International Journal of Cybersecurity Intelligence & Cybercrime

Volume 2 | Issue 2 Article 4

9-6-2019

Blockchain Security: Situational Crime Prevention Theory and Distributed Cyber Systems

Recommended Citation

Blasco, N. J., & Fett, N. A. (2019). Blockchain security: Situational crime prevention theory and distributed cyber systems. International Journal of Cybersecurity Intelligence & Cybercrime, 2(2), 44-59.

IJCIC Center for Cybercrime Investigation & Cybersecurity

Blasco, N., & Fett, N. *International Journal of Cybersecurity Intelligence and Cybercrime, 2* (2), 44-59.

Blockchain Security: Situational Crime Prevention Theory and Distributed Cyber Systems

Nicholas J. Blasco*, Daxia, USA & U.S. Army War College, USA

Nicholas A. Fett, Daxia, USA

Keywords; distributed systems, sidechains, blockchain, situational crime prevention theory

Abstract:

The authors laid the groundwork for analyzing the crypto-economic incentives of interconnected blockchain networks and utilize situational crime prevention theory to explain how more secure systems can be developed. Blockchain networks utilize smaller blockchains (often called sidechains) to increase throughput in larger networks. Identified are several disadvantages to using sidechains that create critical exposures to the assets locked on them. Without security being provided by the mainchain in the form of validated exits, sidechains or state-channels which have a bridge or mainchain asset representations are at significant risk of attack. The inability to have a sufficiently high cost to attack the sidechain while mainchain assets can be withdrawn, along with the disconnect between the integrity of the sidechain and the value of the stolen assets are among the top disadvantages. The current study used a vulnerability analysis and theoretical mathematics based on situational crime prevention theory to highlight the attack vectors and prevention methods for these systems. Much of the analysis can be applied to any distributed system (e.g. blockchain network), particularly any supposedly trustless off-chain component. The equations developed in the current study will hold for any two chains that are bridged and pass value back and forth and provides evidence to suggest a public sidechain is likely not a viable option for scalability due to security concerns. Criminal strategies on blockchain networks in the digital realm are similar to criminal strategies in the physical realm; therefore, the application of criminology can lead to more efficient development and ultimately more effective security protocols.

Introduction

Blockchain technology has existed for a decade, but the concepts that created blockchain have been around for much longer. Distributed computer systems have been employed to facilitate ease-of-use and increase the security of a computer network. Furthermore, the key pieces of cryptography which serve as some of the most attractive security features of blockchain networks was developed long before the technology was even conceived. As with many nascent implementations, many current and

*Corresponding author

Nicholas J. Blasco, Daxia, Suite 100, 118 N. Market St., Frederick, MD 21701. USA.
E-mail: nblasco@daxia.us

proposed structures for these systems still contain vulnerabilities that can be exploited by potential hackers. Analyzing the weaknesses of current technological advances and reviewing criminological theory can give us insight into how and when cyber-attacks on a blockchain network are likely to occur.

Criminological theory, or the study of why people commit criminal offenses, is a recent development in scientific advancement. There are many theoretical frameworks for why individuals become deviant. Some of these frameworks include biological, psychological, and social process, and there are many individual theories that fall within these frameworks. Practically any theory could be used to explain nefarious behavior; however, some theories are more appropriate or explain a phenomenon better than others.

The current study expands upon past research (Blasco & Fett, 2018) by examining a unique set of cybercriminal acts, particularly a 51% attack in this case, and uses theoretical concepts built around the digital environment of potential criminals and the structure of various blockchain network architectures. Strengthening potential targets through the framework of situational crime prevention theory helps account for correlates of crime that are known and unknown. This utilitarian perspective allows blockchain developers to understand the security of blockchain, particularly sidechain, technology and identify its weaknesses.

Situational Crime Prevention Theory

Situational crime prevention theory has been defined as:

> measures (1) directed at highly specific forms of crime (2) that involve the management, design, or manipulation of the immediate environment in a systematic and permanent away as possible (3) so as to reduce the opportunities for crime an increase its risks as perceived by a wide range of offenders (Clarke, 1983, p. 225).

Situational crime prevention theory posits that positive criminology and its study are fundamentally flawed. Despite the decades of studying crime, no research has identified 100% of the dispositions that lead people to commit deviant acts. Therefore, the situational choice theory emphasizes the choices and decisions individuals make instead of focusing on the dispositions that lead individuals to commit crime.

Cornish and Clarke (2003) introduced 25 techniques of situational prevention and divided into five separate categories. These 25 techniques were an extension/revision on the 16 techniques (and 4 categories) of situational prevention previously revised by Clarke and Homel (1997). The first category increases the perceived effort to commit a crime. Increasing the effort to commit a crime includes target hardening, controlling the access to facilities, or controlling tools used to commit crimes. The second category addresses the risks undertaken during the commission of a crime. Reducing anonymity, extending guardianship, or assisting in natural surveillance all increase the perceived risk in getting caught while committing a crime. The third category reduces the rewards associated with the successful completion of a crime. Denying the benefits a criminal would receive by committing a crime, removing the targets, or successfully disrupting markets can all reducing the rewards of a crime. The fourth category is concerned with reducing the provocations that entice criminals to lose impulse control. This fourth category was not included in the first version of the theory but was added later in future revisions of the theory. Frustration reduction, effective techniques to avoid disputes, and successful neutralization of peer pressure lead to reductions in provocations. The final category addresses the removal of excuses criminals use to justify deviant behavior. The removal of excuses forces potential criminals to examine their conscience and stimulate the potential guilt they would feel if a crime were committed.

