EXAMINING LEGISLATIVE ISSUES WITH BLOCKCHAIN TECHNOLOGY

By

JACK HARRISON BIGBEE

_____

A Thesis Submitted to The Honors College

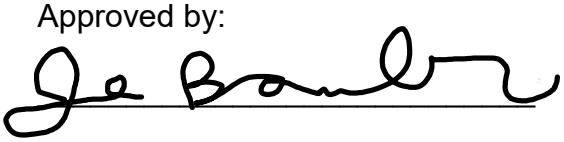
In Partial Fulfillment of the Bachelors degree
With Honors in

Law

THE UNIVERSITY OF ARIZONA

M A Y 2 0 1 9

Approved by:



Professor Jane Bambauer
Department of Law

EXAMINING LEGISLATIVE ISSUES WITH BLOCKCHAIN TECHNOLOGY

Jack Harrison Bigbee

ABSTRACT

The purpose of this thesis is to examine the legislative issues that blockchain technology has created, in the form of a Law student note. Blockchain technology is a disruptive technology that conducts transactions in a decentralized environment. This unique technology has created a host of legislative problems pertaining to accountability, liability, and enforcement. By understanding the types of crimes that can occur on a blockchain, how they can be remedied, and who is potentially liable for them, we revealed several instances where the government may be unable to enforce or regulate blockchain platforms. Blockchain platforms will require unique legislation that adheres to the principles of a decentralized environment without sacrificing authority.

TABLE OF CONTENTS

* * *

INTRODUCTION

Blockchain provides a platform for immutable content storage and unrestricted financial freedom, which in turn creates a lawless digital environment where criminal activity can thrive. Legislative issues concerning the technology revolve around a lack of accountability and liability. Authorities, like Federal and State governments, cannot easily enforce regulations on this technology due to the widespread and immutable nature of the platform[1]. Blockchain platforms can become "tainted" with illegal materials which cannot be removed, and the operators of the nodes can be held liable for possessing or facilitating illegal material[2]. Blockchains can also facilitate illegal financial transactions and assist in white collar crimes[3]. The United States government has not made it clear how it will hold criminals accountable in these situations and how they plan on enforcing laws that regulate decentralized environments[4].

The goal of this thesis is to explore the United States government's ability to enforce regulations that hold entities accountable for certain crimes that are committed on a blockchain platform. I will accomplish this by examining the different types of crimes that can be committed on a blockchain platform. I will also explore ways that these crimes can be remedied. I will investigate how accountability and liability is assigned for crimes committed on a decentralized platform.

WHAT IS A BLOCKCHAIN?

To understand the political and policy challenges facing Blockchain technology, one must have a fundamental understanding of what Blockchain is and how it works.

Blockchain technology is a type of disruptive technology that uses a distributed ledger to create a decentralized trust[5]. This trust can be applied to any number of situations, changing the way trust-based operations work[6]. This technology is however susceptible to nefarious activities such as money laundering and the distribution of illegal materials[7]. Information that

---

[1] (Orcutt)
[2] (McReynolds)
[3] (McReynolds)
[4] (Orcutt)
[5] (Jaikaran)
[6] (Jaikaran)
[7] (Lumb, Treat and Jelf)

is embedded into a blockchain is inherently permanent and in many cases, public[8].

A blockchain is a distributed ledger which contains blocks of transactions[9]. A transaction on the blockchain "is an event in which a resource or asset changes possession from one party to another"[10]. Transactions are signed with a user's public and private key information, essentially confirming its validity[11]. Blockchain works by processing groups of these transactions into blocks[12]. The block of data is then encrypted into the chain of previous blocks using cryptography[13]. The block is assigned a unique cryptographic hash which is used to determine the validity of future and previous blocks[14]. Blocks can only be added to the blockchain if they contain valid data and agree that the previous block hashes are valid[15]. Invalid transactions or blocks cannot be added to the blockchain[16]. This system guarantees that data stored on the blockchain is legitimate and immutable[17].

