HOW WE HANDLE CRYPTOCURRENCY FORKS ON A SERVER

CAN WE MAKE CRYPTOCURRENCY SAFER WITHOUT HURTING IT?

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
David Gray

November 1, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: David Gr   Date: 10/26/2021

ADVISORS

Catherine Baritaud, Department of Engineering and Society

Daniel G. Graham, Rosanne Vrugtman, Department of Computer Science

Over the last year, cryptocurrency has become a household topic, as Perkins (2020), a cryptocurrency policy expert in association with the United States Congress, notes due to recent news about the various currencies, including Bitcoin, Ethereum, and Litecoin, rising and dropping in price drastically, as well as more widespread usage of it (p. 9). According to Simmons (2021), a law doctoral candidate focusing on cryptocurrency regulation, "Cryptocurrency is a digital or virtual currency that uses cryptographical functionality to conduct financial transactions and leverages blockchain technology to achieve a trustless, decentralized, and immutable ledger of account" (p. 87). This power of a cryptocurrency to be a currency without any central backing, which has historically fallen on a government, makes this a different approach to how we can view money. Eyal (2017), an associated director of Cornell University's Initiative for Crypto-Currencies and Contracts, states that cryptocurrencies, such as Bitcoin, rely on the longest chain rule, meaning that if there exists a branch split on the blockchain, choose the branch containing more blocks, and stick with that branch (2017). This process was chosen

The proposed technical paper and loosely coupled STS research will address both the volitivity of the cryptocurrency market as well as the way branch splits work in regard to a server. The objective of the technical report is to propose the synthesis of ideas of cryptocurrency and server-side processing. The synthesis would come together in order to enable a discussion on the topic of cryptocurrency blockchain splits and how a server holding a ledger would either resolve the conflicting information or cause a perm anent split in the cryptocurrency. This synthesis of ideas also brings into question on what can be done about the issues surrounding the blockchain. Kamidoi (2021), a researcher at Hiroshima City University on secure computing protocols, argues there are known issues with cryptocurrency, such as double spending attacks, majority occupation attacks, and use on the darknet (p. 24391). These issues can sometimes be solved by changing the technology; however, areas concerning usage of the currency primarily fall on the government in order to prevent illicit use. The coupled STS research project will serve to explore how certain regulation on cryptocurrency would either enable safer and more reliable transactions on the blockchain, or burden the currency to the point where it cannot be effectively used. The work of the technical and STS work will be accomplished during the Fall 2021 and Spring 2022 semesters, which will equate to a total of 28 weeks, as illustrated by the Gantt Chart in Figure 1.