Various measures have been used to operationalize these five categories. While it is certainly not exhaustive, Ronald Clarke provided detailed tables of these measures in various articles (Cornish & Clarke, 2003; Clarke, 2013). Examples of these measures have changed to become more sensitive to social and political views but there is no reason to suggest the older measures are any less effective. Possible measures that reflect target hardening, guardianship, or concealing targets could be using tamper-proof packages, carrying a cell phone, or using unmarked armored cars. Furthermore, reduced provocations and the removal of excuses could be operationalized as the use of expanded seating or requiring a hotel registration.

These concepts have been applied in many academic studies. Some of these studies included experiments that analyzed the effects of CCTV on the reduction on street crime (Welsh & Farrington, 2009), trends in the black-market poaching, transfer, and sales of illegal goods (Lemieux & Clarke, 2009), analyzing routine activity of internet use and the proclivity to be a victim of identity theft (Reyns, 2013), and the development of crime scripts for the victimization of children by sex offenders (Leclerc, Wortley, & Smallbone, 2011). These studies, and many others, have provided evidence to suggest situational crime prevention theory can lead to the reduction of criminal activity. However, one area of study that has lacked attention is information technology and cybercrime.

Distributed Systems, Blockchains, and Sidechains

Before the concept of blockchains entered the common computer science vernacular, a distributed computer system was identified as multiple computers connected together via distinct nodes. Each of the computers that is connected through a node communicates through an authentication process. Any data transmitted between the nodes is authenticated by an identifier provided by the sender and a second identifier provided by the receiver. Past authenticating agents of distributed computer systems kept a cache of identifiers previously used in data transactions. This cache allowed authenticators to cross-reference past transactions to expedite the authentication process (Wobber, Abadi, Birrell, & Lampson, 1993). The node's authentication agent is contacted to authenticate the transaction if the authenticators do not match a canned authenticator in the cache.

Distributed systems have been a staple of computer networks for decades, however the introduction of the blockchain in 2009 with the release of the Bitcoin Whitepaper (Nakomoto, 2008) has created an immense interest and growth in these systems. Started primarily by cryptographers seeking to have a currency with no trusted third parties, these systems are marked by open networks, distributed consensus mechanisms, and native 'coins' or 'tokens' which represent value in these systems.

Blockchain systems remove central operators by creating a ledger or state machine that is represented as the consensus of the nodes in the network. Instead of relying on one central party to update the state, there are predefined rules for identifying which party gets to update the state and the changes which can be made. Parties in the Bitcoin network (and many others) are selected randomly through a process known as 'Proof-of-Work' (PoW). In this process, parties compete to solve computational puzzles in order to be chosen as the next validator. Once the party is chosen, they submit the next 'block' or set of updates to the state and the other nodes can either choose to accept or reject this block. If it is accepted by the network, a new block is added and a new process of competing to update the state begins. Other consensus mechanisms have slightly different architectures to PoW. In "Proof-of-Stake" (PoS), parties stake the native cryptocurrency and are chosen at random who gets to update the next block. If a party does not update according to the rules of the chain, their stake is "slashed" or taken by the network. Other systems such as “Delegated Proof-of-Stake” (DPoS) use known stakers, and still other consensus mechanisms have DAG based models or even more nascent methods. Overall, the consensus mechanisms have their own use cases and differ in the tradeoff between speed, decentralization, and security.

Blockchains usually incorporate extreme levels of redundancy and distribution in order to secure the network; however, these measures have created very slow and limited networks. Individuals who often wish to scale their own activity do so by ‘locking’ mainchain coins into a contract whose ownership is governed by another chain, or ‘sidechain’, not the individual. Sidechains are additional systems which seek to operate in coordination with another, usually larger or more established, blockchain, or ‘mainchain’. Sidechains can be existing chains which seek to bridge access to larger chains or can be chains created for the single purpose of placing certain transactions on a different chain to reduce the number of mainchain transactions. The basic example is a payment channel where Bob and Alice each lock 100 coins into a contract which refers to a new chain. The new chain is run separately of the mainchain and allows Bob and Alice to transfer back and forth as many times as they want, very quickly without ever having to perform a main chain transaction. When one party wants to withdraw, they can submit a settlement transaction to the mainchain, prove the activity on the sidechain, and parties can now exit the money that locked onto the sidechain.

Sidechains were developed to solve some common challenges currently experienced in the blockchain ecosystem. Scalability is one issue most blockchain project possess. Scalability simply refers to the ability of a platform accommodate any level of use. Currently, blockchain platforms can only handle a limited number of interactions at a time. This is an increasing issue due to the continued adoption of the technology. Rather than increase the block size to accommodate increased volume, sidechains were partially developed as a means to solve the scalability problem.

Applying Situational Crime Prevention Theory to Blockchain Technology

Blockchain security and the threat of attacks are looming concerns in the space considering the amount of digital assets traded on cryptocurrency exchanges daily. Currently, the market capitalization of digital assets is nearly $274 billion (Coinmarketcap.com, July. 2019). The incredibly high market capitalization creates an enormous incentive for would-be offenders to steal even a portion of these assets and an equal incentive for owner/operators of blockchain companies to keep their assets safe.

The most recent statistics estimate that malicious cyber activity costs Americans $57-$109 billion in 2016 alone (The Council of Economic Advisors, 2018). As crypto assets continue to become more mainstream, they will likely become a larger target for cybercriminals. One distinctive feature in cryptocurrencies, as opposed to traditional fiat currencies, is that the traceability of the asset is often very difficult. Whereas normal cybercriminals need to worry about laundering illicit funds or having banks or credit cards chargeback ill-gotten gains, cryptocurrency was built to be irreversible and many untraceable. This means that cyber-attack victims have little to no recourse once the funds are stolen.

