Committee: The Economic and Social Council

Question: Dealing with the rise of Online Banking and Cryptocurrency

Student Officer: Filippos Dounis

Position: Deputy President.

PERSONAL INTRODUCTION

Dear Delegates,

My name is Filippos Dounis, I am 16 years old and I am an IB1 student at Geitonas School. It is my honor to serve as the Deputy President of the Economic and Social Council in the 7th session of the Campion School Model United Nations. This will be my 4th overall conference and my first conference as a student officer. MUN has helped me greatly in my life and has shown me exactly what career path I want to follow in life.

The topic we will be discussing is a topic which has troubled the economics and finance community for quite some time. Not only will we be talking about the rise of online banking institutions such as PayPal, but we will be discussing about the rise of decentralized cryptocurrencies as well, such as Bitcoin and Ethereum. Our goal is to analyse the way these two different systems operate, highlight their strengths and weaknesses, evaluate the way they work and understand why they play such an integral role in today's society. It is crucial to understand that these systems are here to stay and it is our duty to provide certain frameworks that could ensure the harmonic usage of online banks and cryptocurrencies, tackling at the same time all of the problems that these systems might bring with them.

If you have any inquiries do not hesitate to reach me at: filippedounis@protonmail.com

Yours Sincerely,

Filippos Dounis

DEFINITIONS OF KEY TERMS

Proof of Work (PoW)

In Blockchain, this algorithm is used to confirm transactions and produce new blocks to the chain. With PoW, miners compete against each other to complete transactions on the network and get rewarded. (Cointelegraph)

Blockchain

The block chain is a public record of Bitcoin transactions in chronological order. The block chain is shared between all Bitcoin users. It is used to verify the permanence of Bitcoin transactions. (bitcoin.org)

Darknet

A computer network with restricted access that is used chiefly for illegal peer-to-peer file sharing.

V.P.N.

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

Annual Percentage Yield (APY)

The annual percentage yield (APY) is the real rate of return earned on a savings deposit or investment taking into account the effect of compounding interest.

The Onion Router (Tor)

The Onion Router (Tor) is an open-source software program that allows users to protect their privacy and security against a common form of Internet surveillance known as traffic analysis. Tor was originally developed for the U.S. Navy in an effort to protect government communications. The name of the software originated as an acronym for The Onion Router, but Tor is now the official name of the program.

White Paper

White Paper (WP) is a document that helps your prospective customer make an informed decision in favor of your company or a specific product. If the document does not facilitate a decision, it may be anything but not WP. Speaking in the most understandable language, white paper is something between an article and an advertising brochure. The document contains quite useful information and at the same time leads to the fact that the best solution is to purchase a certain product or service. (BitcoinWiki)

Genesis Block

The first block in the block chain. (bitcoin.org)

Bitcoin Mining

Bitcoin mining is the process of making computer hardware do mathematical calculations for the Bitcoin network to confirm transactions and increase security. As a reward for their services, Bitcoin miners can collect transaction fees for the transactions they confirm, along with newly created bitcoins. Mining is a specialized and competitive market where the rewards are divided up according to how much calculation is done. Not all Bitcoin users do Bitcoin mining, and it is not an easy way to make money. (bitcoin.org)

Market Capitalization

Commonly referred to as "market cap," it is calculated by multiplying a company's shares outstanding by the current market price of one share.