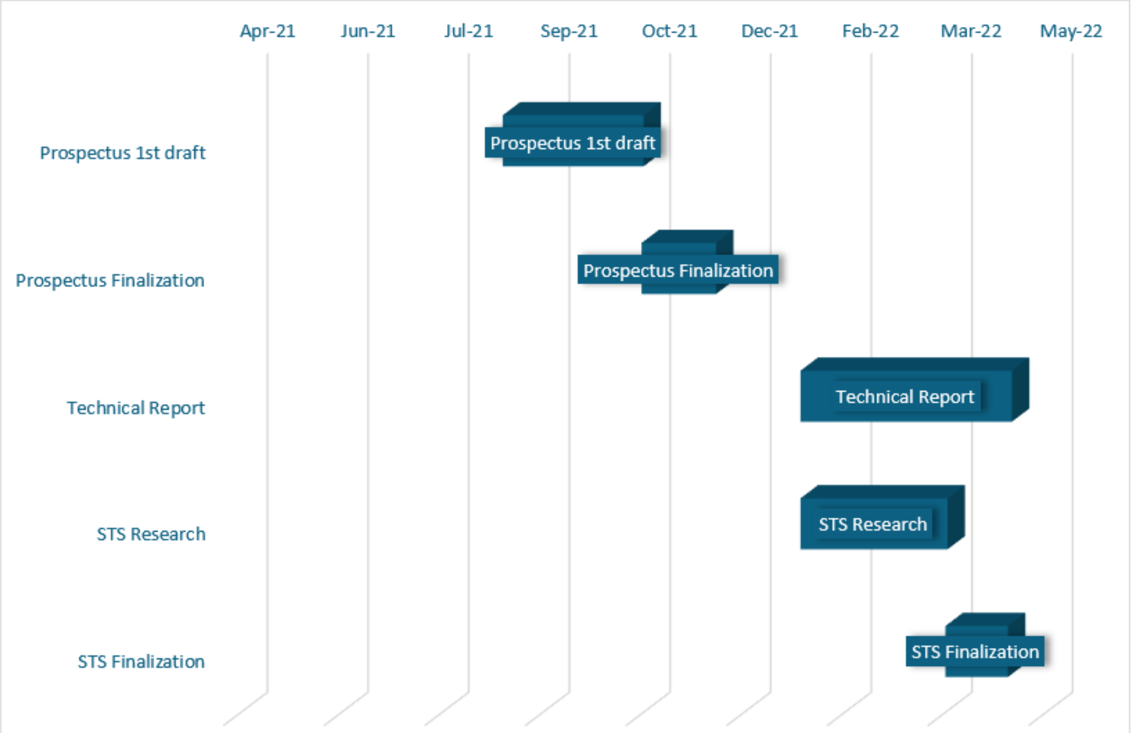

Figure 1 Gantt Chart:
This shows a timeline of the thesis project for David Gray (Gray, 2021)

HOW WE HANDLE CRYPTOCURRENCY FORKS ON A SERVER

With cryptocurrency and its lack of a central structure, there are going to be differences in work and the blockchain has a minor split, causing a disagreement between the mining community of a certain cryptocurrency. According to Fralix (2020) a professor at Clemson University that researches Bitcoin:

> Each miner in the system has its own version of the blockchain, so it is possible for there to exist short intervals of time where the blockchain versions of miners disagree due to propagation delay, which corresponds to the amount of time it takes a miner to communicate the existence of new blocks to other miners in the system, as well as the amount of time it takes the other miners to verify and accept the new block into their respective versions of the blockchain (p.1).

These splits, coupled with the hard forks in cryptocurrency, cause a question on how the ledger gets updated. If there is a difference in the cryptocurrency blockchain, the server that contains the ledger for that particular cryptocurrency needs to be updated with one of the branches.

The technical report, proposes a synthesis of ideas from both the cryptocurrency discussion in Introduction to Cybersecurity, CS 3710, and the Server-side processing discussion from Programming Languages for Web Development, CS 4640. With cryptocurrency having such a major impact in the computer science community, it would be a worthwhile discussion to include on how the currency determines which of the blocks is the correct one versus which is incorrect.

Forks and splits happen for a variety of reasons within cryptocurrencies, including variations in the work done mining the currency. Another reason for a split would be a fundamental difference in how parts of the cryptocurrency mining community view future blocks should be mined. According to Najmul Islam, a researcher of blockchain technology at LUT University, the split between Bitcoin and Bitcoin Cash occurred as a result of an argument between whether or not to increase the block size. Another split the author mentions is the split between Ethereum and Ethereum Classic, which was caused by the former being hacked and causing a major division in the community (2019, p.1).

As seen in Figure 2, there are a significant number of forks in Bitcoin that are hard forks. In a proposed synthesis of these topics, these forks would need to be separated from the soft splits. This is due to how these forks could be dealt with by starting their own ledgers and treating them as their own cryptocurrency. These hard forks as well as the soft splits mentioned earlier, caused by disagreements on proof of work, need to be dealt with on the server containing the ledger, thus making a decision on which cryptocurrency path to go down and adding that chain to the blockchain.

