INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 4

2020

Changing Pattern of Criminal Economy: Use of Cryptocurrencies in Darknet and Criminal Forums

RIDDHI PRATIM DUTTA[1]

ABSTRACT

Cryptocurrencies are a new phenomenon as compared to fiat currencies which have thousands of years old history. Satoshi Nakamoto, a programmer or a group of programmers created the cryptocurrency bitcoin to escape the current trust-based system where we put our trust on central banks to manage economy. Instead a new system – where mathematics and cryptography take position of trust was envisaged. Bitcoin changed the world as more and more people started to get attracted by the idea of currency which is beyond manipulation by governments and financial institutions. But a currency which lies beyond regulation by central banks can also attract criminals who will use them for nefarious purposes. Bitcoin saw huge interest from criminals due to pseudo anonymity inherent in bitcoin. So, from the beginning cryptocurrencies saw growing interest by criminals and money launderers.

This paper traces the origin of bitcoin and how criminal activities interreacted with cryptocurrencies from the beginning. The paper begins by giving the philosophy behind bitcoin and tracing starting of cryptocurrencies. The we discuss what are the causes which makes cryptocurrencies instantly attractive for criminals. We next trace the growth of silk road, an online underground market place and how cryptocurrencies contributed to its growth. We end up discussing future trends and whether banning cryptocurrencies can be an option.

The Cryptocurrencies are rebellion against the current power structure. For that reason, crime will always be a part of that story. people who conceived the idea of virtual coins were aware of the rebellious nature of the beast and many of them foresaw that rise of virtual currencies will attract certain kind immoral individuals. Proponents of cryptocurrencies were ready to accept the cost since they saw surveillance of state as a bigger enemy.

Timothy C. May, an early advocate of the cryptocurrencies wrote," A specter is haunting the modern world, the specter of crypto anarchy. Computer technology is on the verge of providing

[1]Author is a Student at NUJS, Kolkata, India

 [ISSN 2581-5369]

the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation…The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures."[2]

I. EMERGENCE OF CRYPTOCURRENCIES

The group, Cypherpunks, who gave the idea of coins could not implement it in reality. That was possible by Satoshi Nakamoto. Satoshi, who was fed up with people putting their trust in human controlled Central banks wanted to change the system. He argued instead of putting trust on unpredictable people we are better off putting our trust on cryptographic principles. He not only solved "double spending problem"[3] but he added a reward for people who take part in his system. Miners are people who are spending their valuable computing power solving the mathematical problems and getting paid by Bitcoin. The opportunity to get rewarded attracted

[2] Timothy C. May, "*Crypto Anarchist Manifesto*", http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html. (last visited 25th August.,2019).

[3] The Double Spending problem refers to a complication by which a user can replicate any digital asset and send them to various receivers. While in case of general files it isn't a problem but when such files denote monetary value then keeping track of assets poses a problem.

 [ISSN 2581-5369]

a large group of people whose motivation ranged from monetary profit to payment for criminal acts.

For years crime depended on fiat currencies. Profits of crime or tax evasion was harder to conceal. In ancient China people used to send money outside to avoid paying tax to the king. In recent times, people in China are still sending their asset outside, only now they are converting it to cryptocurrencies. Money laundering, or concealing the ill-gotten asset from government was a perennial problem from criminals. Earlier the tactics was to mix the dirty money with legitimate money and move it across the borders in a complicated manner to make it harder to track. But for a determined law enforcement, tracking money was possible with time and effort. Using fiat currency carries too many problems. For example, notes are often marked, heavy and hard to send in distant places. Mechanisms like Hawala, are not everywhere and many Hawala places are not simply trustworthy. After World Trade Center attack USA government started to crack down on Hawala - making it an unstable means to transfer money. Even converting money to asset is a hard task since acquiring too many assets, whether movable or immovable, within a short span of time attracts attention of tax authorities. The answer to these problems started to appear with widespread usage of internet.