This anonymous nature also makes cryptocurrency networks the target for incumbents who view the networks as competitors. Many traditional companies use large third parties as intermediaries for securing aspects of their business. Whether it’s using banks to hold their capital, cloud servers to store their data, or centralized exchanges to find trading partners, intermediaries are a large part of current corporate strategies. Distributed networks have the promise to replace many of these intermediaries with automated smart contracts, rendering their services obsolete. The potential losses for these companies is massive and therefore the networks set to replace them could be an easy target while they are in a nascent development stage.

The world of computer science security analyzes systems from the vantage point of “if a cyberattack or hack can theoretically happen, it will”. This theoretical security model is great for developing new systems but does not preclude traditional criminology from being applied. Hacking is a crime and although the participants may come from different backgrounds than criminals in other fields, the theories still apply. Crimes are committed by people so analyzing the “who, what, where, and why” can lead to more efficient development and ultimately more effective security protocols.

Beebe and Rao (2005) laid out their revised situational crime prevention theory to explain information security in the digital age; the current paper expands on their ideas to accommodate the security issues found in the blockchain era. Beebe and Rao (2005) reviewed the past literature on Straub’s extension on deterrence theory (1987, 1990), the control theories proposed by Dhillon and colleagues (1999, 2001, 2004), and the various hacker taxonomies developed in the 1980s and 1990s (see Smith and Rupp, 2002). Using these digital centric theories coupled with the concepts of Clarke and Homel (1997), Beebe and Rao (2005) modified Clarke and Homel’s opportunity-reducing techniques so the concepts developed for the physical realm can be applied to the digital space. The current paper expands on Cornish and Clarke (2003) and Beebe and Rao’s (2005) concepts by developing analogous measures that go beyond the generality of the digital realm and apply it specifically to blockchain technology. Additionally, the current paper adds nine supplementary digital measures to account for the nine techniques added by Cornish and Clarke (2003) since the Beebe and Rao (2005) paper. Some of these measures include encryption, public key identification, mainchain validation, usable chain with responsive community, and acceptable use policies. Just like Beebe and Rao (2005) paper, it is important to point out that the lists of analogous measures (digital and blockchain) are not exhaustive.

Beebe and Rao (2005) address some of the base technology used in the blockchain ecosystem such as encryption. Encryption is an important characteristic in blockchain technology and its value as a target hardening and a benefit denying mechanism is identified. However, other concepts that provide security such as proof-of-work (POW) and proof-of-stake (POS) are notably absent in Beebe and Rao’s (2005) paper.

Just like the Beebe and Rao (2005) paper, the current paper accepts that blockchain security is a function of the perceived net benefits of the potential criminal along with the perceived net benefits of confederates. However, the perceived net benefits are also a function of the risks, effort, and costs to carry out a criminal offense. One of the most commonly discussed criminal acts in the blockchain ecosystem is known as a 51% attack. A 51% attack refers to a group of miners who control over 50% percent of a blockchain’s hashrate and therefore have the ability to prevent new transactions from taking place. Additionally, this majority control affords the ability to reverse transactions thus permitting the double spending of coins.

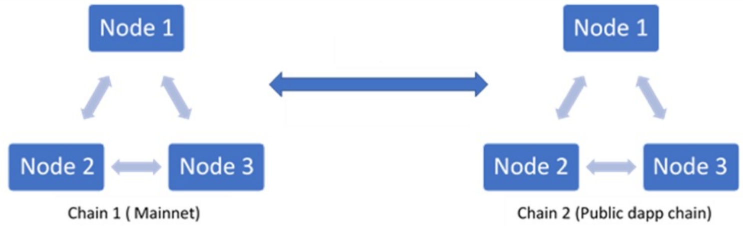

Figure 1. Example of Connected Blockchain Networks

There are several assumptions that must be made in order to fully understand the attack vectors present in connected blockchain based systems. The first assumption requires there to be two blockchains. The first blockchain is the parent chain or the mainchain, and the second blockchain is the child chain or the sidechain. Figure 1 shows an example setup of these two separate blockchain systems. The second assumption requires individuals to be rational beings and thus affected by the aspects of Cornish and Clarke's (2003) theory. Motivation to maximize profits is a natural assumption in finance as well as deviant activity to achieve wealth and success.

Methodology and Analytics

Clarke (1980) introduced a number of propositions that can be tested like individual hypotheses. Beebe and Rao (2005) expanded the propositions laid out by Clarke (1980) by including components of information security. The extension of situational crime prevention theory encapsulates the current studies assumptions with the exception of Propositions 5 and 6 (Beebe & Rao, 2005). Therefore, the extension of situational crime prevention theory and further revision of information security effectiveness to apply to blockchain technology resulted in the following propositions:

Proposition 1. The perceived effort required to break a distributed network is positively associated with the overall perceived cost of committing the act.

Proposition 2. The perceived risk of being caught while trying to break a network is positively associated with the perceived cost of committing the act.

Proposition 3. The perceived cost of breaking a network act is negatively associated with the perceived net benefit of the criminal act.

Proposition 4. The perceived anticipated rewards of a successful attack are positively associated with the perceived net benefit of the act.

Proposition 5. The perceived net benefit of breaking a network is negatively associated with hash rate.

Proposition 6. The level of successful rationalization moderates the influence of perceived net benefit on blockchain security effectiveness.

