockchains have been associated with ransomware attacks primarily as payment methods. In July 2014, for instance, the ransomware CTB-Locker, which infected systems through an email attachment, requested ransom in Bitcoins (Security Alliance, 2017). More recently, in May 2017, the WannaCry crypto-ransomware, which infected around 230,000 computers by exploiting a vulnerability in Windows, requested ransom in Bitcoins (CERT-EU, 2017). Bitcoin may be the preferred method of payment of ransom (Popper, 2015) because accounts are anonymous (making it impossible to trace accounts back to owners who received the ransom) and transactions are irreversible (making it impossible for victims to reclaim the money paid for the ransom). An equivalent of $2,220,909 in Bitcoins have been used as payment method in ransomware attacks (Conti et al., 2018). Given the uncertainty and the risks of ransomware, some companies have been stockpiling Bitcoins to use for payments if they ever become victims of ransomware (Kshetri and Voas, 2017).

A ransomware attack would be unlikely to incapacitate the typical public blockchain because the information in any captured nodes could easily be restored from uncaptured nodes. Because the typical public blockchain's network contains many nodes, it is more resilient to a ransomware attack than the typical private blockchain's network, which includes fewer. On the other hand, the other components of a blockchain ecosystem (oracles, arbitrators, wallets) can be targets of ransomware attacks and should implement general controls against them.

Controls to protect against ransomware attacks range from preventing the attack from occurring to recovering data from backups without paying the ransom. A great many controls have been cited in the literature, including: performing regular backups, applying security patches and updates, deploying security

products, blocking popups, enforcing access control, performing and testing file recovery, disabling macros, avoiding suspicious emails and attachments, avoiding suspicious and unreliable URLs, implementing security awareness programs, and disabling unused wireless connections (Bridges, 2008; Kolodenker et al., 2017; Kumar and Kumar, 2013; Luo and Liao, 2007, 2009; Mohurle and Patil, 2017; Mustaca, 2014; Pathak and Nanded, 2016; Palisse et al., 2017; Prakash et al., 2017). These general controls assist not only with protecting from ransomware attacks but also from other types of attacks.

Based on the risk of ransomware attacks, we propose cybersecurity control 2: *components of the blockchain ecosystem should implement general controls to prevent and recover from ransomware attacks.*

There is a variation on ransomware attack that involves demand for ransom by an attacker who has gained control over the majority of the computing power of a blockchain. This form of attack does not involve malware, but applies to blockchains in which the right to append a block to the chain is gained through computing power. We discuss this type of attacks in the section of centralization of computing power.

### 4.3. Attacks using centralization of computing power

Centralization of computing power is a risk for blockchains when nodes monopolize the right to append blocks to the chain due to their computing power. When the majority of the computing power in a blockchain's network is centralized, whoever controls that power can with impunity discard a valid chain or substitute an invalid chain for a valid one. Attacks based on centralization of computing power (also known as majority attacks or 51% attacks) threaten blockchain immutability, which depends on a large number of nodes being able to independently validate transactions and blocks.

An attack based on centralization of computing power takes advantage of implicit consensus, a mechanism for resolving temporary inconsistencies that can occur in a blockchain. Because of delays in the propagation of information in blockchains, it is possible for two nodes (A and B) to attempt simultaneously to add a block (N+1) to the last block (N) in a chain. These two new blocks (N+1A and N+1B), usually will not contain exactly the same transactions, although both will be valid. This amounts to a temporary inconsistency in the blockchain. The blockchain

now forks after block N and new blocks can be added to either side of the fork, the one following N+1A or the one following N+1B.

To eliminate the inconsistency, implicit consensus specifies that the longer path will be deemed valid and the shorter path will be disregarded. Any node that can add a new block is free to decide which side of the fork to use; over time, one path will have more blocks added than the other. Eventually, nodes will stop adding blocks to the shorter path. Implicit consensus preserves the reliability of the information as long as nodes act independently and have about the same probability of adding new blocks to the chain. There is no need for formal approval or voting among nodes; when nodes append blocks to a path, the nodes are implicitly acknowledging its validity.

The implicit consensus mechanism can become a means for attack on the blockchain when a node has a sufficiently high probability of adding a new block. A node with enough computing power can decide unilaterally which side of a fork will prevail. Moreover, it can create forks retrospectively or prospectively to manipulate the blockchain.

To modify a chain retrospectively, a node may try to substitute a transaction that has already been validated (for instance, substituting transaction X with transaction X^') and has already been added to a block (for instance, to the block three blocks before the current last one [call this earlier block N-3]) by creating a fork just before N-3 (from block N-4). The fork will follow block N-4 with block N-3^', as well as block N-3. The attempt to replace transaction X with X^' will only succeed if the branch of the chain that includes block N-3^' becomes the longest one. Until this is true, other nodes will disregard block N-3^'. However, if the malicious node has computing power sufficient to append enough blocks to the branch of the chain that includes N-3^', it will eventually become longer than the one that includes block N-3. At that time, the implicit consensus mechanism will make the branch of the chain that includes block N-3^' the valid one, leaving the original branch to be disregarded and the original transaction, X, to be forgotten. Figure 3 depicts this situation.

The specific mechanism used to determine which node can append a block to the chain depends on the implementation of the blockchain. Public blockchains dealing with cryptocurrencies such as Bitcoin incentivize nodes to participate by rewarding nodes with cryptocurrency if they add a new block. In this approach,

the right to add a block is earned by solving a computational puzzle (called 'proof of work'). This places nodes in competition to solve the puzzle first. Nodes with more computing power do better at solving puzzles and, therefore, get to add more blocks and earn more cryptocurrency. Rewarding nodes for adding blocks is an incentive to recruit nodes, who might not otherwise dedicate their computing power to the blockchain. However, this mechanism also allows sufficiently powerful nodes to make arbitrary changes to the blockchain.

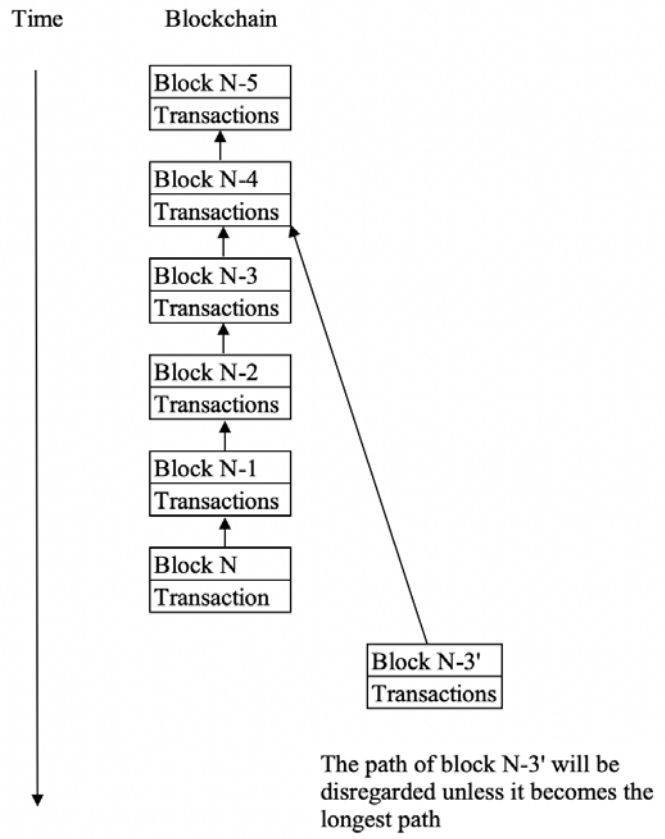


Figure 3. A retrospective fork in a blockchain to change a transaction in block N-3