Criminals were first using digital currencies that are mainly used within games and that are convertible to fiat currencies. They were also using anonymous non-USA based payment processors. Payment processors like Liberty Reserve thrived in this era. Liberty Reserve which was a Costa Rica based digital currency service billed itself as a safest payment processor. The attraction of Liberty Reserve was it allowed transfer of money with only name, email address and birth date. Liberty Reserve accepted money from everybody and no verification or effort was made to authenticate identity of the users. Further employees were required to abide by confidentiality agreement. It quickly became default choice for many criminals along with few legitimate businesses. When FBI took down Liberty Reserve it caught Criminals off guard since many were maintaining account with Liberty Reserve and lost big amount of money. These money transfer businesses became popular because not only they offered anonymity but also low rate for cash transfer. Paying full blown money laundering services is really costly for criminals so when these services offered low rates people flocked to them without caring for the risk. When FBI took Liberty Reserve down, criminals became aware that centralized services run the risk of being shutdown at any time.

Appearance of cryptocurrencies solved a lot of these problems for criminals. Federal Bureau of Investigation, America's premier law enforcement agency, was well aware of the dangers posed by Bitcoin. FBI in their report, published in 2012 pointed out several aspects of Bitcoin

 [ISSN 2581-5369]

which makes it lucrative for criminals. They were tracking money laundering activities through e-gold, Webmoney and other virtual coins. The services were although virtual in nature but many of them were not anonymized correctly and were being operated from centralized location and was easier to track. But FBI pointed out Bitcoin is based on peer to peer protocol. Since it has no central architecture it is harder to track and take it down.

II. Reasons Behind The Use By Criminals

The anonymity offered by Bitcoin is lucrative for cyber criminals. The blockchain, where transactions are recorded, although open for public inspection but does not record personal information. Thus, it is hard to ascertain identities of payer and payee. The anonymity attracted criminals to the Bitcoin initially but we have to point out this anonymity provides a false sense of security. FBI ascertained although Bitcoin itself is anonymous, but when such coins are transferred to fiat currencies they can certainly be tracked. Many times it has been found out criminals used the same wallet address in darknets as well as in clearnet where they exposed their real life identities. Transactional information can be tracked by algorithms which can tell with reasonable certainty who did the transaction at what time.

Then, there are third party Bitcoin services who are beyond the jurisdiction of USA, who provides exchange services and other mechanisms designed to obfuscate the source of the fund. Bitcoin tumbler and anonymizers can make it extremely difficult to track coins. The people who are providing exchange between bitcoin and fiat currencies are not compliant to AML mechanism, thereby attracting interest of criminals.

FBI estimated that Bitcoin would be used primarily in these type of criminal activities,

A. Money laundering – Earlier Money was being laundered through game money, and virtual money. Launderers will shift and use Bitcoin since it protects better anonymity and transactions are easier to make. Large amount of money can be send across borders quickly and with very low transactional cost.

B. Terror Financing and other Criminal donations – Terrorist and their benefactors would be very much attracted to crypto currencies since tracking the coins are extremely difficult and identity of people who are donating can easily be hidden.

C. Payment for crime – Bitcoin will obviously be used as payment for goods and services which are illegal in nature. Payment for malwares, tools for cybercrimes can now be paid securely thanks to cryptocurrencies.

 [ISSN 2581-5369]

D. THEFT OF BITCOIN – As bitcoin started to gain value, hacking exchanges and wallets would be targeted by criminals. There were several hacks in exchanges which resulted loss of thousands of coins of customers. Contents of personal wallets, where coins are kept, were stolen by malwares. There will be significant rise in malwares stealing virtual coins.

E. FRAUDS & PONZI SCHEMES – What FBI did not foresee is prevalence of frauds and Ponzi schemes in the cryptocurrency sector. The huge return of Bitcoin and other virtual coins attracted a host of people who wanted to get rich quick without understanding the market. Bitcoin did provide extraordinary return for a few people before it crashed. But common people bought any kind of virtual coins they could get their hands on and pretty soon many of them turned worthless. Criminals advertised extraordinary return of Bitcoin and were able to raise money from the market exploiting people's greed.

The 2012 report by FBI saw their worst fears materialize in the form of darknet markets. Tor,a system designed by United States military for anonymous communication gave drug sellers and criminals a platform to communicate with their clients. It was only a matter of time someone would set up a shop in the darknet trying to market illegal goods. Emergence of Silk Road satisfied that prophecy.

III. SILK ROAD AND CONTRIBUTION OF BITCOIN

Silk Road was supposed to be a free market economic experiment. A place where a user can buy anything he wants, most of items being of illegal in nature. Its creator was an American guy, Ross Ulbricht, who believed that people should have the right to buy and sell whatever they wanted so long as they weren't hurting anybody else. While Ulbricht banned counterfeits, weapons and child porn, vendors selling there, quickly realized they can play fast and easy with the rules. But mostly Silk Road became famous as the underground website where people can purchase any drug they want.