In regard to Proposition 1, "effort" and "cost" may be defined similarly in certain disciplines (Williamson, 1989). The current paper conceptualizes "effort" as, but not limited to, the time, energy, etc. an individual or organization puts into breaking a network. The "cost" of committing an act or breaking a network refers only to the financial or monetary costs to commit the crime.

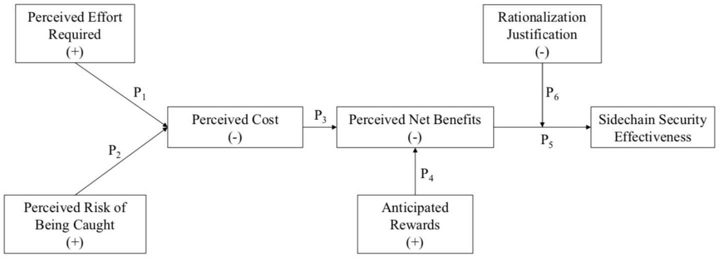
Perceived Effort Required (+)
Rationalization Justification (-)
P_1
P_6
Perceived Cost (-)
P_3
Perceived Net Benefits (-)
P_5
Sidechain Security Effectiveness
P_2
P_4
Perceived Risk of Being Caught (+)
Anticipated Rewards (+)

*Figure 2.*Theoretical Model for Sidechain Security

These propositions are heavily based on the situational crime prevention theory propositions (1-4) and those laid out by Beebe and Rao (2005). This leads to a similar theoretical model to test the effectiveness of sidechains with the added clarification of concepts found in the propositions. Figure 2 is a visual representation of how each proposition influences each other in a theoretical flow-chart. Each proposition carries with it different costs and benefits and are quantified differently by each individual.

It is important to identify the values and cost of a 51% attack in PoW networks, and even more generally, the cost to simply break it in one way or another. Blockchain networks, specifically public crytpocurrency networks, have native and non-native assets. For example, the native token of Ethereum (Buterin, 2014), is Ether, meaning it is the currency used for payments of transaction fees on the network. If, however, one created a token representing 1 Bitcoin on Ethereum, that token would be a 'non-native' asset, since it represents something on another chain (Bitcoin in this case). For demonstration purposes, both of our example networks will be separate Ethereum chains using various forms of Ether (ETH). Where the dApp chain is the sidechain (or not the main network) and dEth the native currency of this chain: the value of the native decentralized application (dApp) chain Ether (dEth) is the summed value of utility tokens on the sidechain's ecosystem. This summed dEth is the native currency of the dApp chain (if one) and, in the case of public PoW sidechains, is used to incentivize the security of the network. Another value that needs to be considered is the summed value of mainchain Ether (mEth) locked onto any single sidechain. Once again, mEth is only the summed amount of Ether locked onto the sidechain, ETH in other Mainnet contracts or wallets or even other sidechains is not included in this value. The cost to actually steal the ETH must also be understood. This cost in the case of a 51% attack is calculated by hashrate which comes from the ability to attract new miners to the sidechain who then compete to mine new blocks.

The minimum cost to steal the mainchain asset on the sidechain (mEth) is determined by placing these values into an appropriate equation. An unfortunate drawback for the hacker would be the proportion of the value received from the attack will be offset from the risks, effort, and costs of the attack. It will be dependent on the setup of the system as to what the terms of withdrawal are now, but assuming non-validated exits (security of the mEth is provided by the sidechain and not the mainchain), a 51% attack on either of the chains can lead to funds being unlocked in the mainchain. For the purpose of this paper however, a 51% attack is too narrow a definition. Depending on the type of network, construction of the smart contracts bridging the chains, or type of consensus mechanism, the cost to break a chain is not singularly the cost of a 51% attack.

Whether this is staking and breaking a relay or validator network, the cost to spam an oracle eternally, or the cost of simply 51% attacking the network, the goal is the withdrawal of the locked Ether. Note that PoS does not make a chain secure from this either, the mechanism to break the chain is just different. Especially in the case of the dPos (delegated Proof-of-Stake) or POA (proof-of-Authority) networks, even beside the point that they are not decentralized, the cost to corrupt the operators of the network is still a finite number.

The main factors that need to be taken into consideration when attacking a network is simply whether the risk, effort, and cost to break the network is less than the reward. Although this cost is associated with the monetary cost of breaking the network, the cost can include the cost of obtaining/switching your miners, the missed value you could accrue mining on other chains, or in the case of staking, the interest that could be generated from that capital if deployed elsewhere. As it applies to situational crime prevention theory, opportunity cost also incorporates perceived effort, perceived cost, and perceived risk which are outlined in Propositions 1-3.

$$a51 = f(\text{perceived risk, perceived effort, perceived cost})$$

To simplify the idea of this cost for our article, 'a51' will be used to measure the total opportunity cost to steal all value on the dapp chain. The basic assumption we can make is that if mEth > a51, the network is unsafe.

Therefore, to maintain stability:

$$a51 > mEth$$

Unfortunately for this simple equation, the benefit to malicious actors in our game theory scenario has been solely focused on the monetary benefit parties could extract from the system. This is likely an exaggerated amount for several reasons: First, the value of a theft must be discounted by the amount one would be able to realistically exit with (value of mEth given a51). How much could the attacker sell the mEth for on the open market if a successful attack were to take place? While the volatility could impact the sale price, the worth of total mEth stolen could dramatically impact the value of the asset. This was seen after the Mt. Gox hack when Bitcoin lost more than 80% of its value (Cheung, Roca, & Su, 2015). Furthermore, will the network accept the attacker's stolen Eth, or will it largely be tainted? Similar to marked bills or money that has been subjected to a dye pack after a bank robbery, many digital assets can be tracked due to the public and decentralized nature of many blockchains. All transactions are recorded onto the distributed ledger which can be read by anyone. Parties will be able to tell if an asset has been tainted based on the last point of egress from a compromised network. If these stolen assets are purchased, then it could be comparable to buying other stolen goods. These factors and more reduce the total value of the mEth.