Blockchains that rely exclusively on a node's computing power to earn the right to append blocks lack controls to ensure that nodes do not collude or to prevent the centralization of computing power. The only control possible is to monitor the computer power that nodes display (Piscini et al., 2017) and expect any overly powerful node to reduce its computing power to a level below what is needed to

take arbitrary actions. As an example of this, in 2014, a pool of miners (Ghash.io) acquired more than 50% of the computing power in the Bitcoin network; they voluntarily reduced their power and pledged not to exceed 40% of the power of the network in future (Frankenfield, 2019).

Based on the risk of centralization of power in blockchains relying exclusively on computing power to earn the right to append a block, we propose cybersecurity control 3: *the computing power of nodes should be monitored constantly to warn when centralization is becoming a threat.*

Not all blockchains use the proof of work mechanism to decide which node has the right to append a block to the chain. In another mechanism, named proof of stake, the node who wins the competition to append a block has a stake on the validity of the block. If other nodes find that the block is invalid, the node proposing the new invalid block loses its stake, and the right to be part of the consensus network. Proof of stake segregates duties because the node appending a block is different from the nodes validating the block.

Other mechanisms eliminate competition and computing power all together, and nodes earn the right to add a block by taking turns (a round-robin approach) or by having the shortest random CPU-generated waiting time (proof of elapsed time). These mechanisms are mostly used in private blockchains because the incentive to participate in the blockchain is to increase the reliability of the information, rather than increasing their wealth.

Based on the risk of nodes manipulating the blockchain in different mechanisms, we propose cybersecurity control 4: *the mechanism used to earn the right to append a block to the chain should reduce the possibility of a node altering the blockchain.*

### 4.4. Attacks breaking cryptographic algorithms

Cryptographic algorithms are used in blockchains as a built-in mechanism to validate transactions (as in the digital signatures of the wallets) and to validate blocks (as in the unique identifiers created for each block). Given enough time, any encrypted code can be broken using a trial-and-error approach. The possibility of breaking an encrypted code would give the ability to modify transactions and blocks, threatening the core of immutability of records. According to Bennett et

al. (1997), cryptosystems with keys of 112 bits may be breakable in 30 or 40 years (using the typical computing power of computers today).

As computing power increases, the time to break an encrypted code decreases. According to Chen et al. (2016), it is likely that by 2030 a quantum computer will be capable of breaking a 2000-bit RSA key in a matter of hours. The risk of increasing computing power led the National Institute of Standards and Technology to announce in 2016 a plan to move to post-quantum cryptography (also called quantum-resistant cryptography) to develop cryptographic systems that will be secure from both quantum and classical computers. The need to evolve blockchains towards quantum cryptographic algorithms to secure cryptocurrencies has already been pointed out (Gao et al., 2018).

Stronger cryptographic algorithms obviously represent stronger controls. Although quantum cryptography is not available yet, algorithms, such as SHA-368—that are stronger than those currently used, such as SHA256 and the RIPEMD—are currently available. However, migrating to stronger cryptographic algorithms is a challenge for blockchains in which the decisions to make changes to the blockchain are fully decentralized, like in Bitcoin. Blockchains in which the decisions to improve the blockchain are centralized (private blockchains and public blockchains like Ethereum) can plan and enforce the migration to stronger cryptographic algorithms.

We discuss the migration of protocols in general in a later section because the possibility of unexpected problems arising during migration increases the vulnerability of a system during the process. In terms of migration plans related to cryptographic algorithms, the plan should evaluate the impact of the migration on all the elements using cryptography. The plan should indicate, for instance, how the private and public keys used for wallets will be updated, and how the nodes will be updated. In addition, the plan should evaluate whether the transition to stronger cryptographic algorithms will have an impact on transaction malleability or other known vulnerabilities.

Based on the increased risk during the migration of cryptographic algorithms, we propose cybersecurity control 5: *a migration plan should be developed for transitioning to stronger cryptographic algorithms.*

### 4.5. Theft of private keys

Private keys (one of the elements of digital signatures) are the basic authorization control that blockchains employ; anyone who knows the private key can conduct transactions with the wallet associated with it. As such, controls should be implemented to prevent unauthorized access to private keys. In public blockchains, the ability to conduct transactions using a single private key, without authenticating the identity of the owner of the wallet, ensures the anonymity of users. However, when private keys are lost, the tokens in the wallet associated with the private key are permanently lost, too. Owners of cybercurrency in public blockchains are aware of the irretrievability of lost private keys and are willing to accept the risks of having a single private key for transaction authorization.

There are several alternatives to using a single private key in a single device. One alternative is to store the private key in multiple devices, even in cold storage (a device not connected to the internet). This alternative protects the owner of the wallet from the failure or loss of the private key when the key is stored in a single device; it increases, however, the number of devices from which the private key can be stolen.

A second alternative is to store the private key in the cloud with a web exchange, such as Bitfinex. This alternative shifts the responsibility of establishing access controls to protect the private key from the owner of the wallet to the web provider. The web exchange can implement common access controls, such as passwords, device or location recognition, or two-factor authentication. With this alternative, the legitimacy and cybersecurity of the web provider is critical. Illegitimate web exchanges can lure customers and then disappear with their private keys, stealing the tokens of all their customers—a form of corporate phishing attack.

Web exchanges should be required to provide evidence of the controls implemented to protect the private keys of the customers, including insurance to reimburse tokens lost from stolen private keys protected by the exchange. Web exchanges should also develop a transition plan in case the web exchange goes out of business. This evidence can be provided with a Systems and Organization Control 2 type 2 report, supplemented with insurance and transition plans.

Based on risks posed by the use of web exchanges, we propose cybersecurity control 6: *web exchanges should provide evidence of controls, including insurance and transition plans.*

Rather than relying on a single private key to authorize transactions, blockchains can also implement a mechanism, called multisig, to require multiple private keys (typically two) to authorize a transaction. Multisig is a mechanism similar to those commonly used in accounting systems that require multiple employees to authorize a transaction. Checking accounts, for instance, can be set to require two signatures to authorize checks with amounts above a designated threshold. In a similar fashion, blockchain multisig issues multiple private keys for a single wallet (three private keys for instance) requiring more than one private key to authorize a transaction (two private keys for instance). Private keys are usually stored in different locations; if a private key is lost, there would still be two private keys available to authorize the transaction. This control would also prevent the use of a stolen private key to conduct a transaction because the attacker would require a second private key. Multisig requires access controls in all points where private keys are stored.