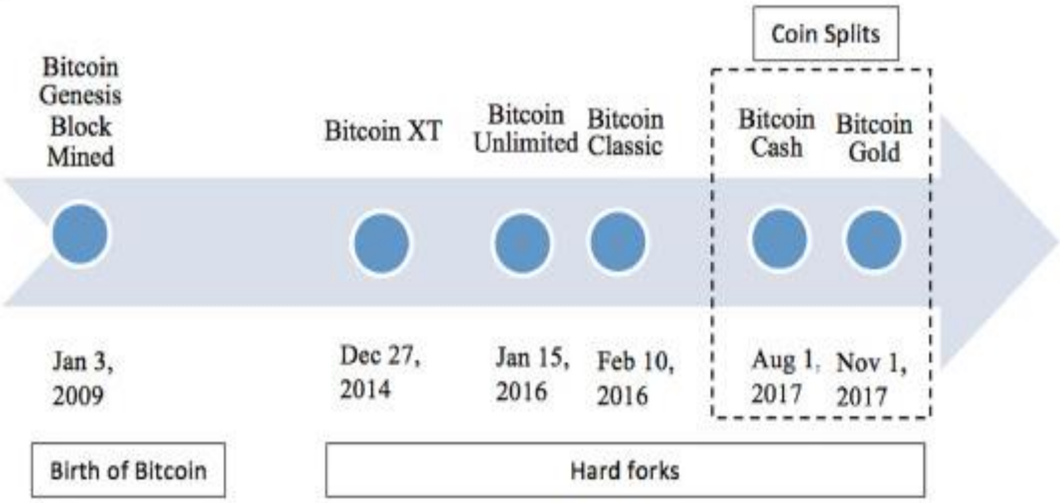

Figure 2 Bitcoin splits
This shows the amount of "Hard Forks" in bitcoin since genesis (Islam, 2019)

Overall, the purpose of this proposed combination of topics would be to reinforce the idea of server-side processing using the cryptocurrency blockchain as a medium. The synthesis of the topics of cryptocurrency and server side processing would allow the server-side processing concept to be coupled with the cryptocurrency blockchain, as well as expanding the topic of cryptocurrency in the Introduction to Cybersecurity class to include a discussion on how the blockchain will handle these splits and forks, and be able to choose the correct block to add onto the blockchain.

CAN WE MAKE CRYPTOCURRENCY SAFER WITHOUT HURTING IT?

Simmons (2021), a law doctoral candidate focusing on cryptocurrency regulation, explains “Cryptocurrency is a digital or virtual currency that uses cryptographical functionality to conduct financial transactions and leverages blockchain technology to achieve a trustless, decentralized, and immutable ledger of account” (p. 87). Cryptocurrency is a relatively new technology, and coupled with the monetary value associated with this technology, the media reports regularly on a variety of topics related to it: how it is a new currency with limited regulation, how the price is all over the place for certain coins, and how cryptocurrency is a tool in large scale criminal activity. Kamidoi (2021), a researcher at Hiroshima City University on secure computing protocols, comments use on the darknet marketplace, where users of cryptocurrencies are purchasing illicit materials (p. 24392). The media attention gives rise to the question of what we can do to slow or stop the illegal activity without significantly reducing the effectiveness of the currency. In order to truly tackle the issues of a technology that needs regulation, examples need to be studied, such as what former securities and exchange commission (SEC) chairman Jay Clayton and former undersecretary to the treasury Brent McIntosh (2021) suggest in regulating the cryptocurrencies like the United States has regulated bearer bonds.

Hacker (2019), a researcher at the European University Institute specializing in big data and securities regulation, including blockchain regulation, makes the argument cryptocurrency is designed to be a currency, it makes logical sense to regulate them as such. However, there are key differences that make this difficult to regulate it exactly the same as the dollar or the euro (p. 99). In this paper, a few commonly used regulations will be analyzed to determine whether or not certain regulations are effectively stabilizing the price and at least slowing the usage of cryptocurrency for criminal activity while keeping the usefulness of the currency, or if the regulations would end up doing more harm than good. The dangers associated with cryptocurrency, some of which are outlined by Perkins (2020), a cryptocurrency policy expert in association with the United States Congress, will be taken into consideration as well, as to find a balance between an unregulated, dangerous, and useful technology against an overly regulated safe but useless technology (p. 15-22). It will also be important to analyze cryptocurrency regulations in select countries so these case studies can see how various degrees of regulation affect different countries. Some examples of regulations, gathered from the Law Library of Congress (2018), include Switzerland where cryptocurrency is fully accepted, versus countries like Iraq where they have explicitly banned usage. Noted in Figure 3, the price of cryptocurrencies between 2015 and 2020 have fluctuated significantly, as can be seen by the pattern of spikes and crashes of the price of three unrelated cryptocurrencies. This uncertainty of the price of all