In addition to discounting the value of mEth after an attack, the expected return of a successful attack on a distributed network must also be discounted by the risk of failure. The exact calculation will depend on the setup of the system, however simple examples of repercussions for failure include: loss of reputation (if you are known), slash of some bond (in Proof-of-Stake systems), and recognition of attack vector (the system can change if it recognizes that you are getting close to a successful attack). The value of the theft must be discounted by the risk of failure of the attack, thus giving us the equation:

$$\textit{Perceived net benefit} = \textit{Expected discounted value of sold Ether} = f(\textit{mEth,post attack Liquidity of mEth, 1-perceived risk of failure})$$

On the other hand, the value of the attack should also be increased by non-mEth gains. Nakamoto (2008) assumed that miners cannot benefit from a price decline. One of the great properties of distributed networks is that even if you break it and steal all of a digital asset like Bitcoin, the assets at that point are worthless. Unfortunately, in today's world though, there are ample opportunities to gain from a price decline. If parties can short the native token on an exchange, the potential compensation could be much larger than even the original valuation of the native token. If for instance, one could short dEth, they would have a profit only limited by their access to capital and the liquidity of the derivatives contract. In addition, the competitors of the dApp have other (albeit harder to measure) benefits of attacking the dApp chain. Competitors to a product may have a decreased opportunity cost due to the addition of the following element as follows:

$$\Sigma \textit{discounted future expected profits given no sidechain} + \Sigma \textit{gains from attack information (shorting)}$$

Whereas the previous state of balance was:

$$a51 > mEth$$

we can now expand to:

$$f(\text{mining profitability relative to other coins})+f(\text{cost of switching miner}) > f(\text{mEth})+f(\text{post attack Liquidity of mEth})+f(1 - \text{perceived risk of failure}) + \Sigma\text{discounted future expected profits given no sidechain} + \Sigma\text{gains from attack information (shorting)}.$$

This cost to destroy the chain (left hand side) can now be represented as constant C.
The probability of success (1 - perceived risk of failure) and post attack liquidity of stolen mEth can be combined to become a less than 1 multiplier of mEth:

$$\beta = (1 - P(\text{Failure}))*E(\text{discount of stolen mEth})$$

Where E(discount of stolen mEth) is the expected discount given to the stolen good; (e.g 90% would imply a 10% value reduction post theft).
Now we arrive on our final solution. For stability to hold:

$$C \geq \beta * mEth + \pi$$

Where:

$$\begin{gathered} C = \text{cost to steal Ether (break chain)} \\ \beta = (1 - P(\text{Failure}))*E(\text{discount of stolen mEth}) \\ mEth = \text{value of external tokens on chain} \\ \pi = \Sigma\text{discounted future expected profits given no DDA chain} \end{gathered}$$

Solutions

The most straightforward solution to deter any potential attack is limiting the amount of value on a given network. Cap the amount of mEth allowed on a sidechain as a function of the probability of a 51% attack. As the mEth-to-CSM ratio becomes greater than the probability of attack increases. This means, the amount of mEth allowed in any one contract is conditional and therefore limited and can be expressed as:

$$mEth\ allowed = f(P(a51))$$

This is still dangerous though as it assumes perfect information with regard to the variables. Even if certain variables (e.g. value of stolen mEth), several of the variables are largely subjective (e.g. benefit to a competitor, perceived risk of failure). The vast amount of information about non-native chain entities and variables also makes the system reliant on a third party to input these values or make judgment calls based upon how they are measured. If you have a public sidechain for example, but only one party controlling the access point, the entire value of the chain is dependent upon the goodwill of that entity to allow continued access up to the security allowance of the network. This reliance on a third party runs in opposition to the purpose of these networks and is likely not ideal for anything other initial bootstrapping periods for the network.

This solution above addresses Proposition 3, Proposition 4, and Proposition 5. The perceived rewards and benefits of an attack are effectively reduced by limiting the value present on the sidechain. This comes at an operating cost that trades scalability for security, a blockchain issue that is solved by the implementation of sidechains. Therefore, extensive use of value limits would effectively reduce the usability of sidechains as a scalable solution.

Another solution to securing sidechains is to have all security provided by the mainchain. This works by having all tokens locked on the other network fully tracked and verified by the origin network.

The largest example of this being done is the Lightning Network on the Bitcoin blockchain (Poon & Dryja, 2016). The basic concept is that two users lock funds into a smart contract. The rules of the contract enforce that all transactions performed off-chain (off the mainchain or on the sidechain) must be proven by signatures of the parties. Here is an example of a payment channel on Ethereum:

> Alice deposits 100 Ether into a smart contract on the mainchain
>
> Alice sends transaction A - 50 Ether to Bob
>
> Bob sends transaction B - 10 Ether to Alice
>
> Alice sends transaction C - 20 Ether to Bob
>
> Alice or Bob wants to withdraw their Ether on the mainchain (take it out of the smart contract).
>
> Alice submits a proof (signed transactions A, B, C)
>
> Bob approves (cannot submit alternative proofs (e.g. a transaction D where Alice sends him more))
>
> The payment channel is closed, and Alice now has 40 Ether and Bob has 60.