Blockchains are not all the same. There are two main types of blockchain, private and public blockchains[18]. A public blockchain is accessible to everyone and anyone can create an encryption key[19]. Private blockchains are blockchains that can only be accessed and utilized by members of the blockchain[20]. They are not accessible to the public[21].

Blockchains can also be permissioned. Permissioned blockchains require an administrator to assign user's abilities within that blockchain[22]. These blockchains are not centralized around the administrative authority because the administrator does not govern the creation of blocks on the blockchain, just what the users of the blockchain can do[23]. Permissionless

---

[8] (Jaikaran)
[9] (Jaikaran)
[10] (Jaikaran)
[11] (Jaikaran)
[12] (Jaikaran)
[13] (Jaikaran)
[14] (Jaikaran)
[15] (Jaikaran)
[16] (Jaikaran)
[17] (Jaikaran)
[18] (Jaikaran)
[19] (Jaikaran)
[20] (Jaikaran)
[21] (Jaikaran)
[22] (Jaikaran)
[23] (Jaikaran)

blockchains give users equal rights and no one user has administrative power[24].

The privacy of a blockchain determines the ability for users to join or observe the blockchain, while the permissions of a blockchain refers to the user's ability to access to it[25].

Blockchains may have users and nodes. The user of a blockchain is the individual that controls the key pair needed to access and perform transactions on the blockchain[26]. Nodes are computing systems that execute on a blockchain platform[27]. Users may have their own node participating on the blockchain, or they can share their computing power with a group of users on a single node; this is known as a pool[28]. Blockchain nodes are incentivized to provide maximum computing power to the platform by rewarding them for their participation[29]. Blockchain platforms can reward miners in different ways, but the specifics of this is not important for understanding the political and policy challenges facing this technology.

CRIMINAL USE

The technology behind blockchain has created unique political and policy dilemmas. Due to the popularity of certain blockchains and its inherent immutability and anonymity, crime can be facilitated on the platform. Terrorist organizations, drug cartels, pedophiles, and other criminals may use blockchain technology to further their criminal activity. Blockchain platforms can assist in performing anonymous transactions without a centralized trust[30]. Blockchain technology can permanently move and store data and currency without a centralized trust[31]. Blockchain technology can be thought of as "digital cash" due to its immutability and its anonymity, essentially bringing capitalism and crime to the digital world.

There are two main types of crime that can be committed on the blockchain platform, data crimes & financial crimes. The crimes are different because of how they use the platform. Data crimes use the blockchain to store data, while financial crimes use the blockchain to store value.

---

[24] (Jaikaran)
[25] (Jaikaran)
[26] (Jaikaran)
[27] (Jaikaran)
[28] (Jaikaran)
[29] (Jaikaran)
[30] (Jaikaran)
[31] (Jaikaran)

DATA CRIMES

Data crimes use blockchain platforms as a medium for storing and distributing illegal data. Arbitrary content can be inserted into blockchain transactions where it is stored permanently. The content can be replicated by anyone with a copy of the blockchain.

Blockchain is unique because of its decentralized and immutable design. If illegal materials, such as child pornography or classified federal documents, are published to a popular public permissionless blockchain, like Bitcoin or Ethereum, the materials cannot realistically be removed. In fact, Wikileaks took advantage of this strategy in 2012 when they uploaded their "CableGate" leak to the Bitcoin Blockchain[32]. The file was embedded into many consecutive transactions performed on the Bitcoin blockchain, and because the file is stored on the Bitcoin blockchain, it cannot easily be removed. The "CableGate" leak is still accessible directly from the Bitcoin Blockchain.

A study performed by RWTH Aachen University in Germany to discover the arbitrary content that was stored on the Bitcoin Blockchain[33]. The study found that a large amount of copyright violations, malware, privacy violations, politically sensitive content, and illegal content was being stored on the Bitcoin blockchain[34]. The study determined that possessing copies of the Bitcoin blockchain could put individuals in certain countries at risk of prosecution[35].