Multisig is stronger when the access controls of web exchanges can be supplemented with algorithms to identify unusual transactions, similar to algorithms used by credit card institutions to identify possible fraudulent transactions. For instance, a wallet with three private keys can assign two of the private keys to the wallet owner and the third private key to the web exchange. A transaction can be authorized with one of the private keys of the wallet owner and the private key of the web exchange. The algorithm would flag suspicious transactions that would need to be confirmed with the wallet owner before providing the necessary second private key to authorize the transaction. Because the owner has two private keys, the owner can always bypass the exchange and authorize the transactions with the two private keys.

Based on risks of using a single private key, we propose cybersecurity control 7: *the authorization of critical transactions should require multiple private keys.*

### 4.6. Usurped public keys

Public keys (one of the elements of digital signatures) are used in blockchains as unique identifiers of wallets; public keys are the destination address in a

transaction. Although public keys are known by the general public, wallets and web exchanges should implement controls to prevent unauthorized access to public keys. Attackers may change references to the victim's public key (perhaps in a web page) to the attacker's public key, diverting the tokens sent to the legitimate address to the attacker's address.

There is a malware named BitcoinStealer—a variation of the ransomware "Jigsaw"—that substitutes the public key of the wallet attacked with the attacker's public key (Palmer, 2018). The attacker's address has the same characters at the beginning and end of the legitimate address, making it difficult for the wallet owner to identify the change without closer examination (Palmer, 2018). It is expected that malware attacks to substitute public keys will become more popular because the attack is more reliable, non-intrusive, and profitable than other attacks (Chong, 2018).

Attacks to public keys have also been reported in web exchanges in which attackers gain access to the website and change the public key displayed on the site. Our review of the literature identified multiple successful attacks in which the change of the public key went unnoticed for some time, in one case, amounting to $10 million diverted (Bryk, 2018; De, 2017). Preventing these attacks requires the implementation of the usual controls to prevent ransomware and unauthorized access controls.

In addition to these controls, a duplicate of the public key could be stored separately, so a program can continuously and automatically compare the public key in the wallet or the website to the public key stored somewhere else. The program would note the change of the public key almost immediately, enabling the correction of the public key promptly to prevent losses.

Based on the possibility of illegitimate changes to public keys, we propose cybersecurity control 8: *the accuracy of public keys should be continuously and automatically tested.*

### 4.7. Transaction malleability attacks

A transaction malleability attack is the creation of a modified copy of a transaction that enables the attacker to receive tokens from a modified transaction and, at the same time, claim that no tokens were received, deceiving the sender into issuing a new transaction to transfer more tokens. This cybersecurity threat is

possible because of the way in which transactions are identified and propagated among the nodes of a blockchain. Blockchains without appropriate cybersecurity controls (up-to-date protocols for validating transactions) and wallets without proper controls, can lead senders to be unaware of modified transactions, and fall into the deception of issuing new transactions. Although transaction malleability could affect different implementations of blockchains, the vulnerabilities of Bitcoin's blockchain have been widely analysed (Andrychowicz et al., 2015). We anchor our discussion on transaction malleability on Bitcoin's blockchain.

Blockchains identify transactions by assigning a unique identifier (Tx_ID) to each transaction. The unique identifier is created based on the content of the transaction (sender, receiver, amount, and other information). If the transaction data is modified, the resulting unique identifier is different. A malicious receiver can modify some information of the transaction data, changing the syntax of the transaction—and the Tx_ID as a result—without changing the semantics; that is, the tokens are still transferred from the sender to the receiver. The sequence of a malleability attack is: 1) the sender creates a transaction to transfer tokens to a receiver (who is the attacker). The wallet computes the corresponding Tx_ID and broadcasts the transaction to other nodes in the blockchain. This transaction will be ready to be validated and inputted into a new block. 2) The attacker receives the transaction, modifies it and broadcasts the modified transaction with its new identifier Tx_ID', hoping that the modified transaction will be validated and inputted into a block before the original transaction. If the modified transaction is the one validated and inputted into a block, the tokens associated with the transaction will be transferred to the attacker and the validation of the original transaction will fail, allowing the attacker to claim that the tokens were not received. The sender will not find the transaction with the identifier Tx_ID in the blockchain and would be deceived into issuing a new transaction to transfer tokens.

It seems counterintuitive that the original transaction will fail to be validated when the sender might have tokens in the wallet. For instance, the sender owns 100 tokens and issues a transaction to transfer 20 tokens; apparently, the original and the modified transaction should be able to cash 20 tokens each, leaving 60 tokens in the wallet. This operation would be similar to creating a falsified copy of a check and cashing the check twice (the original and the falsified copy). However,

tokens in blockchains are different from money because—as mentioned in the section introducing blockchain—tokens are unique, and they are locked and unlocked with the digital signature of the owner. In a transaction malleability attack, the receiver will get the tokens from the modified transaction and lock them, making the receiver the new owner. So, when nodes try to validate the original transaction, the digital signature of the sender will fail to unlock the tokens, as now the tokens are locked by the attacker.

The locking and unlocking of tokens are coded in small scripts that may be part of the transaction data, and if so, the small script would be included to compute the unique identifier of the transaction. Wuille (2019) identified nine different ways in which transactions can be modified through a transaction malleability attack in Bitcoin. One way in which an attacker can modify a transaction is by slightly changing the script that locks and unlocks tokens with innocuous instructions, in such a way that the changes would not affect the programming logic nor the execution of the script (Rajput et al., 2018), but would modify the unique identifier of the transaction if the script is part of the transaction data used to compute the unique identifier.

Transaction malleability attacks of this type can be prevented by excluding the small script that locks and unlocks the tokens in the computation of the unique identifier, so if an attacker modifies the script, the identifier of the transaction would remain the same. In 2017, the blockchain used in Bitcoin was updated with a protocol called SegWit (Segregated Witness) that prevents a transaction malleability attack altering the small script by excluding the data from the digital signatures in the small script in the calculation of the unique identifier of the transaction. Although different forms of transaction malleability attacks have been identified, potential new ways of malleability attacks should be investigated.

Based on the risks posed by transaction malleability attacks, we propose cybersecurity control 9: *protocols to identify and prevent known malleability attacks should be deployed.*

### 4.8. Flawed or malicious smart contracts

A smart contract is a program stored in a blockchain that executes automatically when the conditions specified (and programmed) in the contract are fulfilled. They are called smart contracts because the transaction remains latent (inactive) waiting for the conditions to be fulfilled; the fulfillment of the conditions trigger

the transaction coded in the program to be inexorably completed. For instance, a contract may indicate that a given number of tokens (cryptocurrency or any other token managed by the blockchain) are to be transferred from the wallet of company A to the wallet of company B when company B delivers some specified set of goods to company A. The smart contract includes: a) the latent transaction (tokens to be transferred), and b) the condition that needs to be fulfilled to trigger the execution of the transaction (delivery of the goods). Although smart contracts were originally proposed to execute transactions, smart contracts could also be used to support audits (Rozario and Vasarhelyi, 2018)

The automatic execution of a program when a set of conditions are fulfilled is not a new concept in information systems. Accounting information systems, for instance, can be programmed to send a warning message when the funds in a checking account are low. Also, suspicious credit card transactions automatically trigger requests for credit card holders to verify the transaction. What makes smart contracts unique is that, once they are inserted in a blockchain, the contract cannot be disabled or modified (because of the immutability of the data stored in the blockchain), ensuring that the transaction will be executed as originally agreed.

