Secured Card: Using Frontend to Increase Business and Improve User Satisfaction

Managing Cryptocurrency's Impact in Darknet Marketplaces

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
Eric Kharitonashvili

Spring 2022

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.

ADVISORS

Kent Wayland, Department of Engineering and Society

Daniel Graham, Department of Computer Science

General Research

Problem

How will cryptocurrency develop and be used by governments, people, and companies when taking into account its previous use in illegal marketplaces?

Illegal transactions are supposed to take place in alleyways, park benches, and even public malls. However, the rise of darknet marketplaces has added a new venue to this game – anonymous online transactions. Using decentralized currencies, the players in this new age cybercrime world are recognized by their usernames and 35-character wallet addresses. These darknet markets have been transacting over a billion dollars of illegal merchandise per year (ElBahrawy, A., Alessandretti, L., Rusnac, L. *et al.*, 2020, n.p.) Between 2011 and 2013, one of the first and most infamous darknet marketplaces, the silk road, transacted a total of 9.5 million bitcoin (United States of America v. Ross William Ulbricht page 6). When the site closed, the total aggregate amount of Bitcoin transacted was 24.5 million. This accounts for over 1/3 of all Bitcoin transactions, legal and illegal, at the time. Given that crypto is being accepted as payment by legal stores at an ever-growing rate, the percentage of illegal transactions as compared to total transactions is decreasing. However, analyzing the roots of crypto currencies' beginnings as a currency and how strongly this is tied to darknet marketplaces can yield insights into how society affected this technology's emergence as a multi-trillion-dollar market and how society will continue to affect the overall use of this technology.

As society adopts cryptocurrencies, a lot of different blockchains will be used, and coins will have to be able to transfer from one to another. What is the difference between a blockchain and a coin? A blockchain describes the protocols of the network and is made up of computers doing computational work by executing the instructions for these protocols. Coins are what the workers get paid and rewarded with when they execute these instructions. Ethereum is the blockchain and ETH is the coin (although they are commonly used interchangeably). With many different coins and blockchains serving different purposes, it is important to be able to have these coins interact. If an NFT is minted (created) on the Ethereum blockchain, there should be an easy way to buy it with Bitcoin if cryptocurrency and decentralized goods are to be exchanged efficiently. My technical project will focus on bridging this gap.

Developing a
Cryptocurrency Bridge

With a world having growing uses of cryptocurrency, how will these coins interact with each other?

Online transactions as an American are generally convenient and minimal in fees. Overseas, however, currency exchanges need to take place, international tax laws need to be followed, and while systems for these regulations may already be in place, country-to-country trust is required to keep these regulations in check. This system could benefit much from decentralization and blockchain technology.

In the future, it could very well be possible that each country has its own cryptocurrency for its online transactions. This could automate the taxation process, give the governments accurate data on company purchases, and allow a currency native to the internet that is linked to the fiat currency that they have. Being able to convert euros to dollars, dollars to yen, and more in a decentralized application can automate much of the oversea internet transaction problems. But how would a system like this work?

Current systems that swap coins are called cryptocurrency bridges. In general, there are two kinds – centralized and decentralized. The centralized systems work similarly to the current currency swapping system. Trust is required in the person or entity doing the swapping. The way decentralized systems work is with smart contracts.

Smart contracts are code that runs in a blockchain. Concretely, if Harry promised Bill he would pay him 1 Eth on Christmas in 2023, Harry or Bill could code a smart contract that will automatically transfer an Ethereum coin to Bill's wallet on Christmas 2023. This code will be coded in the Ethereum blockchain and the transaction will be guaranteed to happen. My technical project will be a crypto bridge decentralized application that uses these smart contracts in the background to make the project possible.

The way decentralized crypto bridges work is by freezing and deploying copy coins in another blockchain (Peter Robinson, 2021, n.p.) Generally, these work as a one-to-one exchange. A Bitcoin holder may want to spend his Bitcoin to buy something on the Ethereum blockchain (like an NFT for example.) To do this, a decentralized crypto bridge would create a “token” of Bitcoin in the Ethereum blockchain. A token is just a representation of another coin in a separate blockchain. The decentralized crypto bridge would freeze the original and real Bitcoin in a hidden wallet – thus ensuring that the newly created token is backed one-to-one with the original coin. In other words, decentralized bridges exchange coins from one blockchain to another. They do this by freezing the original asset and creating a representation of this asset called a “token” in another blockchain.

