CESC 590 - How are Silk Road, The Dark Web and Bitcoin connected?

Lilibeth Blandon,
011815009

Niti Patel,
029348200

Priyanka Movva Ramesh,
029338073

The author of the paper: Andrew Sergeenkov

Publication Year: 2021

SECTION 1:

HISTORICAL SETTING OF DARKWEB AND BITCOIN*:*

The blockchain technology is a distributed ledger system that is shared among the individuals that utilize it to conduct transactions. It gives anonymity and security to both the user and the transaction, which is why crypto currencies like Bitcoin and now Monero, and Ethereum are used for the transaction. Anonymity and security are like two sides of the same coin; on one hand, where they can be used for good things like preserving people's privacy, supporting freedom of speech, and so on; where on the other hand, they can be used to carry out illegal activities like cyber terrorism, where wrongdoers typically go unpunished for their doings. While blockchain has numerous benefits, they also have significant drawbacks. For example, enhanced security and anonymity served as a fuel for dark web users to conduct illicit transactions using cryptocurrencies such as bitcoins which is independent of any central authority such as banks or government and engage in unlawful activities. Bitcoin swiftly became the payment method of choice for unlawful businesses engaging in facilitating illegal trades on the dark side of the internet in its early years. It is difficult to talk about Bitcoin's origins without addressing its infamous ties to the dark web, and how these ties were used as a significant argument against the viability of digital assets. The Silk Road, the first online dark web marketplace, used Bitcoin prominently as an alternative to traditional and tightly restricted payment systems. In this paper, we will look at how the dark side of the internet arose and how Bitcoin became entangled in its web.

SECTION 2:

BLOCK CHAIN

Blockchain can be described as a linked list of blocks in which it contains any data. In terms of Bitcoin, it contains the transaction information between two people. With blockchain, two parties can make a transaction and this data can't be tampered with because of its immutability property as well as having a cryptographic hash which serves as a digital signature. This signature is so unique that can't be reversed once it is hashed. Blockchain inherits a lot of properties of a Distributed Ledger Technology. Some features are that it is distributed, immutable, anonymous, secure, unanimous, time stamped, programmable.

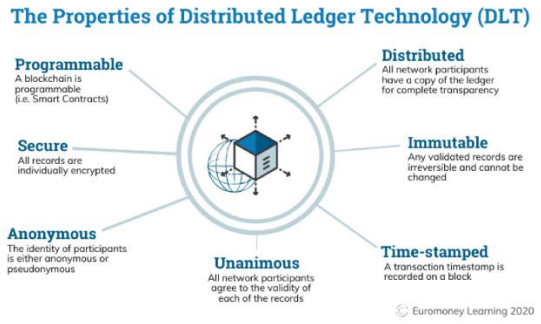

Fig.1. Properties of Blockchain [2]

DARK WEB

The dark web, also known as the dark net, is a place where anonymity is preserved when using the internet. It was originally intended for censorship but grew instantly into a place where anyone can share anything and can sell anything. The anonymity it preserves has caused the rise of illegal activities to take place in this system. Since there is no service provider to track these activities, people are open to selling drugs, ammunition, and many more. The dark web was able to exists because of the creation of the browser Tor (The Onion Routing). The main intent for this browser was to have a more private browsing network. Tor works by routing internet traffic to different destinations which makes it exceedingly difficult to find the source of this traffic.

SILK ROAD AND ITS DISCOVERY

Silk road is a digital marketplace that is used for the dark web, and it was founded by Ross Ulbricht. Ross Ulbricht intended to create a marketplace platform in which anyone can buy anything and have it delivered to your house with the key notion of being anonymous. Moreover, because traditional marketplaces like PayPal had a way to track the users, this was not ideal for the dark web users. That is why Silk Road became a great platform for selling illegal goods. Silk Road used Bitcoin to make payments and it also provided other services such as a system for vendor reviews, an escrow service, and a way to communicate with others privately through messages.

BITCOIN

Bitcoin is a decentralized digital currency that manages transactions on a peer-to-peer network using cryptography algorithms. Here decentralized technology of blockchain acts as the main component, where Bitcoin users handle their accounts (public address) and transactions using a private key without revealing their identity.

BITCOIN TRANSACTION

Once the transaction is received, bitcoin nodes accept and register the transaction into Bitcoin *Mempool* only if it is cryptographically acceptable(valid). Bitcoin node creates mathematical equation called

"mining process" by collating a set of transactions from mempool, thus the creation of new Bitcoin block happens only if Bitcoin node solves the mining process and verified by other Bitcoin nodes, generated new block is finally linked to the Bitcoin blockchain.

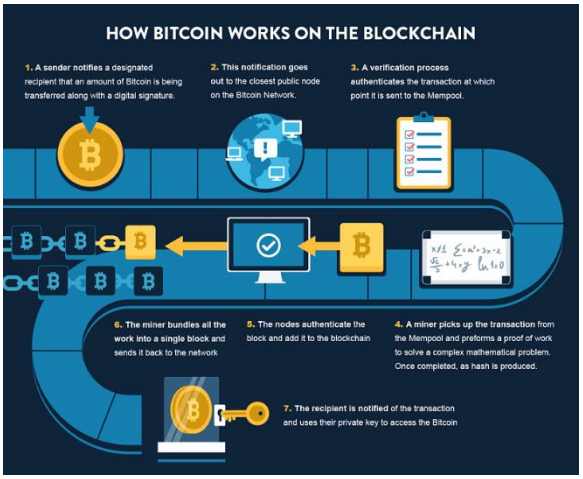

Fig 2. Bitcoin transaction [3]

SIGNIFICANCE OF BITCOIN IN DARK WEB

Bitcoin inherits the below-mentioned features of blockchain which caused global to embrace it with wide-open arms.