Silk Road started to gain attention with the piece[4] on Gawker magazine, who described it as amazon of mind altering substances. It also came into notice of law enforcements who began investigations into it.

Silk Road was able to function and grow due to two key technologies. First is anonymous network Tor where it was hosted and second was using Bitcoin as a payment system. When silk road began, barely few people had heard the name of Bitcoin let alone using it. For law enforcements, it was a unique challenge, being confronted with a technology barely few years

[4] Adrian Chen, "*The Underground Website Where You Can Buy Any Drug Imaginable*", Gawker, https://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.

 [ISSN 2581-5369]

old. But Ross correctly identified potential of Bitcoin and latched onto it.

He wrote, unfortunately a little too hastily, "We've won States War on Drugs because of Bitcoin"[5].Silk Road adopted Bitcoin because it gave them a veil to hide. Unfortunately, Ross didn't realize Bitcoin is not as anonymous as it was thought to be. While it is true that personal identification of payer and payee is not tied to the coin, but the digital ledger is open to see and investigated by everybody. Real world identity of Bitcoin users although hard to trace at first but correlating other transactions done from the same addresses, police were able to find out identity of the users pretty accurately. Later, to counter the tracking of coins of Silk Road used services of the coin mixers/tumbling services which made following the trail of transactions extremely difficult.

With the help of Bitcoin Ross foresaw a monumental shift in the power structure of the world. Today, with the help of technologies like Bitcoin Ross argued people can, not only control flow of information but also flow of money.in his vision, state is being cut out of the equation one sector at a time and power will return to the people.

But to use Bitcoin as a day to day currency, Ross had to overcome a practical problem which has been plaguing Bitcoin since inception, its volatility. Silk road allowed the site's dealers to peg their Bitcoin prices to Dollar. Which means a user is paying Dollar value regardless of the prices in Bitcoin. And in the backend Silk Road offered a currency hedging system, which protected site dealers from fluctuation of Bitcoin's prices when goods were in transit.

Silk Road copied the business model of more popular legal websites such as Amazon and EBay , by using escrow services and verified digital payment system. It was a site that was trusted by its users who were mostly interested in drugs. FBI with other agencies spend a considerable time tracking the "dread Pirate Roberts", online identity of Ross and in the end few simple mistakes cost him his freedom. Ross Ulbricht is serving life sentences in prison with no hope of coming out anytime soon.

But Silk Road showed a future of possibilities which was soon followed by other copy cats. Silk Road at its peak were making millions in sales and its sales figure crossed billions of dollars. So, naturally seeing the success of Silk Road, other major drug dealing sites came into existence. Silk Road had to compete with rivals like Atlantis, a forum which started to advertise on YouTube. Atlantis, managed by an online identity Vladimir, started to encroach on Silk

[5] Andy Greenberg, "*Meet the Dread Pirate Roberts. The Man Behind Booming Black market Drug Website Silk Road",* (Sep. 2,2013), Forbes, https://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/#6690b5028b73.

 [ISSN 2581-5369]

Road's business. Even after FBI took down Silk Road, there were several version of Silk Road floating on Dark net.

In July,2017 various enforcement agencies working together took down one of the largest online market Alphabay. Going by the conservative estimate Alphabay alone had over 25000 listings of drugs. It had over 200,000 users and 40000 vendors. They not only sold drugd but toxic chemicals, counterfeiting identity services, hacking tools and malwares.

Today, online drug market forums are plenty and they are using the same business model of Silk Road with better operational security. And they are using not only Bitcoins but other virtual coins that offer better protection.

IV. FUTURE TRENDS - ZCASH AND MONERO

In Internet Organized Crime Threat Assessment report of 2017, Europol cautioned although Bitcoin is still most used currency in darknet, more secure currencies like Monero and Zcash, along with Ethereum is gaining foothold. These currencies are uniquely lucrative for criminals since they provide better privacy protection. They not only make the transacting parties anonymous but the transaction history also become anonymous. This privacy focused coins, by eliminating transaction history makes it virtually impossible to trace financial information. They achieve this feat by either mixing the transaction history data or eliminating it altogether. But since Monero has been longer in the market people certainly trust Monero better due to reliability.