The inexorability of the execution of a smart contract is not only its greatest strength, but it is simultaneously its greatest weakness; smart contracts can be incorrect or hide malicious code. As a result, a cybersecurity control should identify threats embedded—on purpose or inadvertently—in smart contracts before they are inserted in a blockchain (Dai and Vasarhelyi, 2017). A nascent industry satisfies this need by offering auditing of smart contract code where one or more auditors evaluate the code for vulnerabilities before its insertion into a blockchain. BountyOne, for instance, follows a decentralized audit model with three steps to audit smart contracts (BountyOne, 2019). In the first step, a small number of auditors work independently to review the smart contract and write an audit report. In the second step, senior auditors review and rank the audit reports. In the third step, the highest-ranking audit report is open to all the auditors affiliated with BountyOne for audit.

Smart contracts should not only be audited before being inserted to a blockchain, but the audit should be conducted by an independent entity—someone not involved in the transaction and connected with the nodes in the blockchain.

Independence is necessary to avoid potential conflicts of interest that can reduce evaluation objectivity.

Based on the risks posed by flawed or harmful smart contracts, we propose cybersecurity control 10: *smart contracts should be audited by an independent entity before being inserted into a blockchain.*

### 4.9. Compromised oracles and arbitrators

Smart contracts are usually tied to events in the real world: the delivery of physical goods, the transfer of property, the delivery of a digital key to activate the software, or any other transaction. As a result, an important component in smart contracts is the entity—one outside the blockchain—who verifies the event has happened. These external entities, known as oracles, communicate to the blockchain when an event in the world has happened, activating the trigger in the smart contract that executes the transaction.

Oracles and arbitrators are components of the blockchain ecosystem; the information they provide impacts the reliability of the information in a blockchain. Oracles are intermediaries between blockchains and events in the world (as opposed to digital events). Arbitrators are, as the name implies, referees in a disputed transaction. Oracles and arbitrators should be protected against systems threats (unauthorized access, denial of service attacks, ransomware, and others) to preserve the integrity of the information they provide. In addition, they should be independent from the rest of the components of the blockchain ecosystem to preserve their objectivity in performing their duties. Oracles and arbitrators should also implement controls to authorize and verify the information before it is sent to the blockchain.

Compromised oracles might send information about events that have not happened, as if they had happened (for instance, indicating that goods have been delivered, when in fact they have not been delivered). Conversely, an oracle might not send information about an event that has in fact happened. Compromised arbitrators might send information favoring the incorrect party in the dispute, or might refuse at all to resolve a dispute, stalling the transaction indefinitely. Oracles and arbitrators should implement segregation of duties, in which the entity (person/department/system) recording the event should be different from the entity (person/department/system) verifying the event. Only

transactions that have been independently verified should be sent to the blockchain.

Based on the risk of compromised oracles and arbitrators, we propose cybersecurity control 11: *oracles and arbitrators should implement independent verification controls to ensure the reliability of the information sent to a blockchain.*

Similar to other components of the blockchain ecosystem, oracles and arbitrators should be independent from parties of the transaction, nodes, and smart contract auditors. Segregation of duties suggests that oracles, as providers of information, should not be responsible for recording transactions, which is the responsibility of the nodes, or for auditing smart contracts, which is the responsibility of smart contract auditors. Segregation of duties will also prevent, for instance, an oracle associated with company B fraudulently indicating that company B delivered the goods to company A when, in fact, the goods have not been delivered. Moreover, the independence of oracles and arbitrators should be evaluated beyond the legal structure of the companies, as oracles, arbitrators, nodes, or transaction parties can collude without being legally associated. In addition, independence should be monitored constantly, as collusion might start at any time.

Based on segregation of duties for oracles and arbitrators, we propose cybersecurity control 12: *oracles should be independent from other components of the blockchain ecosystem (transaction parties, nodes, and smart contract auditors).*

### 4.10. Disorderly migration of protocols

Migrating protocols, as the name implies, refers to deprecating the use of one or more protocols in the blockchain and substituting them with new protocols. As any ecosystem, the blockchain ecosystem needs all of its components to agree on the protocols to be used. As new vulnerabilities arise or more efficient protocols are developed, the ecosystem should evolve. The way in which protocols are migrated depends on the blockchain implementation.

The blockchain used in Bitcoin, for instance, has a mechanism known as Bitcoin improvement proposal. In this mechanism, an upgrade is proposed, but it will be deployed only if the majority of the nodes' computing power accepts it. This mechanism favors complete decentralization, but risks the rejection of protocols

needed to improve the performance or attenuate the vulnerability of the blockchain. For instance, the SegWit protocol to prevent transaction protocol has not been fully deployed by all nodes in the Bitcoin blockchain (Kim, 2019).

In other public blockchains, like Ethereum, there is a group of experts in charge of its evolution. Aspiring members of the Ethereum ecosystem must agree, before joining the ecosystem, that they will adopt the protocols as determined by the group of experts. Similarly, private blockchains determine the required upgrades promoting a smoother transition than fully decentralized blockchains. The degree to which upgrades are centralized to make them mandatory influences the risks of having multiple protocols coexisting or failing to adopt necessary updates.

Based on the risks of a disorderly migration of protocols, we propose cybersecurity control 13: *the migration of protocols should be enforced.*

Despite having a tighter influence on the migration of protocols, any migration can lead to unexpected consequences. As such, as other ecosystems, blockchains should implement controls for evaluating the potential consequences of the migration and plan for rollbacks in case of unexpected consequences.

Based on the risks of unexpected consequences in the migration of protocols, we propose cybersecurity control 14*: a complete migration plan should be developed to migrate protocols.*

## 5. A PROPOSED FRAMEWORK FOR CYBERSECURITY CONTROLS FOR BLOCKCHAIN ECOSYSTEMS

Internal controls are the policies and procedures developed to ensure reliability of information, efficiency of operations, and compliance with regulations. Our control framework focuses on cybersecurity controls to ensure the reliability of the information in a blockchain. This framework can inform a comprehensive internal control framework that addresses the efficiency of operations, and compliance with regulations. For instance, blockchains storing data from Europeans must comply with the General Data Protection Regulation (GDPR). A comprehensive control framework for blockchain should include compliance with GDPR, among other laws. The scope of our framework is limited to the cybersecurity controls to reasonably ensure the reliability of the information stored in a blockchain.