An article published by Independent about the illegal content lurking on Bitcoin's blockchain claims that cryptocurrency traders in 112 countries can be implicated in breaking the law[36]. According to the article, "Interpol and Kaspersky Lab did warn that blockchain technology could potentially be open to misuse in March 2015, saying there was a possibility illegal or inappropriate data could be "injected and permanently hosted" with no means of wiping it, creating a "safe haven" for cyber-criminals"[37].

FINANCIAL CRIMES

Financial crimes use blockchain platforms as a medium for storing value. Money can be laundered on the blockchain through the use of mixing services and anonymity. Hacks can occur where cryptocurrency can be

[32] (Matzutt)
[33] (Matzutt)
[34] (Matzutt)
[35] (Matzutt)
[36] (Sommerlad)
[37] (Sommerlad)

stolen from users' wallets. Financial crimes are monetary transaction related crimes that occur on a blockchain platform.

Financial crimes flourish on blockchain platforms. A reason for this is because blockchain platforms like Bitcoin can facilitate money laundering[38]. Using mixing services, Bitcoin can be split up and laundered so that is cannot be traced back to its source[39].

Law enforcement's ability to track criminals and enforce regulations makes a massive impact on the amount of blockchain related financial crime that is committed in that country. Cryptocurrency exchanges in countries where there are little to no regulations on exchanges receive 36-times more Bitcoin from money launderers than those with appropriate rules in place[40].

Hackings play a massive role in the financial crimes that occur using a blockchain platform. According to CNBC, "Roughly $1.1 billion worth of cryptocurrency was stolen in the first half of 2018"[41]. Thefts from hackings are so prevalent among blockchain networks that Hackernoon published an article titled "Learn Blockchain's Top 25 Hacks in History"[42].

Criminal Use

Crimes that are committed on the blockchain are unique to other crimes. In the real world, a child pornography distribution ring can be stopped, and the illegal material can be destroyed. On a blockchain platform, the information cannot easily be removed by law enforcement and can be undetectably accessed. Cryptocurrency's are frequently being abused to commit financial crimes, and there are not sufficient regulations put in place to stop this. The fundamental issues that exist with these crimes is the lack of accountability and the inability to enforce regulations.

Remedies

Crimes that occur on a blockchain platforms can be remedied. Money that is stolen can be returned and data that is shared can be censored – it is just extremely difficult to do. This section will examine the remedies for the two main types of blockchain crime.

---

[38] (Canellis)
[39] (Canellis)
[40] (Canellis)
[41] (Rooney)
[42] (Hu)

FINANCIAL CRIMES

The immutable nature of the technology makes censorship not impossible, but very improbable on blockchain networks[43]. For most blockchain setups, a hard fork would have to occur in order to censor or change the existing blockchain[44]. Hard forks can serve to be effective solutions for remedying financial crimes that are committed on the blockchain.

Forking occurs when a change is made to the blockchain's code that creates a new version of the blockchain[45]. Two forms of forking exist, hard forks and soft forks. Hard forks create two working versions of the same blockchain, one with old rules and one with new rules[46]. Soft forks only create two versions of the same blockchain, however only the one with the new rules will work[47]. Chart 1 below shows how soft forks work, while Chart 2 shows how hard forks work:

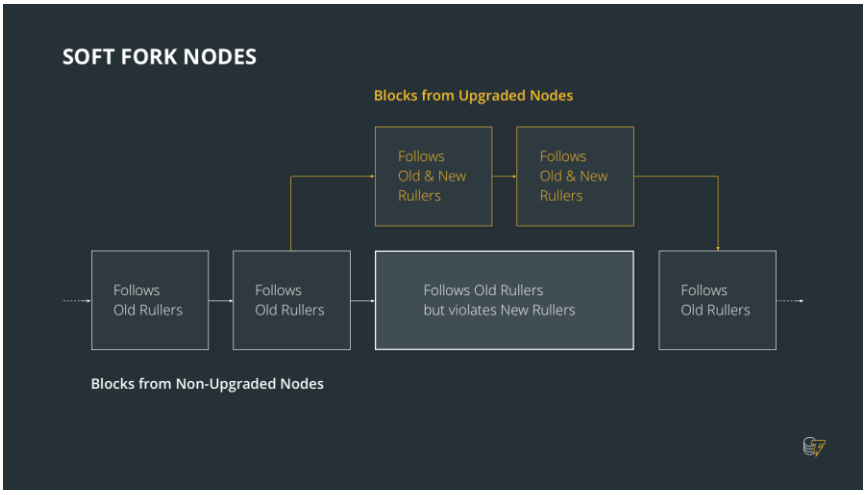


Chart 1[48]

[43] (Greenspan)
[44] (What is Hard Fork)
[45] (Frakenfield)
[46] (Frakenfield)
[47] (Frakenfield)
[48] (What is Hard Fork)

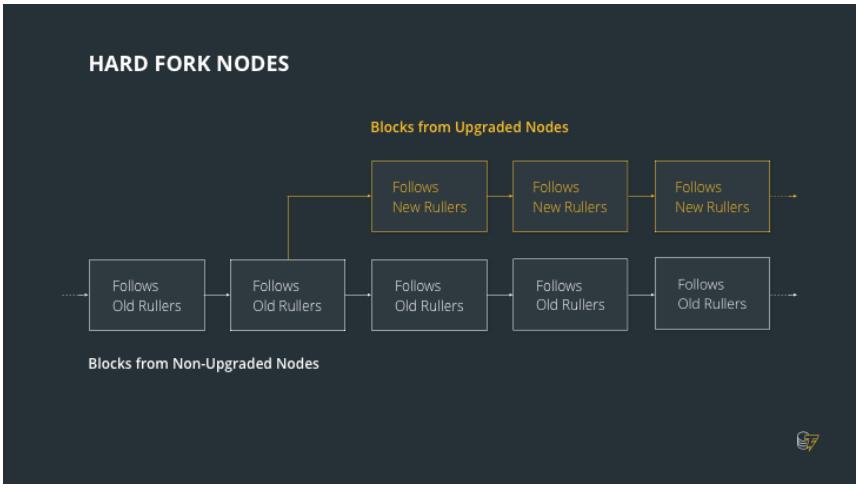


Chart 2[49]

There is only one way to "rewind" a blockchain, and that is to implement a hard fork, sometimes known as a rescue fork[50]. A rescue fork is a hard fork that is implemented on the blockchain that has new protocols and rules that censor or edit previous transactions.

An article published on the popular blockchain technology website Multichain proposes that in blockchain systems there is no such thing as perfect immutability[51]. Ethereum, a popular public permissionless blockchain, voted for a hard fork in June 2016 to fix an exploit that affected a $250,000,000 investment[52]. A minority did not agree to the proposed changes, thus the old version of Ethereum became Ethereum Classic[53]. After going into effect, the hard fork returned the stolen funds back to the original investors[54].

The 2016 Ethereum hard fork is an example of how public permissionless blockchains are not perfectly immutable, and how certain criminal activity can be circumvented through the use of rescue forks. However, it is important to note the repercussions of using this solution.

A second blockchain was created as a result of this hard fork. Ethereum Classic is the old version of the Ethereum blockchain that does not contain the code that returned the stolen funds back to its original

---

[49] (What is Hard Fork)
[50] (Lumb, Treat and Jelf)
[51] (Greenspan)
[52] (Greenspan)
[53] (Greenspan)
[54] (del Castillo)

investors. Ethereum Classic still has value because not everyone agreed to the hard fork patches. Everyone that had Ethereum at the time of the hard fork will now have that same amount in Ethereum Classic. If you owned 1 Ethereum coin at the time of the hard fork, you now own 1 Ethereum coin and 1 Ethereum Classic coin.