My technical project will focus on building a decentralized crypto bridge focusing on Bitcoin to Ethereum token transactions. To do this, I will research and implement a Bitcoin wallet creation and freezing algorithm and build a system of Ethereum smart contracts that create tokens equivalent to the amount of Bitcoin in the frozen wallet. Then I would need to code a protocol to transfer this asset into the user's Ethereum wallet. This will provide a documented and open-source framework for other cryptocurrencies to adopt when dealing with coin swapping from one blockchain to another.

Relationship Between Cryptocurrencies and Darknet Marketplaces

How have and will darknet marketplaces affected and continue to affect the development of crypto and blockchain technologies?

The terms "dark web" and "deep web" are often incorrectly used interchangeably. The deep web refers to all parts of the internet. This includes all .com sites, .net sites, and private connections like routers in the home. The dark web refers to the part of the deep web that is anonymous through encryption. Normally, users surfing the web can be easily tracked by the government. However, dark web protocols allow for user anonymity while browsing online. The most popular protocol, Onion Routing, was invented by the US Navy as a way to not allow foreign governments to track ship-to-ship messages sent over the internet (US Naval Research Academy.) Nearly all darknet marketplaces use this protocol to create websites where online purchases cannot be tracked and vendors cannot be found. This level of anonymity is why drugs, fraud, and guns can be found in these markets. However, for a long time, darknet marketplaces could host their site without being tracked, but purchases could be traced back to users. This changed with the advent of Bitcoin and cryptocurrency.

Currency, even more so than technology, relies on trust. When Bitcoin was first created, the cryptocurrency had no place to be transacted online except in user-to-user transactions in the Bitcoin forum. People liked and trusted the anonymous nature of Bitcoin. Online money, be it

PayPal or credit cards, is inherently linked to personal identification. Bitcoin is not. A wallet can be created and Bitcoin spent without linking anything to one's real name, location, or personal information. Because of this, Darknet markets are oftentimes seen as the catalyst of cryptocurrency, as they were the first large adopters of Bitcoin as payment (ElBahrawy, *et al,* 2020, n.p.) Without these markets, it may have taken much longer for the crypto snowball to gain steam. However, being so heavily connected to illegal markets has left an imprint on cryptocurrency as a whole to this day. The most prominent effects of crypto being linked to these marketplaces can be split into three categories: legal, technical, and public opinion.

Legally, the darknet marketplaces have increased government control on cryptocurrencies, forcing large crypto exchanges like Coinbase and Gemini to begin associating crypto wallet addresses with real-life identities. This has resulted in less tax evasion and made it harder to anonymously purchase illegal items like drugs or guns online – as payments can be tracked back to identities. Governments have also begun adopting cryptocurrency for their own use. An example of this is El Salvador making Bitcoin its "official currency" (Arslanian, et al. 2021, p.3) However, governments like China are also currently working on their digital currency. Having money like this on the blockchain could allow governments to have greater oversite, control, and data on their money. In fighting darknet activities, governments have begun changing laws regarding the privacy of cryptocurrency. This in turn has caused a change in how darknet markets work and how people transact with them, which may cause another round of government intervention thus restarting the cycle. Analyzing this cyclic pattern and researching laws that have affected darknet marketplaces as well as how people have reacted to these changes may be a way to gain insight into how darknet markets and cryptocurrency evolved together. Looking into the future, as cryptocurrency grows, this may act as a precedent for how legal stores will adopt and use cryptocurrency as well.

In response to these laws, technology has progressed to keep criminals hidden. Ways to launder Bitcoin online were developed. One such method is called a “Mixer.” These collect a percentage fee of the coin meant to be “mixed” and rapidly transact “clean” and “dirty” money with different wallets in order to anonymize where the coin came from, i.e., the government can’t tell if the coin was sent to an illegal vendor. New coins have developed with more privacy in mind as well. Monero and Dash are examples of coins that have used a different method of proof in their blockchains in order to make their transactions completely anonymous and untraceable (Saberhagen, 2013, n.p.) The advent of new coins and technology viable for darknet marketplaces impact domains other than just illegal transactions. Controlling governments like China and North Korea may struggle to find ways to track these coins – giving their people more control and privacy. Companies reliant on consumer data may also begin to lose profits if legal stores begin accepting these private coins. Creating a more private society in this internet age is not a new idea, the widely used term for this is called Web 3.0. Ever since the internet came around, people have been giving up more and more privacy to companies and governments. However, developments in coins that protect data and give back control of that data to users may cause societal shifts. If keeping user data becomes a viable option, how will that impact the landscape of the internet? Will the surface web become more like the dark web? Investigating darknet technologies that allow for data to be privatized like P2P encryption for messaging or Tor net relays for hosting the onion routing protocol and comparing those to current internet technologies for the same things may give insight into how the future of the internet, if a Web 3.0 architecture comes to fruition, will look and how people on that internet will interact.