Our framework identifies the different components of a blockchain ecosystem and their associated risks and controls. Table 3 lists the different components of a blockchain ecosystems and the risks identified. This table also identifies whether the risk is exclusive of blockchain ecosystems or the risk is applicable to any other system. Although the risks are identified with a particular component, a cybersecurity breach on any component will impact the reliability of the information in the blockchain.

| Component | Risk | Exclusive to blockchain |
|---|---|---|
| Nodes | Centralization of computing power | Y |
| | Breakable cryptographic algorithms | N |
| | Disorderly migration of protocols | N |
| | Unexpected consequences in migration protocols | N |
| Wallets | Ransomware | N |
| | Corporate phishing through web exchanges | N |
| | Loss or theft of private key | N |
| | Usurped public key | N |
| | Transaction malleability | Y |
| Oracles and arbitrators | Distributed denial of service attack | N |
| | Ransomware | N |

| | | |
|---|---|---|
| | Compromised oracles or arbitrators | N |
| | Collusion | N |
| Web exchanges | Ransomware | N |
| | Loss or theft of private key | N |
| | Usurped public keys | N |
| Smart contract | Flawed or malicious code | Y |

Table 3. Blockchain ecosystem components and identified risks

As table 4 shows, we identified thirteen risks, most of them applicable to any other information system. Blockchain components are not exempt from ransomware attacks, distributed denial of service, or other attacks affecting other systems. Also, as is true of other systems using digital signatures, there are risks associated with public and private keys. However, we identified three risks exclusive to the blockchain ecosystem: centralization of computing power, transaction malleability attacks, and flawed or malicious code in smart contracts.

In addition to identifying risks, our framework proposes controls to mitigate risks. Although some of these controls are commonly used in other information systems, (e.g., segregation of duties), our framework customizes the controls as they apply to the different components of the blockchain ecosystem. Our framework also includes controls proposed in the literature (e.g., the use of multiple private keys to authorize transactions) and proposed new controls (e.g., testing the accuracy of public key). Table 4 summarizes the proposed control related to the risks they are meant to mitigate.

| Risk | Controls |
|---|---|
| Distributed denial of | Reduce the surface area of potential attacks and establish baselines |

| | |
|---|---|
| service attack | on normal traffic. |
| Ransomware | Implement general controls to prevent and recover from ransomware attacks. |
| Centralization of computing power | Monitor the centralization of computing power.<br><br>Implement protocols to earn the right to append a block that reduce the possibility of a node altering the blockchain. |
| Breakable cryptographic algorithms | Developed a plan for transitioning to stronger cryptographic algorithms. |
| Corporate phishing through web exchanges | Provide evidence of controls, including insurance and transition plans. |
| Loss or theft of private key | Require multiple private keys to authorize critical transactions. |
| Usurped private key | Test the accuracy of public keys continuously and automatically. |
| Transaction malleability | Deploy protocols that identify and prevent known malleability attacks. |
| Flawed or malicious code | Conduct an independent audit of the smart contract code. |
| Compromised oracles or arbitrators | Implement independent verification for information sent to a blockchain. |
| Collusion of oracles or arbitrators | Monitor the independence of oracles and arbitrators from other components of the blockchain ecosystem. |
| Disorderly migration of | Enforce migration of protocols |

| | |
|---|---|
| protocols | |
| Unexpected consequences of protocol migration | Develop a complete migration plan |

Table 4. Proposed cybersecurity controls to mitigate risks

Our framework does not distinguish controls for public and private blockchains. The implementation of controls should consider that the relative smaller number of nodes of private blockchains compared to public blockchains make the former more vulnerable to some risks; however, private blockchains have more flexibility to implement more stringent controls. For instance, enforcing the migration of protocols is only possible for private blockchains and for public blockchains with centralized decision making (such as Ethereum).

## 6. DISCUSSION

We developed a framework for cybersecurity controls for blockchain ecosystems drawing from the practitioner and academic literature. We identified thirteen risks, ten common to other information systems, and three exclusive to blockchain ecosystems (centralization of computing power, transaction malleability attacks, and flawed or malicious code in smart contracts). The proposed framework focuses on cybersecurity controls to protect the reliability of the information stored in the blockchain. However, as any other information system, blockchains face risks other than cyberattacks that should be addressed by a comprehensive internal control system. The cybersecurity framework proposed in this paper can inform such a comprehensive framework.

As is true of any control system, the implementation of controls for blockchains should evaluate the trade-off between security and performance. Controls are costly and slow down the speed at which transactions can be processed. For instance, requiring multiple private keys to authorize a transaction might delay transactions that should be recorded immediately. However, the wait might be justified considering the amount of the transaction.

Because control frameworks are essentially broad, organizations can use them as guides to create specific control structures tailored to their situations. We envision others using the framework we have developed as a model for policies and

practices (operational and audit) to ensure sound cybersecurity activities across a variety of settings. In developing specific policies and practices, organizations may engage in design research projects (Hevner et al., 2004) that would take our framework as one input. One view on design research (Walls et al., 1992) recommends that designers begin with one or more kernel theories to provide basic knowledge concerning the phenomena of interest. According to Gregor and Jones (2004), such theories can be frameworks. They maintain "the term theory encompasses what might be termed elsewhere conjectures, models, frameworks, or bodies of knowledge" (2004, p. 314). The knowledge that serves as theories in support of design research can sprout from many varied sources and may even be embodied in existing artifacts (Gregor and Jones, 2004). We maintain that the framework presented here can serve as a kernel theory to guide future design research under a wide range of conditions.

The framework proposed provides guidance to develop standards for blockchain controls and audit. It could be useful to regulators as they seek to define rules under which blockchain ecosystems should operate. The framework can be also be useful to foster a research agenda for evaluating the efficiency of the controls, for instance, or for developing alternative controls to mitigate the risks identified.

A limitation of the framework is that some controls are broadly stated (i.e. conduct an independent audit of the smart contract code). To provide actionable guidance, these controls should be further developed in detail. Another limitation is the currency of the framework. The framework identified risks based on the technology used in blockchain implementations today. As with any other information system, the framework must be updated as blockchains evolve. Similarly, this framework, as any other internal control framework, can be thwarted; the most stringent controls can be circumvented with collusion.

Although this framework focused on control principles rather than the technology behind blockchains, the close intertwining of technology and controls in blockchains highlights the need for accountants to understand, at least at the conceptual level, the technology that enables blockchains to ensure the immutability of records. This framework could be used to guide updates to the accounting curriculum to ensure accountants have the necessary knowledge to audit cybersecurity controls in blockchains.

## 7. CONCLUSION

In this paper, we conducted an exhaustive review of practitioner and academic literatures concerning the demonstrated and potential weaknesses of the blockchain ecosystem. We reviewed published reports concerning actual attacks on blockchain-based systems, potential weaknesses in blockchain implementations, and suggestions for preventing/reducing such attacks/weaknesses.

Having carried out this review, we constructed a control framework organized in terms of risks and controls. The framework primarily concerns cybersecurity controls that help to reasonably ensure the reliability of the information in a blockchain. It identifies thirteen risks for systems in the blockchain ecosystem, three of which apply to blockchain implementations only. The blockchain-only risks include: centralization of computing power, transaction malleability, and flawed or malicious smart contracts. The framework associates controls with each risk. Some of these controls had been proposed in the existing literature; some we have defined. We adapted existing controls (ones suitable for non-blockchain systems) for use in the blockchain ecosystem.

The framework has both practical and academic value. It can aid instructors in accounting and information systems in choosing concepts for their curricula. It can aid cybersecurity auditors in maintaining a comprehensive view of what can go wrong with blockchain ecosystems. It can serve researchers in accounting and information systems as one input, a form of kernel theory, for design research projects aimed at creating improved cybersecurity control artifacts.