In terms of our analysis, this security mechanism renders P = 0. By making the probability of them successfully exiting with the mEth 0, then the benefit of breaking the network is that of the competitor analysis. Parties can still break your sidechain (e.g. corrupt a central party, 51% attack if another public chain, or attack the method for transmitting data back and forth between the chains), but the locked asset (mEth) is safe. Currently, there are also serious limitations to sidechains like this, one solution for this is Plasma (Poon & Buterin, 2017).

This solution outlines Proposition 1 and Proposition 2 by increasing the efforts, risks, and costs of breaking a sidechain. Increasing attributes related to security will logically increase the cost of breaking the sidechain. The mainnet of any blockchain is going to be inherently stronger the sidechain. This strength will bolster the weakened immunity of the sidechain until the sidechain has garnered the hashrate required to run independently from the mainnet. This appears to be the most attractive solution to scalability and security for the time being. However, continual updates to security to increase efforts, risks, and cost of an attack could increase opportunities to attack the network.

As these solutions are implemented, the perceived net benefit is altered (Proposition 6). Some solutions will impact selective propositions laid out in this paper, but any solution will affect Proposition 6. Rationalization changes the net benefit perceived by the attacker, but this psychological concept can lead attackers to be overly confident when they have no reason or be cautious when faced with a complex but weak network. Developing a network and effective security functions should serve to deter would-be attackers, decrease net benefits, and defend against attacks that are committed.

The Role of Miners and Mining

Mining Rewards

If the relationship between value locked on the sidechain and new miners is linear (b=1) then there is no risk that an a51 will occur. However, if there is an exponential growth in value without a corresponding growth in new miners then a51 risk will begin to develop. That risk will rise exponentially with the volume of mEth on the sidechain. Since we do not want to limit usage of the platform (mEth), the only way to increase security on the network is to increase a51 (get more miners). There are a few ways to do this:

First, the network can incentivize miners by paying miners in mEth instead of the native currency. The majority of distributed systems (Bitcoin, Ethereum, etc.) compensate their miners in the native digital asset that is being mined. However, it may be wise to pay miners in mEth if faith in the native asset is low because of its new status in the ecosystem. This can be done in a centralized manner by simply setting a pool of mEth aside on the mainchain for proof-of-mine on the sidechain.

Second, the network can "peg" the value of dEth or at least give the native asset a minimum value. The volatility of cryptocurrencies has been notorious since their inception almost a decade ago. This volatility has lead retail and institutional investors hesitant to enter the market. However, the volatility of cryptocurrency has the possibility of deterring miners because the value of an asset could be worthless. That being said, the network could make dEth a stablecoin. A stablecoin is a cryptocurrency whose value is tied to the value of a more stable asset like the US dollar or precious metals like gold or silver (Cao et al., n.d.). Most stablecoins, such as DAI (Bajic, 2018) or Tether (Tether International, 2018), are pegged to the US dollar and do not fluctuate in value the same way other assets change. This would essentially guarantee the miner proper remuneration for their participation.

Third, the network can incentivize the ownership of dEth. Incentivizing miners to own dEth can occur in several ways including, the promise of dividends or the expectation of increased value in the native asset. According to a 2017 survey conducted by Yahoo Finance, almost 71% of people who purchased Bitcoin made money on their investment. Conversely, only around 8% of investors in Bitcoin lost money (Yahoo Finance, 2017). Networks can provide current statistics on the performance of similar products or digital assets to provide a proxy as to how a native asset will perform. This information could give confidence to potential miners which could lead to increased participation. In a similar way, the network can identify similar projects that provide evidence of substantial gains in their valuation. If the valuation of a company is likely to increase, then accepting dividends may entice miners to start mining on the platform.

Miner Participation

For public sidechains with a PoW structure, a great amount of initial investment is needed on the side of miners to make the sidechain safe. However, this creates a chicken and egg scenario as the network is only safe (and worth money) if lots of miners are present and miners will only enter a scenario if their efforts are compensated (network is worth money). If too few users are active on a sidechain then there is no incentive for miners to mine any sidechain asset. A potential solution is a merged mining outcome where the miner will be paid in the mainchain asset as well as the sidechain asset. This however can be very expensive to pay miners on your network in a non-native asset. The structure can be done in such a way that the reward in mEth is tied to usage on the sidechain, however there can then be issues due a sudden influx in usage of the sidechain. This creates a significant flood of mainchain asset on the sidechain without the support of a sufficient miner base to secure it. This creates a scenario where it's more valuable for an actor to attack the sidechain for the mainchain asset for a large, one-time payday as opposed to choosing a moral and potentially more lucrative long-term option of becoming a miner.

Additionally, to clarify the motive for stealing specific assets can only be applied to stealing mainchain assets. It is not logical to break a sidechain with the intention of stealing the sidechain's assets because the value of the sidechain asset would plummet in the wake of a hack. As is the case with most 51% attacks in crypto networks, parties who hack the network need to rely on some off-chain (or other chain) component which is treating the chain as finalized. If you break the sidechain and steal 100% of the assets for instance, the sidechain will likely update itself to be more secure (e.g change PoW algorithm) and revert back the changes. In order to benefit, one would need to be able to take the assets to an off-chain component (e.g. an exchange or mainchain) and trade those assets for non-native tokens of the sidechains. Therefore, any intent to break the sidechain would be to discard the sidechain asset completely and sell the mainchain asset whose value would suffer little to any loss.