In their Website Monero expands upon the philosophy behind the project. Monero developers take privacy very seriously as their goal is to protect Monero users in a court of law. Their goal is to make privacy accessible to all, regardless of knowledge level of users. A user should be confident enough to trust Monero and should not feel any need to change their spending habit. Monero Improved decentralization architecture of Bitcoin and made sure developmental decisions are open for public inspection. Since its inception Monero quickly became one of the biggest cryptocurrency of recent times.

Criminals are accepting Monero and ransoms are nowadays demanded to be paid in either Zcash or Monero. Already in a recent kidnapping in Norway, suspect was asking for payment in Monero. This trend will continue in foreseeable future. Most Darknet markets have added Monero as their payment option. While asked about the criminal use of their coins, Monero developers argued that their coin doesn't encourage crime but encourages commerce. We can see that presently these commercial activities happen to be of criminal nature.

 [ISSN 2581-5369]

A. USE OF SMART CONTRACTS IN CRIMINAL UNDERGROUND

It is anticipated that criminals would shift from traditional oral agreement to more privacy focused smart contracts. Smart contracts are digital applications which can fulfil the purpose of agreements - built on top of blockchain, these applications are able to execute itself on verification of certain prewritten conditions. Europol assumes if contract creator has the skill to create those applications, many criminal services would be dealt by these contracts.

These criminal smart contracts(CSC) are already shown to be theoretically possible and can be executed in practice. Juels et al[6] showed Criminal Smart Contract can facilitate leakage of confidential information, leakage of cryptographic keys and various real-world crimes like murder, arson etc.

Right now, implementing these types of smart contracts are tricky as the existing smart contract architecture like Ethereum blockchain are not capable enough to handle such transactions but in future these are definitely possible.

V. CONCLUSION - RESPONDING TO THE NEW CHALLENGE – IS BANNING EFFECTIVE?

Usual response to any unknown technical challenge is to ban them outright. In last few years Virtual coins were either declared illegal or made harder to operate in many jurisdictions. The problem is as virtual coins live within the internet and it is almost impossible to monitor internet effectively banning virtual coins does not work in reality. Chinese government tried to shut down Bitcoin exchanging platforms for last two years. They closed domestic platform and then blocked access to foreign platforms. For them the most concerning factor was flight of capital to foreign shore. Chinese government also close down Initial coin offerings. Although government claims that Bitcoin usage dropped and ICOS are absent, in reality most companies just shifted base elsewhere. Many companies went to South Korea or other nations where they started to operate services and Chinese citizens are using Bitcoin relying on Tor or VPN. Chinese citizens are still taking part in ICOs although they nowadays have to travel to the next country. So, banning Bitcoin can't be the solution. Secondly, banning virtual coins ensures that governments don't get capital gain taxes which can be a substantial amount.

Instead of banning coins better education about risks and providing necessary information to consumers are the first step. Crimes that are being committed using cryptocurrencies will drop

[6] Ari Juels et al, "*The Ring of Gyges : Investigating the future of criminal Smart Contracts*", https://www.initc3.org/files/Gyges.pdf.

 [ISSN 2581-5369]

down significantly when law enforcements get better equipment and training to understand and inspect blockchain. Education and providing better forensic technologies to investigating agencies should be priority. Efforts should be made to use considerable private expertise present in India to track and regulate cryptocurrencies. Banning them altogether would harm our capacity to develop new technologies in this sector.

One of the unintended consequence of banning cryptocurrencies is development of Blockchain related technologies get hampered. Many developers refuse to work in crypto related startups being afraid of legal hassles. India along with other countries are looking to encourage blockchain related developments. So, banning cryptocurrencies will definitely impact blockchain developments.

Instead, regulating them strictly and better education provide an effective solution. After Security Exchange Commission (SEC), America's capital market regulator, mounted a long and detailed campaign pointing out the shortcomings of Initial Coin offerings, the frauds related to ICO came down considerably in recent years. Also, tightening lax regulations meant that the people who are looking to float fraudulent ICOs had to seek other arrangements and people have better options within consumer protection domain. Thus, comparing the approaches taken by China and America, far saner option is to regulate virtual coins comprehensively instead of declaring them illegal outright.

*****

 [ISSN 2581-5369]