It is also important to point out that this solution would be ineffective for remedying data crimes, such as pedophilia or pirated software being stored on the blockchain. This is because hard forking creates two separate blockchains operating under different rules. The newer blockchain will not contain the illegal information, but the older blockchain still exists. The older blockchain would need to be completely eradicated to truly censor the data.

DATA CRIMES

Hard forking is not a very effective method of censoring or removing illegal data that has been stored on the blockchain. It is difficult to remedy data crimes because of the widespread nature of the platform. As soon as something is embedded into a big public blockchain it is essentially permanent, as it has been distributed to nodes all over the world. It is difficult to "clean up" data crimes, making the illegal information inaccessible, due to the decentralized environment that it occurred in.

The German University that scanned the Bitcoin blockchain looking for arbitrary data also released a paper that describes countermeasures that can be taken to prevent data crimes on the blockchain platform[55]. Their study found that, "mandatory minimum fees as well as mitigation of transaction manipulability via identifier commitments significantly raise the bar for inserting harmful content into a blockchain"[56].

Mandatory minimum fees on transactions impose a fee on the amount of arbitrary data being stored on the blockchain[57]. According to the paper, this method would inflate the cost of inserting a single 20 kilobyte JPEG into the Bitcoin blockchain to over a million dollars[58].

Mitigation of transaction manipulability via identifier commitments essentially means replacing the blockchain protocol that allows data to be arbitrarily inserted with a new protocol that cannot be manipulated.

Both of these proposed solutions can be deployed easily to blockchain technologies and can prevent nefarious arbitrary data storage.

---

[55] (Matzutt, Thwarting Unwanted Blockchain Content Insertion)
[56] (Matzutt, Thwarting Unwanted Blockchain Content Insertion)
[57] (Matzutt, Thwarting Unwanted Blockchain Content Insertion)
[58] (Matzutt, Thwarting Unwanted Blockchain Content Insertion)

A research article published in the Journal of the Association for Information Systems examined the accountability aspect of Blockchain legislation. According to the paper, accountability is an aspect of blockchain technology that will require compliance with governing institutions[59]. Their research found that identity is a key factor when it comes to accountability issues facing blockchain[60].

Two proposed solutions were: 1) creating platforms that associate user's public addresses with their driver's license and 2) creating reputation scores for public addresses[61]. If a crime is committed on a blockchain platform and there is no identity associated with the public address, it is nearly impossible for authorities to enforce regulations that hold the individual user accountable.

These proposed solutions deter criminal activity by sacrificing anonymity. These features would likely need to be legally mandated, as anonymous cryptocurrencies and blockchain platforms are very popular.

ACCOUNTABILITY & LIABILITY

The wide range of criminal uses and the unique design of blockchain technology emphasize the importance of different approaches to accountability and liability depending on the specific scenario. Some criminal scenarios will require holding the user accountable, while other scenarios will focus on code-writing core groups. This section will examine the potential liability of users and nodes that operate on a "tainted blockchain" as well as the core developer groups that code the platform.

CDA 230 LIABILITY

Section 230 of the Communications Decency Act says "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider"[62]. Section 230 is important because it legally protects online companies from illicit content their users might share.

There is an important distinction that needs to be made in order to receive legal coverage from CDA Section 230. Technology companies that offer a platform for their users must stand out as facilitators and not decision-makers. The developers of the technology cannot consciously make decisions that assist criminal activity. An online company called Backpage plead guilty to human trafficking after it was found that they knowingly facilitated a

[59] (Beck, Müller-Bloch and King)
[60] (Beck, Müller-Bloch and King)
[61] (Beck, Müller-Bloch and King)
[62] (Electronic Frontier Foundation)

platform that condoned human trafficking[63].