As stated earlier, the basis of currency is trust. Russia’s currency, the Ruble, nearly halved in value when Russia started war in Ukraine. This is because people lost trust in the government backing the Ruble. Cryptocurrency, just like any other currency, relies on trust for its value to be determined. Given most cryptocurrency is not backed by a government or small group of people, where does this trust come from? A technology purist may argue that the trust is in the technological system and protocols of the coin. However, that is not the whole story. Many people who buy and sell cryptocurrency know very little about the technology. It seems like trust in this domain is built on a variety of factors, a major one being public opinion and sway. This can be seen when Elon Musk, one of the most popular public figures that supported Dogecoin, debuted on SNL and the price of Doge dropped by almost 30% (Sigalos, 2021, n.p.) Being historically tied to the darknet, how has this affected the public’s opinion of Bitcoin and cryptocurrency as a whole? As cryptocurrency begins to be adopted in more legal stores, will people still remember or care about crypto’s illegal history? To analyze these questions about how society views cryptocurrency, scraping online forums like Twitter or Reddit with proven machine learning models involving sentiment analysis (models that assess how positive written statements are) may be an answer. However, online forums are inherently biased as a data source. Many countries do not have internet, and many people do not use Twitter or Reddit. Demographically these people tend to be younger and more adept at technology. This could skew the results when applied to a broader population in a multitude of ways both positively and negatively. Analyzing other forms of media like print news for older audiences or asking older demographics their opinions on cryptocurrency with surveys and weighting their responses alongside web scraping may be a way to course-correct.

Conclusion

How intimate is the relationship between crypto and darknet markets? The growth of cryptocurrency relied heavily on darknet markets as this was the first widespread use of decentralized currency to buy goods. As these darknet markets grew, so did the value and trust of cryptocurrency as a whole. People saw the currency working and put more faith and trust in it. More and more, technological development of this technology grew as the market grew larger. Eventually, cryptocurrency started being used outside of these markets, thus the darknet markets contribute less to the total percent of cryptocurrency transacted, however, its influence continues to leave marks on the technology as it develops.

The research on the origins of cryptocurrency, as well as working on cryptocurrency use in a multitude of blockchains could play a part in predicting the future development of the technology and the socio-technological network in which people will participate. Analyzing the pivotal relationship between where crypto was originally used and where crypto might go gains insight as to why people were attracted to this technology in the first place as well as how people may use it in the future.

References

"Sealed Complaint 13 MAG 2328: United States of America v. Ross William Ulbricht", 2014, https://www.justice.gov/usao-sdny/press-release/file/1278151.

Robinson, P. (2021). Survey of crosschain communications protocols. *Computer Networks*, 200. https://doi.org/10.1016/j.comnet.2021.108488

Saberhagen, Nicolas, V. (2013). CryptoNote v 2.0

Department for Business Innovation and Skills. (2016, May). Success as a knowledge economy: Teaching excellence, social mobility and student choice [White Paper]. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/523396/bis-16-265-success-as-a-knowledge-economy.pdf

"Home." *NRL*, US Naval Research Laboratory, https://www.nrl.navy.mil/itd/chacs/

ElBahrawy, A., Alessandretti, L., Rusnac, L. *et al.* Collective dynamics of dark web marketplaces. *Sci Rep* **10,** 18827 (2020). https://doi.org/10.1038/s41598-020-74416-y

Arslanian, Henri, et al. *El Salvador's Law: A Meaningful Test for Bitcoin*. (2021) https://www.pwc.com/gx/en/financial-services/pdf/el-salvadors-law-a-meaningful-test-for-bitcoin.pdf.

Sigalos, MacKenzie. "Dogecoin Plunges Nearly 30% during Elon Musk's SNL Appearance." *CNBC*, CNBC, 16 Oct. 2021, https://www.cnbc.com/2021/05/08/dogecoin-price-plummets-as-elon-musk-hosts-saturday-night-live-.html.

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering

Eric Kharitonashvili

Spring 2022

Technical Project Team Members
Eric Kharitonashvili

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

Signature Eric Kharitonashvili

Approved Daniel Graham, Department of Computer Science

Approved Kent Wayland, Department of Engineering and Society