TIMELINE

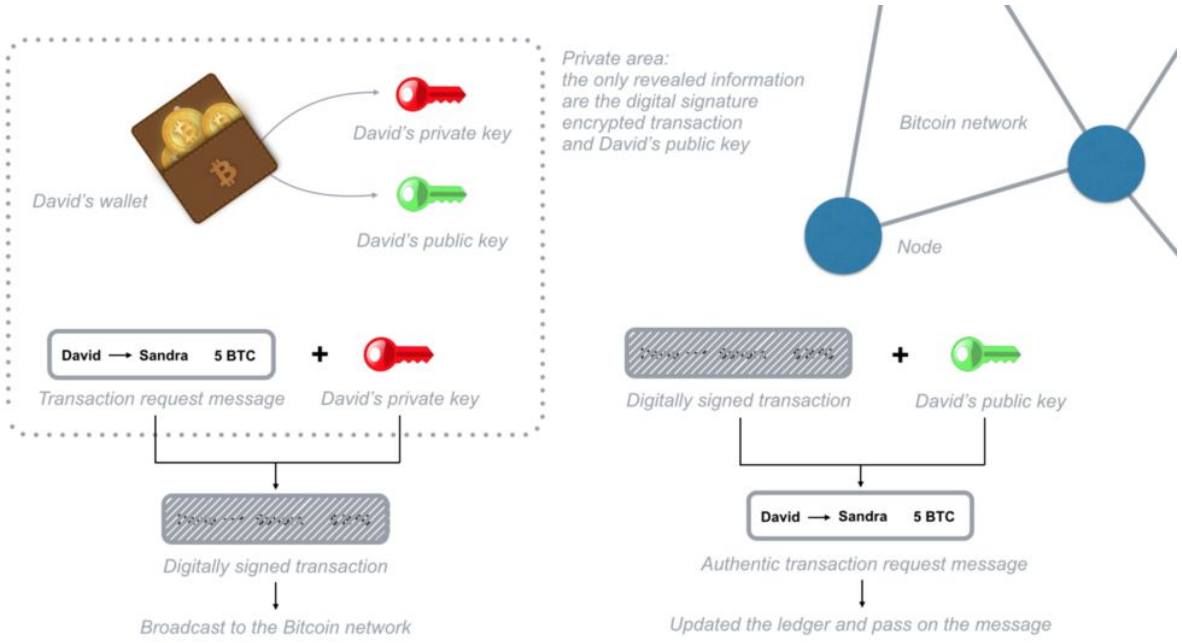
Date	Description of Event
1980s	The concept of the distributed computer starts to emerge.
1983	The Bank of Scotland offers NBS' costumers the first internet banking service in the UK, 'Homelink'.
2001	8 US banks have at least 1 million online users each.
2008	Satoshi Nakamoto publishes the whitepaper of bitcoin.
2007	Apple launches the iPhone and online banking shifts from the personal computer to the smartphone.
2009	The bitcoin genesis block is mined.
2010	The first bitcoin purchase takes place (10,000 BTC) for a pizza. (today it would be worth $6,000,000)
2010	Bitcoin's market cap exceeds $1M USD.
2011	BTC reaches parity with USD.
2011	Silk Road V.1 launches
2013	Bitcoins' market cap surpasses $1B. (10x growth in less than 3 years)
2013	Silk Road V.1 gets is taken down by law enforcement.
2013	Vitalik Buterin publishes the whitepaper of ethereum.
2014	Blockchain technology company R3 is founded and soon forms a consortium of over 40 legacy financial groups
2015	Ethereum's genesis block is created.
2016	Bug in ethereum DAO exploited and attacked.
2016	Gem launches Gem Health Network with Philips Blockchain Lab.
2017	Alpha Bay and Hansa market are taken down.

TOPIC DISCUSSION

The Blockchain

In order to discuss on cryptocurrencies it is of utmost importance to understand how the system behind them works and its main characteristics. As mentioned before this system is the blockchain. The blockchain allows the exchange of value without having to put trust in to a central authority or institution such as a bank. The way it succeeds in doing so is by being completely decentralized. The blockchain does not run on a single computer or server. It "lives" on every computing device which is connected to the network. These devices are also known as nodes and each device holds a copy of the entire log of transactions. This distinct feature of the blockchain means that each device connected to the network can view everyone's transactions. This can be seen both as a good and a bad thing. Many may think that this means that there is a complete lack of privacy. In fact that is a completely wrong statement. The fact that everyone can see the addresses and the funds being exchanged among the network does not mean that the users sending the funds can be identified. That is because by default wallets are not tied with real identities.

Security in the blockchain is also guaranteed. Unlike a traditional financial institution there is almost no risk of funds being sent to the wrong recipient by the system. Each transaction in the blockchain requires the existence of a wallet from which the funds will be transferred. Having in mind that the only individual who should be accessing this wallet is the owner each wallet is protected by a strong, special cryptographic protocol. This protocol generates two unique digital keys for each wallet, a public one and a private one. Similarly to PGP encryption if a message is encrypted with a specific public key, only the person who has access to the paired private key can view the encrypted message. In simpler terms when a transaction occurs and it gets encrypted with a wallet's private key a digital signature is created which is then used by every computer connected to the blockchain in order to verify it and ensure that it is a legitimate request.