LIABILITY OF NODES ON A TAINTED BLOCKCHAIN

Nodes and users that own a copy of a blockchain can be potentially exposed to content that could subject them to prosecution, if the blockchain becomes tainted[64]. A blockchain becomes "tainted" when illegal materials have been stored on it.

An article published in Coin Telegraph discusses the idea of nodes being prosecuted for hosting illegal content. The article asked corporate attorney Dean Steinbeck if nodes can be prosecuted for hosting illegal content, he replied:

> "Possession of child pornography is a crime, though it is still unclear how child pornography laws apply to node operators who are not viewing or curating the data being stored. These laws were drafted to be technology agnostic, meaning there is no exception for Blockchain nodes, so its likely that node operators will be treated like other data storage providers, for example, Facebook, Amazon Web Services, Google, etc."[65]

The attorney went on to explain that the true center of this issue should be what is the appropriate punishment for nodes that "did not know they were in possession, never viewed the unlawful content, and did not knowingly distribute it"[66].

The article highlights another issue, there is a lack of legislation regarding this kind of activity[67]. There is a high demand for clear legislation that regulates this disruptive technology and gives users a clear understanding of their legal liability under the law.

CORE DEVELOPER GROUP LIABILITY

Unfortunately, Core Developer Group Liability is very unclear as well. There has been no clear application of CDA 230 liability to blockchain platforms yet and current regulations do not clearly explain which regulations affect which blockchain platforms. However, the judicial system does offer a unique insight to how these problems might be addressed in the future.

---

[63] (Manchester)
[64] (Mattzutt)
[65] (Jenkinson)
[66] (Jenkinson)
[67] (Jenkinson)

The US District Court for the Northern District of California is handling one case that may have an incredible impact on the accountability and liability issue that faces the technology. Currently there is a pending class action lawsuit against the team that developed the cryptocurrency Nano (XRB) and the CEO of BitGrail[68].

The Class Action Complaint explores two relevant enforcement and accountability questions that pertain to blockchain political policy: Are certain blockchains considered securities that must follow SEC regulations, therefore rendering the code writers liable for damages? And, can the United States government effectively order a rescue fork operation on a blockchain?

A. Background

On February 8, 2018 an unauthorized transaction was performed on BitGrail, a platform that allowed customers to purchase XRB, that resulted in $170,000,000 worth of XRB being stolen[69].

According to the lawsuit, the Nano Development team worked closely with BitGrail and recommended the service as a secure platform to purchase XRB[70]. Nano Development is being accused of either not doing their due diligence when recommending a safe place to purchase their product or knowingly disregarding material concerns about BitGrail's platform in terms of safety and security[71].

B. Is it a Security?

A large aspect of this case hinges on determining whether or not Nano Development violated United States securities laws by not registering the cryptocurrency as a security with the SEC[72]. The Nano Development team did not register the cryptocurrency with the SEC, nor did they file for an exemption[73].

The Nano Development team distributed XRB for free via a faucet system, which is an argument that has been used to claim that they do not pass the Howey test to be considered a security[74]. The plaintiff argues that because Nano has "absolute control over essentially every aspect of XRB

---

[68] (FABIAN v. NANO)
[69] (FABIAN v. NANO)
[70] (FABIAN v. NANO)
[71] (FABIAN v. NANO)
[72] (Jimenez)
[73] (FABIAN v. NANO)
[74] (Jimenez)

and its value" it is a security[75]. The Defendants have filed a motion to dismiss the lawsuit by claiming that XRB is not a security and therefore they cannot be held liable or accountable for losses incurred by XRB purchasers[76].

If the court finds that XRB is indeed a security, Nano Development could be liable to provide rescissory, compensatory, punitive and injunctive relief to their investors[77]. In this scenario, the court would be assigning liability to the Nano Development team and they would be subjected to the SEC's security regulations. This could have massive implications on the entire cryptocurrency community.