Concerns and Limitations

One of the largest concerns for situational control theory is the phenomenon of displacement. Displacement has been defined as "... a change in offender behavior, along illegitimate means, which is designed to circumvent either specific preventive measures or more general conditions unfavorable to the offender's usual mode of operating" (Gabor, 1990:66). Criminal displacement occurs when effective crime control strategies are implemented (Gabor, 1990). Displacement (Clarke 1983), has been labeled as a concern for situational crime prevention theory and its practical implementations; however, many people do not share these sentiments. Several theorists have laid out arguments in opposition to displacement (Clarke & Weisburd, 1994; Cornish & Clarke, 1987, 1989), while other researchers have set out to test the theoretical assumptions of displacement and found little support for the concept (Barr & Pease, 1990; Bowers & Johnson, 2003; Brantingham & Brantingham, 2003; Weisburd et al., 2006; Weisburd & Green, 1995). Furthermore, Guerette and Bowers (2009), found evidence to suggest that the benefits of crime reduction in targeted areas outweighs the costs caused by increases in crime caused by displacement.

Temporal displacement is waiting until the creators of a project create an error in their programming. Many projects today are open sourced and therefore are subject to scrutiny by hobbyists, competitors, or potential criminals. Network upgrades happen frequently and are a potential vulnerability when non-native assets are at stake. A criminal may also wait until volume increases on a network if security issues are not fixed. This would lead to a bigger "take" instead of the small gains garnered from a short-sighted, impulse driven attack.

Tactical displacement is a change in the modus operandi of a criminal. A criminal may modify their way of doing things if a blockchain employs a specific security protocol that protects against a criminal's normal method of attack. One specific example is the use of ASIC resistant PoW algorithms to prevent 51% attacks. Bitcoin uses a specific PoW algorithm that allows for Application-specific integrated circuits (ASICs) to be used for mining. Attackers who wish to build up enough hashrate to 51% attack a network would likely buy up enough ASICs to have a majority. For smaller chains (non-Bitcoin), a PoW algorithm similar to Bitcoin represents a major security vulnerability since a mining pool or large miner could simply switch from mining Bitcoin to mining the smaller network. If this happened, the large Bitcoin miner would likely have a very large proportion of the hashrate on the smaller chain. To prevent this, smaller chains usually utilize 'ASIC resistant' algorithms for their PoW. This prevents miners from easily switching networks and attacking the network. The criminal would then be required to change their attack strategy from a pure ASIC based over run of the hash power to a more nuanced strategy specifically developed for the new algorithm.

Another example is that of the DAO hack (Daian, 2016; Siegel, 2016). This specific attack used a little-known attack called a 'reentrancy attack', where the attacker successfully tricked the smart contract into allowing all of the funds to be withdrawn. At the time, the DAO smart contract held 15 percent of all Ether. Rather than allowing the attacker to run away with the stolen Ether, the network was forked (or reverted) back to the state where he did not perform the attack and the smart contract was liquidated to the proper owners. With this attack vector now very well known, smart contract developers are more cognizant to prevent this attack and criminals must use different methods to attack the contract.

Conclusion

In the current paper, the authors analyzed the viability of sidechains and the crypto-economic incentives that may differ from running just one network. Noted are the numerous disadvantages and security concerns to using sidechains. Without security being provided by the mainchain in the form of validated exits, sidechains or state-channels which have a bridged or mainchain asset representation are at a significant risk of attack. By using both theoretical mathematics along with presenting attackers of these networks as criminals, the analysis utilized situational crime prevention theory to perform a vulnerability analysis of the base claims of sidechains. Much of the analysis can be applied to any distributed system (e.g. blockchain network), especially any decentralized off-chain component. The equations developed in the current study will hold for any two chains that are bridged and pass value back and forth and provides evidence to suggest that use of a sidechain must be accompanied by centralization in the consensus mechanism or security provided by the mainchain for all but trivial uses.

Testing the theoretical assumptions laid out in the paper can be difficult due to the fact that decentralized networks rely on anonymous participants and are secured through often costly hardware or built-in incentives; however, this does not indicate additional research cannot or should not be undertaken. Future studies should focus on the parties who have briefly attempted or considered committing an attack or hack on a distributed network. The decisions made by individuals to forgo attacks are just as valid as those who have tried to attack networks. These results could provide evidence to suggest support for the situational crime prevention theory and the mathematical assumptions proposed here in the paper.

Blockchains are complex systems, and the risk and perceived effort cannot be empirically captured from existing attacks. A 51% attack has never occurred in a laboratory experiment, so a quasi-experimental design would have to be employed to generate the situations where a person may attack a network. Furthermore, testing these concepts may have to be done using abstract constructs. Zelditch (1969) made the argument for studying complex organizations in a laboratory; therefore, studying the distributed cyber systems and abstract concepts that construct peoples' perceptions could be accomplished. However, the results of these studies should not be directly generalized or applied without careful consideration as many assumptions would have to be made about an individual's thought process and behavior to conduct these simulations. These assumptions might allow for too much error to use the simulation's results effectively. In summation, the paper serves as a cautionary tale for the implementation of sidechains but a glimmer of hope for the trajectory of security in the blockchain ecosystem.

References

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology, 4*, 643-656.

Bajic, M. D. (2018). *Coin payment processor whitepaper.* Coinpaymentprocessor.org.

Barr, R., & Pease, K. (1990). Crime placement, displacement, and deflection. *Crime and Justice, 12*, 277-318.

Beebe, N. L., & Rao, V. S. (2005, December). Using situational crime prevention theory to explain the effectiveness of information systems security. *In Proceedings of the 2005 SoftWars Conference,* Las Vegas, NV (pp. 1-18).