## 8. REFERENCES

ANDRYCHOWICZ, M.; DZIEMBOWSKI, S.; MALINOWSKI, D.; MAZUREK, Ł. (2015): "On the Malleability of Bitcoin Transactions", In Brenner, M., Christin, N., Johnson, B., Rohloff, K. (Eds.). Financial Cryptography and Data Security. Springer, Berlin, Heidelberg. Vol. 8976: 1-18. https://doi.org/10.1007/978-3-662-48051-9_1

ANTONOPOULOS, A. (2017): "Mastering Bitcoin: Programming the Open Blockchain", 2nd ed. O'Reilly Media.

AWS. (2019): "What is a DDoS Attack?". https://aws.amazon.com/shield/ddos-attack-protection/

BENNETT, C.; BERSTEIN, E.; BRASSAD, G.; VAZIRANI, U. (1997): "Strengths and Weaknesses of Quantum Computing", SIAM Journal of Computing, Vol. 26, No. 5: 1510-1523. https://doi.org/10.1137/s0097539796300933

BOUNTYONE, (2019): "Decentralized Smart Contract Audits". https://bountyone.io/auditsLanding

BRIDGES, L. (2008): "The Changing Face of Malware", Network Security, No. 1: 17–20. https://doi.org/10.1016/s1353-4858(08)70010-2

BRYK, A. (2018): "Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology". https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors

CERT-EU. (2017): "Wannacry Ransomware Campaign Exploiting SMB Vulnerability". https://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-012.pdf.

CHEN, L.; JORDAN, S.; LIU. Y., PERALTA; R., PERLNER, R.; and SMITH-TONE, D. (2016): "Report on Post-Quantum Cryptography". https://doi.org/10.6028/nist.ir.8105

CHONG, N. (2018): "The Jigsaw Ransomware Has Been Revived to Steal Bitcoin from Unsuspecting Users". https://www.newsbtc.com/2018/07/20/the-jigsaw-ransomware-has-been-revived-to-steal-bitcoin-from-unsuspecting-users/

CONTI, M.; GANGWAK, G.; RUJ, S. (2018): "On the Economic Significance of Ransomware Campaigns: A Bitcoin Transaction Perspective." Computers & Security, Vol. 79: 162-189. https://doi.org/10.1016/j.cose.2018.08.008

DAI, J.; VASARHELYI, M. A. (2017): "Toward Blockchain-based Accounting and Assurance", Journal of Information Systems, Vol. 31, No. 3: 5-21. https://doi.org/10.2308/isys-51804

DE, N. (2017): "Hacks, Scams and Attacks: Blockchain's 2017 Disasters". https://www.coindesk.com/hacks-scams-attacks-blockchains-biggest-2017-disasters

FRANKENFIELD, J. (2019): "51% Attack". https://www.investopedia.com/terms/1/51-attack.asp

GAO Y.; CHEN, X.; CHEN, Y.; SUN, Y.; NIU, X.; YANG, Y. (2018): "A Secure Cryptocurrency Scheme Based on Post-quantum Blockchain." IEEE Access, Vol. 6: 27205–27213. https://doi.org/10.1109/access.2018.2827203

GREEVINK, B. (2018): "What Is a DDoS Attack and What Are the Consequences?". https://www.trimm.nl/en/blogs/wat-is-een-ddos-aanval-en-wat-zijn-de-risicos

GREGOR, S.; HEVNER, A. (2013): "Positioning and Presenting Design Science Research for Maximum Impact," MIS Quarterly, Vol. 37, No. 3: 337-355. https://doi.org/10.25300/misq/2013/37.2.01

GREGOR, S.; JONES, D (2004): "The Formulation of Design Theories for Information Systems," in Linger, H. et al. (Eds.) Constructing the Infrastructure for the Knowledge Economy: Methods and Tools, Theory and Practice, New York: Kluwer Academic, 83-93. https://doi.org/10.1007/978-1-4757-4852-9_4

HEVNER, A.; MARCH, S.; JINSOO, P.; RAM, S. (2004): "Design Science in Information Systems Research", MIS Quarterly, Vol. 28, No. 1: 75-105. https:/doi.org/10.2307/25148625

ISACA (2019): "Blockchain Preparation Audit Program", ISACA, https://next.isaca.org/bookstore/audit-control-and-security-essentials/wapbap

KHATRI, Y. (2019): "Singapore-Based Crypto Exchange DragonEx Has Been Hacked". https://www.coindesk.com/louis-vuitton-owner-lvmh-is-launching-a-blockchain-to-track-luxury-goods

KIM, C. (2019): "One Year Later, What's Holding Back SegWit Adoption on Bitcoin?". https://www.coindesk.com/one-year-later-whats-holding-back-segwit-adoption-on-bitcoin

KOLODENKER, E.; KOCH, W.; STRINGHINI, G.; EGELE, M. (2017): "PayBreak: Defense Against Cryptographic Ransomware", In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, Abu Dhabi, United Arab Emirates, April 06-06, 599-611. https://doi.org/10.1145/3052973.3053035

KSHETRI, N.; VOAS. J. (2017): "Do Crypto-Currencies Fuel Ransomware?", IT Security, Vol. 19, No. 5: 11-15. https://doi.org/10.1109/mitp.2017.3680961

KUCHLER, H. (2016): "Cyber attacks Raise Questions about Blockchain Security". https://www.ft.com/content/05b5efa4-7382-11e6-bf48-b372cdb1043a

KUMAR, S.; KUMAR M. (2013): "Cryptoviral Extortion: A Virus Based Approach." International Journal of Computer Trends and Technology, Vol. 4, No. 5: 1149-1153. http://www.ijcttjournal.org/Volume4/issue-5/IJCTT-V4I5P38.pdf

LI, X.; JIANG, P.; CHEN, T.; LUO, X.; WEN, Q. (2017): "A Survey on the Security of Blockchain Systems", Future Generation Computer Systems (forthcoming). https://doi.org/10.1016/j.future.2017.08.020

LIELACHER, A. (2018): "More 51% blockchain attacks expected". https://bravenewcoin.com/insights/more-51-blockchain-attacks-expected

LUO, X.; LIAO, Q. (2007): "Awareness Education as the Key to Ransomware Prevention", Information Systems & Security, Vol. 16, No. 4: 195–202. https://doi.org/10.1080/10658980701576412

LUO, X.; LIAO, Q. (2009): "Ransomware: A New Cyber Hijacking Threat to Enterprises." In Jatinder N. D. Gupta and Sushil Sharma (Eds.). Handbook of Research on Information Security and Assurance,1-6. https://doi.org/10 .4018/9781599048550.ch001

MOHURLE, S.; PATIL, M. (2017): "A Brief Study of Wannacry Threat: Ransomware Attack 2017", International Journal of Advanced Research in Computer Science, Vol. 8, No. 5: 1938-1940. https://doi.org/10.26483/ ijarcs.v8i5.4021