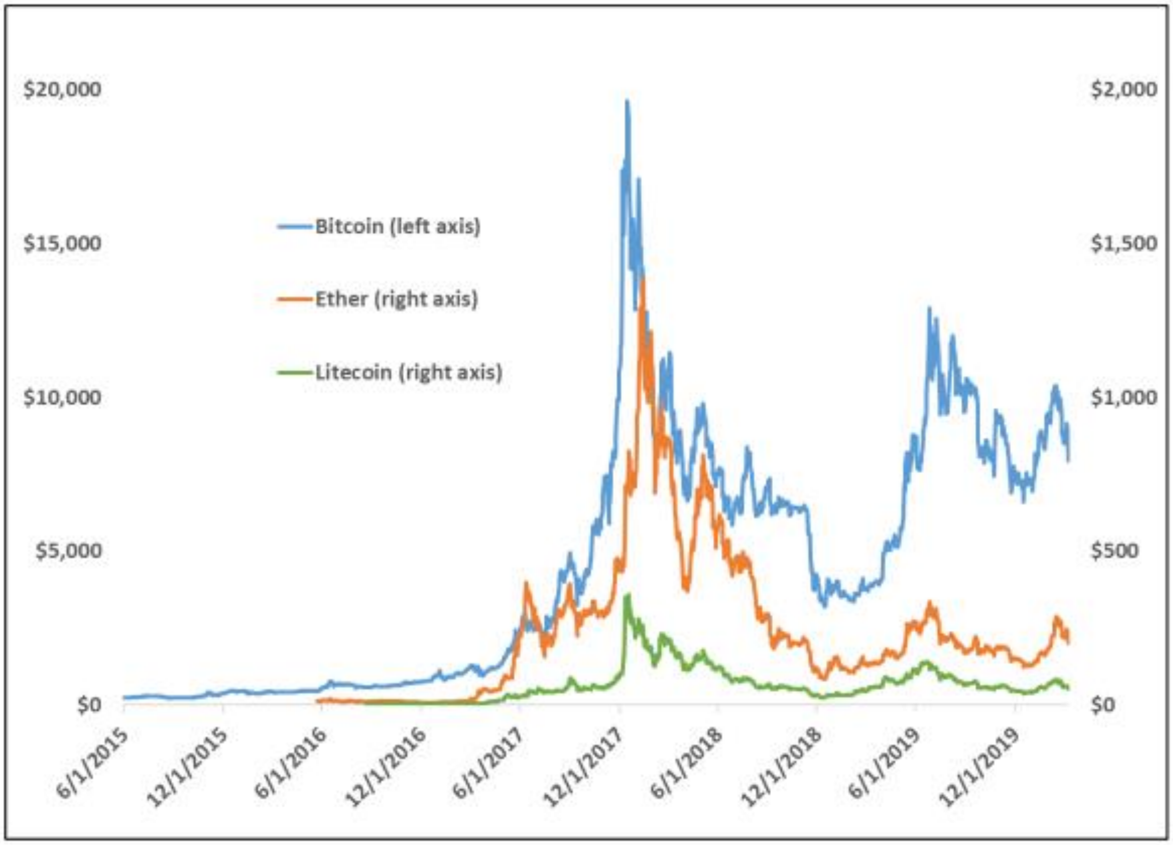

Figure 3: The price of Bitcoin, Ethereum, and Litecoin between June 1st 2015 and January 1st 2020 (Perkins page 9)

cryptocurrencies is a major reason to regulate these currencies sooner rather than later, in order to stabilize the market and make it so cryptocurrency investing is not as much of a gamble.