Blasco, N. J., & Fett, N. A. (2018). Aligning incentives for bridged sidechains. *Medium*. Retrieved from https://medium.com/@nfett/aligning-incentives-for-bridged-sidechains-5bb85d405dab

Bowers, K. J., & Johnson, S. D. (2003). Measuring the geographical displacement and diffusion of benefit effects of crime prevention activity. *Journal of Quantitative Criminology, 19*(3), 275-301.

Brantingham, P. J., & Brantingham, P. L. (2003). Anticipating the displacement of crime using the principles of environmental criminology. *Crime Prevention Studies, 16*, 119-148.

Buterin, V. (2014). *A next-generation smart contract and decentralized application platform*. Github.

Carson, E. A. (2018). *Prisoners in 2016* (NCJ 251149). Washington, DC: Bureau of Justice Statistics.

Cao, Y., Dai, M., Kou, S., Li, L., & Yang, C. (2018). Designing stable coins. Retrieved from https://duo.network/papers/duo_academic_white_paper.pdf

Cheung, A., Roca, E., & Su, J. J. (2015). Crypto-currency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices. *Applied Economics, 47*(23), 2348-2358.

Clarke, R. V. (1980). Situational crime prevention: Theory and practice. *The British Journal of Criminology, 20*(2), 136 - 147.

Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. *Crime and Justice, 4*, 225-256.

Clarke, R.V. & Homel, R. (1997). A revised classification of situational crime prevention techniques. In: Lab, S.P., ed. Crime prevention at the crossroads (pp. 17-27). Cincinnati, OH: Anderson.

Clarke, R. V. (2013). Seven misconceptions of situational crime prevention. In *Handbook of Crime Prevention and Community Safety* (pp. 65-96). Philadelphia, PA: Routhledge.

Clarke, R. V., & Weisburd, D. (1994). Diffusion of crime control benefits: Observations on the reverse of displacement. *Crime Prevention Studies, 2*, 165-184.

Coinmarketcap.com. (2019, August). *Global charts.* Retrieved from https://coinmarketcap.com/charts/

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology, 25*(4), 933-948.

Cornish, D. B., & Clarke, R. V. (1989). Crime specialisation, crime displacement and rational choice theory. *Criminal Behavior and the Justice System* (pp. 103-117). Berlin, Heidelberg: Springer.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies, 16*, 41-96.

Daian, P. (2016). DAO attack, 2016. Retrieved from http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit.

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security, 7*(4), 171-175.

Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers & Security, 20*(8), 715-723.

Dhillon, G., Silva, L., & Backhouse, J. (2004). Computer crime at CEFORMA: a case study. *International Journal of Information Management, 24*(6), 551-561.

Gabor, T. (1990). Crime displacement and situational prevention: Toward the development of some principles. *Canadian Journal of Criminology, 32*, 41-73.

Guerette, R. T., & Bowers, K. J. (2009). Assessing the extent of crime displacement and diffusion of benefits: A review of situational crime prevention evaluations. *Criminology, 47*(4), 1331-1368.

Leclerc, B., Wortley, R., & Smallbone, S. (2011). Getting into the script of adult child sex offenders and mapping out situational prevention measures. *Journal of Research in Crime and Delinquency, 48*(2), 209-237.

Lemieux, A. M., & Clarke, R. V. (2009). The international ban on ivory sales and its effects on elephant poaching in Africa. *The British Journal of Criminology, 49*(4), 451-471.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Poon, J., & Buterin, V. (2017). *Plasma: Scalable autonomous smart contracts.* Plasma.io.

Poon, J., & Dryja, T. (2016). The bitcoin lightning network: Scalable off-chain instant payments. Retrieved from https://lightning.network/lightning-network-paper.pdf.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216-238.

Siegel, D. (2016). *Understanding the DAO attack.* Retrieved from http://www.coindesk.com/understan ding-dao-hack-journalists.

Straub Jr, D. W. (1987, December). Controlling computer abuse: An empirical study of effective security countermeasures. *ICIS 1987 Proceedings.* 277-289.

Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Tether International. (2018). *Tether whitepaper.* Technical Report. Tether International Limited, Hong Kong. Retrieved from https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf.

The Council of Economic Advisors (2018, February). *The cost of malicious cyber activity to the U.S. economy.* Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Weisburd, D., & Green, L. (1995). Policing drug hot spots: The Jersey City drug market analysis experiment. *Justice Quarterly, 12*(4), 711-735.

Weisburd, D., Wyckoff, L. A., Ready, J., Eck, J. E., Hinkle, J. C., & Gajewski, F. (2006). Does crime just move around the corner? A controlled study of spatial displacement and diffusion of crime control benefits. *Criminology, 44*(3), 549-592.

Welsh, B. C., & Farrington, D. P. (2009). Public area CCTV and crime prevention: An updated systematic review and meta-analysis. *Justice Quarterly, 26*(4), 716-745.

Williamson, O. E. (1989). Transaction cost economics. *Handbook of Industrial Organization, 1*, 135-182.

Wobber, E., Abadi, M., Birrell, A., & Lampson, B. (1993). *U.S. Patent No. 5,235,642.* Washington, DC: U.S. Patent and Trademark Office.

Yahoo Finance. (2017). *Yahoo finance bitcoin survey.* Retrieved from https://www.surveymonkey.com/results/SM-7QY5VM9J8/

Zelditch Jr, M. (1969). Can you really study an army in the laboratory? *A Sociological Reader on Complex Organizations,* 528-539.