MUSTACA, S. (2014): "Are Your IT Professionals Prepared for the Challenges to Come?", Computer Fraud & Security, Vol. 3: 18–20. https://doi.org/10.1016/s1361-3723(14)70472-5

ORCUTT, M. (2019): "Once Hailed as Unhackable, Blockchains Are Now Getting Hacked". https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

PALISSE, A.; LE BOUDER, H.; LANET, JL.; LE GUERNIC, C.; LEGAY, A. (2017): "Ransomware and the Legacy Crypto API", In Cuppens F., Cuppens N., Lanet JL., Legay A. (Eds.). Risks and Security of Internet and Systems, Vol. 10158. 11-28. https://doi.org/10.1007/978-3-319-54876-0_2

PALMER, D. (2018): "This Old Ransomware Has Been Revamped as Bitcoin-Stealing Malware". https://www.zdnet.com/article/this-old-ransomware-has-been-revamped-as-bitcoin-stealing-malware/

PATHAK, P.; NANDED, Y. (2016): "A Dangerous Trend of Cybercrime: Ransomware Growing Challenge", International Journal of Advanced Research in Computer Engineering & Technology, Vol. 5, No. 2: 371-373. http://ijarcet.org/wp-content/uploads/IJARCET-VOL-5-ISSUE-2-371-373.pdf

PERKINS, C. (2019): "Blockchain Attacks and the Fight for Immutability". https://www.jdsupra.com/legalnews/blockchain-attacks-and-the-fight-for-87600/

PISCINI, E.; DALTON, D.; KEHOE, L. (2017): "Blockchain & Cyber Security", Deloitte.https://www2.deloitte.com/tr/en/pages/technology-media-and-telecommunications/articles/blockchain-and-cyber.html

POPPER, N. (2015): "For Ransom, Bitcoin Replaces the Bag of Bills", The New York Times. https://www.nytimes.com/2015/07/26/business/dealbook/for-ransom-bitcoin-replaces-the-bag-of-bills.html

POWELL, B. (2018): "Not Only is a 51% Attack on Blockchain Possible, but It's Coming: Is Bitcoin's Blockchain as Secure as You Think?". https://blocklr.com/news/51-attack-blockchain-more-likely-than-you-think/

PRAKASH, K.; NAFIS, T.; SANKAR, S. (2017): "Preventive Measures and Incident Response for Locky Ransomware", International Journal of Advanced Research in Computer Science, Vol. 8, No. 5: 392-395. https://doi.org/10.26483/ijarcs.v8i5.3311

PRIYA, P. (2019): "Cryptopia Assures Users of Its Commitment to Reopening Exchange; Provides Update on Lost Funds". https://ambcrypto.com/cryptopia-assures-users-of-its-commitment-to-reopening-exchange-provides-update-on-lost-funds/

RAHMANI, H.; SAHLI, N.; KAMMOUN, F. (2009): "Joint Entropy Analysis Model for DDoS Attack Detection in Information Assurance and Security", Fifth International Conference on Information Assurance and Security, Vol 2: 267-271. https://doi.org/10.1109/ias.2009.298

RAJPUT, U.; ABBAS, F.; OH, H. (2018): "A Solution towards Eliminating Transaction Malleability in Bitcoin", Journal of Information Processing Systems, Vol. 14, No. 4: 837-850. https://doi.org/10.3745/JIPS.03.0101

RAPOPORT, M. (2018): "PwC Has an Answer for the Blockchain: Audit It", Wall Street Journal, March 16, 2019. https://www.wsj.com/articles/pwc-has-an-answer-for-the-blockchain-audit-it-1521194401

RISBERG, J. (2018): "Yes, the Blockchain Can Be Hacked". https://coincentral.com/blockchain-hacks/

ROZARIO, A.; VASARHELYI, M. (2018): "Auditing with Smart Contracts", The International Journal of Digital Accounting Research, Vol. 18, No. 1: 1-27. https://doi.org/10.4192/1577-8517-v18_1

SALEH, M.; MANAF, A. (2014): "Optimal Specifications for a Protective Framework Against HTTP-based DoS and DDoS Attacks," in International Symposium on Biometrics and Security Technologies, Kuala Lumpur, Malaysia, August 26-27. https://doi.org/10.1109/isbast.2014.7013132

SECURITY ALLIANCE (2017): "Know Your Ransomware: CTB-Locker". https://www.secalliance.com/blog/ransomware-ctb-locker/

SGANDURRA, D.; MUÑOZ-GONZÁLEZ.; MOHSEN, R.; LUPU, E. C. (2016): "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection". https://arxiv.org/abs/1609.03020

STROM, D. (2018): "Blockchain Exploits and Mining Attacks on the Rise as Cryptocurrency Prices Skyrocket". https://securityintelligence.com/blockchain-exploits-and-mining-attacks-on-the-rise-as-cryptocurrency-prices-skyrocket/

WALLS, J. G.; WIDMEYER, G. W.; El SAWY, O. A. (1992): "Building and Information Systems Design Theory for Vigilant EIS", Information Systems Research, Vol. 3, No. 1: 36-59. https://doi.org/10.1287/isre.3.1.36

WUILLE, P. (2019): "Dealing with Malleability". http://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki

ZAGHLOUL, E. (2018): "Beginners Guide on Blockchain Security Attacks Part 1—Network". https://medium.com/zkcapital/beginners-guide-on-blockchain-security-attacks-part-1-network-ca4e74435723

## Appendix 1: Cybersecurity descriptions

| Concept | Description |
|---|---|
| Distributed denial of service attack | Attack launched from multiple sources to make computers' resources unavailable to users. |
| Man-in-the-middle attack | Attack where the attacker intercepts the traffic between two parties, and possibly altering the communication between them. |
| Ransomware | Malware (malicious software) designed to force users to pay a ransom in exchange of regaining access to their files and systems. |
| Hash function | Function that receive a message as an input and generates a unique output value derived from the content of the message. Hash functions should: 1. Make computationally infeasible to find an input based on the output, and 2. Make computationally infeasible to find any two different inputs with the same output (collision resistant). |
| SHA | A Secure Hash Algorithm (SHA) is a government standard hash function developed by the National Institute of Standards and Technology (NIST) used to provide integrity. |
| Threat | Circumstance that can result in an undesirable outcome. |
| Malware | Malicious Software. |
| Cryptographic algorithm | A computational procedure that takes inputs plus a cryptographic key, to produce an output. |
| Digital signature | The encrypted hash of a message, encrypted with the sender's private key. |
| Hash value | The result of applying a hash function to information. |

| | |
|---|---|
| Private key | A key associated with an entity that should not be disclosed. |
| Public key | A key associated with an entity that may be disclosed publicly. |
| ECDSA | Encryption algorithm approved by the National Institute of Standards and Technology. |