Anonymity: Execution of transactions without leaving a trace is extremely beneficial in the dark web.

Security: Dealers of the dark web require safe and reliable means of getting their illicit fund without getting an intrusion from the government can be achieved using bitcoin.

Dark Web was proposed to encourage the freedom of the press and open discussions instead, it is greatly misused for malicious purposes like drugs mafia, child pornography, etc. Bitcoin is one of the most used cryptocurrencies in the dark web apart from other cryptocurrencies like Litecoin, Monero, and dash.

Dark wallet has been created to enhance the data anonymization by obfuscating bitcoin transaction. Dark wallet is also called as "Coin mixer" as it uses Coin mixing method for the transaction. "Smart Mixer" or "Dark Wallet" has become the primary instrument of money laundering used actively in the Dark web by criminals.

According to the Australian study, about 47% (nearly half !!) of the Bitcoin transaction were allocated to satisfying the cravings of dark web mafias.

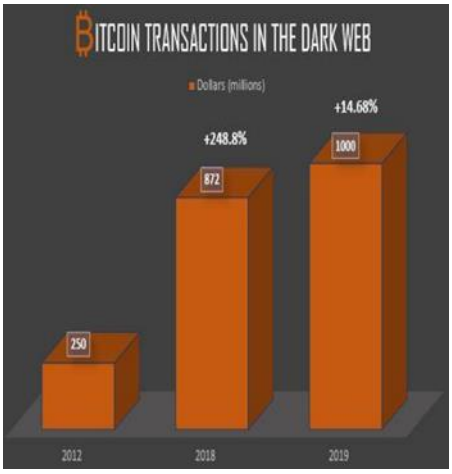

Fig 3. shows the usage of Bitcoin in various categories of dark web transactions.[2]

CLOSE RELATIONSHIP BETWEEN BITCOIN AND SILK ROAD

Creating a dark net marketplace originally failed because the traditional way of making payments involves a bank and so any transactions that happen can be stopped immediately. With a bank in place, the bank can easily detect false transactions and data being modified in the payment system. That is why Silk Road uses Bitcoin since the digital asset stored in the blockchain does not need a 3rd party like a bank. Bitcoin helped the Silk Road marketplace in having a payment system that is deregulated and lacks boundaries.

WAYS TO REGULATE AND TRACE TRANSACTIONS

Till now we have seen what the dark web and bitcoin are, the key role of blockchain technology in handling and making bitcoin transactions much more secure. It's time to discuss a few ways to stop or trace the activities happening over the dark web.

INTERPOL (International Criminal Police Organization) as a partner with European-Union, assisted in the development of a blockchain analytics tool that supports the tracing of cryptocurrency transactions and to search for cryptocurrency addresses and tags called "*GraphSense*".

And they are developing another tool called "Dark Web Monitor" which will allow gathering data on criminal activity on Darknet and a few inventory data like IP addresses, Darknet marketplace domains, PGB keys.

IS CRYPTOCURRENCY STILL USED IN DARKWEB?

Yes, cryptocurrencies are still used in the Dark web, and a shift towards privacy-oriented currencies is taking place which led to the evolution of 3200 cryptocurrencies now. But due to the increases in transaction fees and extreme volatility of price, the level of anonymity and decline in the rate of completion of transactions are the causes for declination in the use of Bitcoin on the dark web.

SECTION 3:

REVIEW:

The good thing from this paper is that when the author was explaining the inception of SilkRoad and how Bitcoin was used as a payment system only because of the anonymity but in the last section of the paper the author stressed that Bitcoin is a ledger system, and the transactions can be traced out and hence with the wallet address we can get to know about the real-life user details.

The bad thing we observed was that the author should have used a pseudo name for the SilkRoad founder because even though he contributed to the dark web, one needs to appreciate his ingenuity no matter what the creation has been for.

The ugly was that the author introduced Bitcoin as a currency and its usage in illicit transactions and should've emphasized in a small introduction as well as pros and cons.

SECTION 4:

IDEA: Using the existing Dark Web technologies we can design a platform for judicial system to get the digital proof of a crime from witness anonymously.

REFERENCES:

[1] Andrey Sergeenkov: How are Silk Road, The Dark Web and Bitcoin connected? https://coinmarketcap.com/alexandria/article/how-are-the-silk-road-the-dark-web-and-bitcoin-connected

[2] SHIV HARI TEWAR: Abuses of Cryptocurrency in dark web and ways to regulate them. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3794374

[3] Harsh Maurya- The In-Depth Guide to Bitcoin That Won't Leave You Frustrated. https://www.vpnmentor.com/blog/ultimate-guide-bitcoin/

[4] Blockchain, Cryptocurrencies, and the Dark Web https://hackernoon.com/blockchain-cryptocurrencies-and-the-dark-web-1a6d85916314