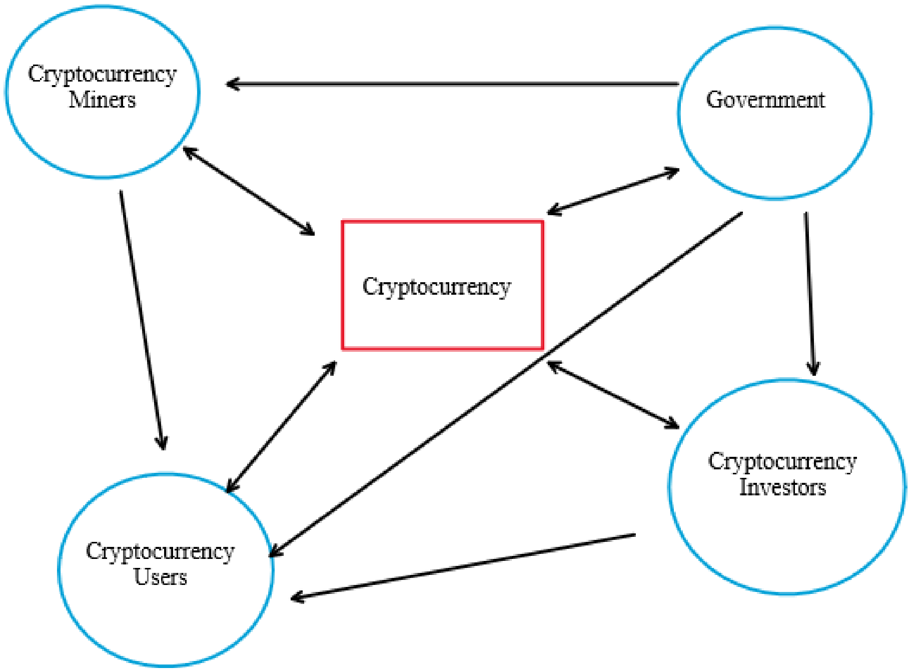

Figure 4: Cryptocurrency ANT model. This shows all the relationships between cryptocurrency, the government, users, miners, and investors (Gray, 2021)

To determine the success or failure of the regulations, the major parties involved with the intended use of cryptocurrency will be analyzed in regards to how the regulations benefitted or harmed their usage of cryptocurrency. For this research, Actor Network Theory, a theory pioneered by Michael Callon and John Law to analyze how various groups interact in a network, will be used (Law & Callon, 1988). The actor network model that will be used, pictured in Figure 4 encompasses all actors, including the government, cryptocurrency miners, and the users. In this model, we see that the currency influences every other actor, and every other actor influences different aspects of it. The government has significant influence over the other actors as well, since if there is regulation, the investors, the miners, and the users can all be affected, depending on which actors the regulations target. Due to this ability to regulate users, miners, and investors, as well as the ability to enforce this, the government has the influence it needs to be able to regulate users where it needs to.

TECHNOLOGY FIXES OR GOVERNMENT REGULATION

While complete government oversight could solve some issues plaguing cryptocurrency right now, the very nature of the technology prohibits this. The Institute of Electrical and Electronics Engineers (IEEE, 2020), a group of engineers who set industry standards for technology, has defined a process for cryptographic payments to include a process for anti-money laundering imbedded in the technology (p. 10). Adding the government to the verification of these payments in an oversight role would significantly hinder the ability of the technology to quickly allow payment between a merchant and customer. The very nature of cryptocurrency also, according to Simmons, a law doctoral candidate focusing on cryptocurrency regulation, is for the technology to remain decentralized, and therefore, the government or any body cannot have a direct control over every aspect (2021). It is important to note there exist aspects the government cannot control, and in those instances, the solution needs to come from a technological footing, not a regulatory one. For instance, resolving splits in a blockchain has the longest chain rule, and resolving hard forks in the blockchain requires server-side changes. It is up to the government, when making any regulation, to analyze the situation, determine which regulations are necessary to only hinder the illicit usage of cryptocurrency without hindering the legitimate usage, and which solutions are feasible on the government's side. This is once again comparable to regulation of bearer bonds, which allowed corporate bonds to continue, but stopped the usage of bonds for illegal activity, as noted by former SEC chairman Jay Clayton and former undersecretary to the treasury Brent McIntosh (2021).