## Appendix 2: Known blockchain security events

| Incident | Date | Blockchain | Description | Source |
|---|---|---|---|---|
| 1 | 2014 | MtGox | Transaction malleability<br><br>Went bankrupt | Bryk, 2018 |
| 2 | 2014 | Bitcoin | Centralization of computing power<br><br>> 51% of total hash power attained by Ghash.io, one mining pool; not an attack -- Ghash.io voluntarily reduced their computing power to 40% or less | Frankenfield, 2019 |
| 3 | 2014 | Eligius mining pool | Centralization of computing power<br><br>Selfish mining attack on pool; loss of 300 BTC | Bryk, 2018 |
| 4 | 2015 | Bitcoin | Distributed denial of service<br><br>Attack by Coinwallet.eu to prove point of ease of attack | Risberg, 2018 |
| 5 | 2015 | Bitcoin | Distributed denial of service<br><br>Flood attack of 80,000 small transactions, followed by millions of small transactions over the next year -- intended to make a point in debate concerning transaction size | Risberg, 2018 |
| 6 | 2016 | Bitfinex | Not disclosed<br><br>Cyber-attack -- loss of $65 million (Source reports attack, not its details) | Kuchler, 2016 |
| 7 | 2016 | Ethereum DAO | Distributed denial of service<br><br>Loss of $50 million | Kuchler, 2016; Strom, 2018 |
| 8 | 2016 | Ethereum | Flawed or malicious code<br><br>Attack via contract code -- loss of $80 billion | Bryk, 2018 |

| Incident | Date | Blockchain | Description | Source |
|---|---|---|---|---|
| 9 | 2016 | Krypton | Centralization of computing power<br><br>51% attack -- attack by '51 Crew', ransom demand, which Krypton refused to pay; Krypton now out of business | Frankenfield, 2019; Risberg, 2018 |
| 10 | 2016 | Shift | Centralization of computing power<br><br>51% attack -- attack by '51 Crew', ransom demand, which Shift refused to pay; continues to operate | Frankenfield, 2019; Risberg, 2018 |
| 11 | 2017 | Ethereum DAO | Transaction malleability<br><br>Attacker exploited code to repeatedly refund ethers without updating balance -- loss of $50 million | Risberg, 2018 |
| 12 | 2017 | Parity | Loss or theft of private key<br><br>Bug in multi-signature wallets led to compromise of fundraisers for at least three ICO's -- loss of 150,000 ethers, worth around $105 million | De, 2017 |
| 13 | 2017 | Enigma | Usurped private key<br><br>After password attack on website, Ethereum address replaced on startup's platform, redirecting $500,000 (eventually returned) | Strom, 2018 |
| 14 | 2017 | Enigma | Corporate phishing<br><br>Fake token presale, defrauded investors of at least 1,500 ethers: compromised website, mailing lists, administrator accounts -- funds not recovered, although control of business regained | De, 2017 |
| 15 | 2017 | Tether | Loss or theft of private key<br><br>Tokens taken from company's virtual treasury and sent to unknown Bitcoin | De, 2017 |

| Incident | Date | Blockchain | Description | Source |
|---|---|---|---|---|
| | | | address -- more than $30 million lost | |
| 16 | 2017 | Bitcoin Gold | Corporate phishing<br><br>Bogus service for cashing out tokens following blockchain split, seemed to be endorsed by Bitcoin Gold -- theft of more than $3 million in various cryptocurrencies from wallets | De, 2017 |
| 17 | 2017 | Parity | Transaction malleability<br><br>User found a bug that froze wallets containing more than $275 million in ether | De, 2017 |
| 18 | 2017 | CoinDash | Usurped private key<br><br>Attacker replaced the intended Ethereum address for CoinDash's initial coin offering with another one, causing funds to go to unknown party -- loss of $10 million | Bryk, 2018;<br><br>De, 2017 |
| 19 | 2017 | NiceHash | Loss or theft of private key<br><br>Either a mining malware attack (per Strom) or the compromising of an employee computer, giving access to the marketplace's system (per De)-- loss of 4,700 BTC, worth between $64 million and $78 million | De, 2017; Strom, 2018 |
| 20 | Np | Bancor exchange | Not disclosed<br><br>Details not provided by source | Bryk, 2018 |
| 21 | Np | Litecoin Cash | Not disclosed<br><br>Details not provided by source | Powell, 2018 |
| 22 | Np | Blockchain.info | Loss or theft of private key<br><br>Hack of key generation to access private keys -- loss of 250 BTC | Bryk, 2018 |
| 23 | Np | Hardware | Loss or theft of private key | Bryk, 2018 |

| Incident | Date | Blockchain | Description | Source |
|---|---|---|---|---|
| | | wallets | Researchers able to get private keys, PIN's, recovery seeds, passphrases | |
| 24 | Np | Bitcoin | Corporate phishing<br><br>Chainalysis (a security analysis firm) created 250 fake bitcoin nodes to collect information about transactions; Bitcoin accused them of a Sybil attack; Chainalysis claimed that they had only done so for research purposes | Zaghloul, 2018 |
| 25 | 2018 | Coincheck | Loss or theft of private key<br><br>NEM blockchain coins stolen from wallets | Bryk, 2018 |
| 26 | 2018 | Monacoin | Centralization of computing power<br><br>51% attack (additional details not provided by source) | Lielacher, 2018; Ortcutt, 2019; Powell, 2018 |
| 27 | 2018 | Verge | Centralization of computing power<br><br>Suffered three 51% attacks during year:<br><br>In the first, a miner used spoofed timestamps to mine blocks at a very fast rate (one block per second), taking a reported 250,000 XVG.<br><br>In the second, using a similar approach, miners were able to mine at 25 blocks per minute, taking $1.7 million.<br><br>A third attack occurred, but losses were not reported. | Lielacher, 2018; Ortcutt, 2019; Powell, 2018 |
| 28 | 2018 | ZenCash | Centralization of computing power<br><br>51% attack -- loss of $700,000 through double spending | Lielacher, 2018; Powell, 2018 |

| Incident | Date | Blockchain | Description | Source |
|---|---|---|---|---|
| 29 | 2018 | Electroneum | Centralization of computing power<br><br>51% attack (additional details not provided by source) | Lielacher, 2018 |
| 30 | 2018 | Gambling site | Flawed or malicious code<br><br>Exploit of contract flaw -- loss of $4 million | Orcutt, 2019 |
| 31 | 2018 | Vertcoin | Centralization of computing power<br><br>51% attack -- $100,000 in double spending | Perkins Cole, 2019 |
| 32 | 2018 | IOTA wallets | Corporate phishing<br><br>Loss of around $4 million | Bryk, 2018 |
| 33 | 2018 | Bitcoin Gold | Centralization of computing power<br><br>51% attack -- loss of $18 million through double spending | Frankenfield, 2019; Perkins Cole, 2019; Powell, 2018 |
| 34 | 2019 | Cryptopia | Not disclosed<br><br>Two security breaches (perhaps exit scam) -- Ethereum holders lost 100%, Litecoin holders lost 43%, BTC holders lost 14% | Priya, 2019 |
| 35 | 2019 | Ethereum Classic | Centralization of computing power<br><br>51% attack -- reorganized the blockchain and allegedly permitted double spending of $1.1 million | Orcutt, 2019; Perkins Cole, 2019 |
| 36 | 2019 | DragonEx | Loss or theft of private key<br><br>Exchange hacked for undisclosed amount in several cryptocurrencies -- some assets retrieved | Khatri, 2019 |

Np: Date not provided in the article