C. Court Ordered Rescue

The other significant aspect of this lawsuit can be found in the Prayer for Relief. The Prayer for Relief in the Class Action Complaint asks for judgement that the Defendants offered and sold unregistered securities in violation of federal securities laws and:

> "A judgment awarding Plaintiff and the Class equitable restitution, including, without limitation, rescission of their investments in all XRB held in accounts at BitGrail, restoration of the status quo ante, return to Plaintiff and the Class all cryptocurrency or fiat currency they paid as a result of Defendants' unlawful and unfair business practices and conduct, and an order requiring NANO to "rescue fork" the allegedly missing XRB into a new cryptocurrency in a manner that would fairly compensate Plaintiff and the Class for each missing XRB and would eliminate all of the "missing" XRB;"[78]

This proposed remedy is groundbreaking in the world of crypto-law. The possibility of a court ordered "rescue fork" (or "hard fork") would be unprecedented and very unique from an enforcement perspective.
An article published in the MIT Technology Review described some of the unanswered legal questions that could arise with the proposed rescue fork remedy:

> "A hard fork is kind of like creating parallel universes. […] If the judge in the Nano case were to order a hard fork, would people who refused to switch to the new chain be

[75] (Jimenez)
[76] (Jimenez)
[77] (Jimenez)
[78] (FABIAN v. NANO)

> violating the order? Would the court try to prevent cryptocurrency exchanges from listing the original coins? Could developers continue working on the original, unforked protocol?"[79].

The article also points out:

> "Unlike proprietary software code on a company server, public distributed ledgers aren't controlled by any one entity. Instead, they are hosted by multiple "nodes" in a network that can be distributed across the world. This raises new logistical questions, […] For example, how would a court impose such an order on people outside the US? "[80].

A court ordered rescue fork might seem like an extremely difficult solution in many cases, especially on a big public permissionless platform where it could be difficult to get over half of the nodes to comply with the court order. However, in the case of Nano Development, the solution may actually be a viable one.

According to the Class Action Complaint, "the Nano Core Team possesses more than 50 percent of the total voting power" and "in addition to the Nano Core Team, a total of nine other representatives comprise the ownership of over 96% of the total voting power"[81]. Since the Defendants in the case have a majority of the total voting power, theoretically, a court order that implements a rescue fork that returns the lost XRB would be easy. However, this case is a special exception and the same order could not easily be issued for large public permissionless blockchains.

In the Nano case, the voting power of the development team was so concentrated that they had effectively centralized its decentralized blockchain platform. The Nano blockchain is effectively an oligarchy, where only a few individuals have the power to make decisions that can change the blockchain. Therefore, if a rescue fork is not initiated the only people that benefit from the hack is the Nano Development team. Under this theory, the Nano Development team is not acting as a facilitator but a decision maker that is aiding in the criminal activity occurring on the platform. Nano may be in violation of CDA Section 230 under this theory, as they would be knowingly facilitating and assisting criminal activity.

There are many political and policy related questions that have been brought to light thanks to the Nano Development Class Action Complaint.

---

[79] (Orcutt)
[80] (Orcutt)
[81] (FABIAN v. NANO)

These questions demonstrate how difficult it will be to effectively legislate this technology.

CONCLUSION

My thesis studied the United States government's ability to hold criminals accountable for criminal activity that occurs on the blockchain platform. By examining the different types of crime that can occur on the blockchain and how those crimes can be remedied, we were better able to understand the problems facing the legal process by which the government can enforce the law. Investigating potential liability for users and node operators, as well as core developers, we were able to see that these issues are extremely complex and will require very meticulous problem solving and lawyering to resolve. Until these issues are resolved, Blockchain platforms will continue to be safe haven for crime.

REFERENCES

"Learn Cryptography - 51% Attack.". n.d. learncryptography.com/cryptocurrency/51-attack.

Beck, Roman, Christoph Müller-Bloch and John Leslie King. "Governance in the blockchain economy: A framework and research agenda." *Journal of the Association for Information Systems* 19 (2018): 1020-1034.