Noted by Haynes, "Owing to [cryptocurrency's] decentralized nature they evade traditional forms of state regulation, lack a provider or issuer that could be held accountable, or a central database," (2020, p. 249). With this in mind, the regulations that do fill in the gaps can only be placed onto the users of the technology. As pointed out by Clayton, regulating cryptocurrency the same way as bearer bonds had been regulated would be a good start to get in the right mindset (2021, paragraph 7). In order to regulate cryptocurrency, the government would need to regulate the users of the technology, rather than attempting to regulate a technology that is resistant to traditional regulation.

This research project will be in the form of a scholarly article outlining the ways the government can effectively regulate cryptocurrency without ruining the purpose that cryptocurrency serves. It will analyze how certain cryptocurrency regulations have faired in practice, in select countries such as Switzerland and Iraq, where as outlined by the Law Library of Congress (2018), they have implemented opposing regulations of making Switzerland a cryptocurrency haven and Iraq banning cryptocurrency. Using these case studies, the research will hopefully determine whether or not those regulations could be applied to the US government.

REFERENCES

Clayton, J., & McIntosh, B. (2021, June 6). Crypto Needs Regulation, but It Doesn't Need New Rules. *Wall Street Journal*. https://www.wsj.com/articles/crypto-needs-regulation-but-it-doesnt-need-new-rules-11623007528

Eyal, I. (2017, January 1). *Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities*. Computer, 50(9), 38 - 49.

Fralix, B. (2020, June 1). *On classes of Bitcoin-inspired infinite-server queueing systems.* Queueing Systems, 95(1/2), 29 - 52.

Gray, David (2021). Cryptocurrency ANT Model. *Prospectus.* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Gray, David (2021). Gantt chart UVA Computer Science capstone. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Hacker, P., Lianos, I., Dimitropoulos, G., Eich, S., & Oxford Scholarship Online - VIVA (2019). Regulating Blockchain: Techno-social and Legal Challenges. Oxford, United Kingdom: *Oxford University Press*.

Haynes, A., & Yeoh, P. (2020). Cryptocurrencies and Cryptoassets: Regulatory and Legal Issues. Abingdon, Oxon*: Informa Law from Routledge*.

IEEE Electronic Library (IEL) Standards (2020). *2143.1-2020 - IEEE Standard for General Process of Cryptocurrency Payment*. S.l.: IEEE, 9-12.

Islam, A.K.M. N., Mäntymäki, M., & Turunen, M. (2019, November 1). Why do blockchains split? An actor-network perspective on Bitcoin splits. *Technological Forecasting & Social Change*, 148.

Kamidoi, Y., Yamauchi, R., & Wakabayashi, S. (2021, January 1). A Protocol for Preventing Transaction Commitment Without Recipient's Authorization on Blockchain and It's Implementation. *IEEE Access,* Access, IEEE, 9, 24390 - 24405.

Law, J., & Callon, M. (1988). Engineering and Sociology in a Military Aircraft Project: A Network Analysis of Technological Change. *Social Problems*, *35*(3), 284–297. https://doi.org/10.2307/800623

Law Library of Congress (U.S.) (issuing body) (2018). *Regulation of Cryptocurrency Around the World*. Washington, D.C.: The Law Library of Congress, Global Legal Research Center.

Perkins, David W. (Analyst in Macroeconomic Policy), & Library of Congress (2020). *Cryptocurrency: The Economics of Money and Selected Policy Issues* (Library of Congress public ed.). Washington, D.C.: Congressional Research Service.

Simmons, A. (2021, January 1). *Regulating Libra: Will Legal and Regulatory Uncertainty Prevent the Launch of Facebook's Cryptocurrency Project*?. Journal of Business and Technology Law, 16(1), 83 - 118.