Canellis, David. "Here's how criminals use Bitcoin to launder dirty money." 26 November 2018. *Hard Fork | The Next Web.* thenextweb.com/hardfork/2018/11/26/bitcoin-money-laundering-2.

del Castillo, Michael. "Ethereum executes blockchain hard fork to return dao funds." 20 July 2016. *CoinDesk.* https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds.

Electronic Frontier Foundation. *Section 230 of the Communications Decency Act*. n.d. www.eff.org/issues/cda230.

FABIAN v. NANO. No. 3:19-cv-00054. UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA. 3 January 2019. Class Action Complaint.

Frakenfield, Jake. *Hard Fork - Investopedia*. 6 February 2019.

Greenspan, Gideon. "The Blockchain Immutability Myth." 4 May 2017. *MultiChain.* https://www.multichain.com/blog/2017/05/blockchain-immutability-myth/.

Hu, Jeff. "Learn Blockchain's Top 25 Hacks in History." 7 February 2019. *Hackernoon.* http://www.hackernoon.com/tech-explained-top-24-blockchain-hacks-in-history-first-half-40c390dc4a96.

Jaikaran, Chris. *Blockchain: Background and Policy Issues*. 28 February 2018. Congressional Research Service Report.

Jenkinson, Gareth. "Child Abuse Content on Bitcoin Blockchain: Can Node Operators Be Prosecuted?" 22 March 2018. *Cointelegraph.* www.cointelegraph.com/news/child-abuse-content-on-bitcoin-blockchain-can-node-operators-be-prosecuted.

Jimenez, Decrypt /. Guillermo. "Nano cryptocurrency seeks dismissal of $170 million “rescue fork” lawsuit." 9 April 2019. *Decrypt Media.* decryptmedia.com/6396/nano-cryptocurrency-seeks-dismissal-170-million-rescue-fork-lawsuit.

Lumb, R., D. Treat and O. Jelf. "EDITING THE UNEDITABLE BLOCKCHAIN--Why distributed ledger technology must adapt to an imperfect world." *URL https://newsroom. accenture. com/content/1101/files/Cross-FSBC. pdf [last accesssed: Oct. 2017]* (2016).

Manchester, Julia. "Backpage.com pleads guilty to human trafficking." 12 April 2018. *The Hill.* https://www.thehill.com/policy/technology/382962-backpagecom-pleads-guilty-to-human-trafficking.

Mattzutt, Roman et al. "POSTER: I Don’t Want That Content! On the Risks of Exploiting Bitcoin’s Blockchain as a Content Store." *ACM SIGSAC Conference on Computer and Communications Security*. Vienna, 2016.

Matzutt, Roman, et al. "A quantitative analysis of the impact of arbitrary blockchain content on bitcoin." *Proceedings of the 22nd International Conference on Financial Cryptography and Data Security*. Springer, 2018. blockchain.comsys.rwth-aachen.de.

—. "Thwarting Unwanted Blockchain Content Insertion." *IEEE International Conference on Cloud Engineering (IC2E)*. Ed. IEEE. 2018.

McReynolds, Emily, et al. "Cryptographic currencies from a tech-policy perspective: Policy issues and technical directions." *International Conference on Financial Cryptography and Data Security*. Berlin: Springer, 2015.

Orcutt, Mike. "Fork this: What an unprecedented court battle says about the future of cryptocurrency." 19 April 2018. *MIT Technology Review.*

Rooney, Kate. "$1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do." 7 June 2018. *CNBC.* www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html.

Sommerlad, Joe. "Bitcoin: Child sexual abuse images found embedded within cryptocurrency's blockchain ." 21 March 2018. *Independent.* http://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-price-latest-child-sexual-abuse-images-blockchain-illegal-transactions-research-a8266226.html.

"What is Hard Fork." n.d. *Cointelegraph.* www.cointelegraph.com/bitcoin-cash-for-beginners/what-is-hard-fork#what-is-a-soft-fork.