Digital Signature transaction encryption simplified (https://medium.com)

The way the blockchain work could be summed up as the following:

A node (computer) connected to the network creates a transaction which is then signed with a digital signature, the private key. The transaction is then evaluated by the other nodes connected to the blockchain and gets validated.

Once the transaction is validated by the network it is considered confirmed and it is included in a "block". This block is a collection of data which gets linked with other blocks in chronological order and creates a chain of information or blocks.

The block that was just created becomes a part of the blockchain and links itself to the next block by utilizing certain cryptographic methods. This is when the block gets its first confirmation by the network and the transaction it's second. The transaction continues to get confirmed every time a new block is being generated. By the time the transaction reaches its sixth confirmation the transaction is considered final.

Now that we have established a basic understanding on how the blockchain works we are going to analyze three cryptocurrencies of great importance, bitcoin, ethereum and monero. Through these three we will be able to understand the reasons for which they have seen such an exponential growth in popularity, the reasons for which they are gradually replacing fiat currencies as well as the dangers that cryptocurrencies bring with them.

Bitcoin (BTC)

Bitcoin is the first cryptocurrency ever created. It was founded in 2009 by “Satoshi Nakamoto”. It is believed to be a pseudonym and the founder’s/s’ identity remains a mystery. Bitcoin enables users to send instant payments anywhere in the world with absolute security and low costs. It is a peer-to-peer system that operates under no central authority.

Many believe that bitcoin is the future of all money and it will be soon replacing all fiat currencies in the name of a global decentralized cryptocurrency as the main means of performing transactions. Bitcoin was created to solve the main issue of all currencies, all the trust that's required to make a currency work. Trust should not be a criterion in such a financial system, as trust is volatile and prone to disappoint and collapse. By using the concept of distributed computing and decentralization bitcoin completely replaces the need for trust.

As stated by the bitcoin foundation " Bitcoin Transactions are:

- Permissionless and borderless. The software can be installed by anybody worldwide.
- Do not require any ID to use. Making it suitable for the unbanked, the privacy-conscious, computers or people in areas with underdeveloped financial infrastructure.
- Are censorship-resistant. Nobody is able to block or freeze a transaction of any amount.
- Irreversible once settled, like cash. (but consumer protection is still possible.)
- Fast. Transactions are broadcasted in seconds and can become irreversible within an hour.
- Online and available 24 hours a day, 365 days per year."

Many argue that Bitcoin is better used to store value, as it is too volatile and with too many fluctuations in price to be a currency used for everyday transactions. The truth is bitcoin is great for both. It serves both as "digital gold" and easy to use money for everyday spending at the same time.

Stored Bitcoins have the following characteristics:

- Only 21 million bitcoins will ever exist as that is its max supply. Printing more bitcoin is both theoretically and technically impossible.
- Are easy to protect and hide.
- Have zero storage costs. The number of bitcoins does not play any role in the way they are stored. Storing 1 bitcoin will cost you the same with storing 500 bitcoins, $0.
- No transaction takes place unless it is mutual and agreed.

Contrary to popular belief bitcoin transactions are not anonymous. The blockchain is public for everyone to examine. Thus it is easy for someone to track the movements of certain funds and follow the money from the original address to the destination address.

Ethereum (ETH)

Ethereum is currently the second-largest cryptocurrency after Bitcoin. According to ethereum's site "Ethereum is the foundation for a new era of the internet:

- An internet where money and payments are built in.
- An internet where users can own their data, and your apps don’t spy and steal from you.
- An internet where everyone has access to an open financial system.
- An internet built on neutral, open-access infrastructure, controlled by no company or person."

Launched in 2005, Ethereum is the first and leading programmable blockchain. It shares many characteristics with other cryptocurrencies such as having its currency (ETH), it "lives" on the blockchain, it is scarce and it can be sent from anyone to anyone, from anywhere to anywhere.

Dapps

"Dapps" stands for Decentralized applications. They are the reason for which ethereum is so similar but at the same time so different from other cryptocurrencies such as bitcoin. Anyone can program a "dapp" by using the appropriate software. Once a decentralized application is deployed it will run as programmed and stay on the blockchain. The fact that they are decentralized means that no single entity or person controls them. There is no restriction on the type of service that can be created based on the ethereum blockchain with most of them being:

- Cryptocurrency wallets. These wallets enable you to make low-cost instant payments with Ethereum or any other asset you can imagine.
- Financial applications. These applications enable you to borrow, lend, or invest your digital assets.
- Games. Many games can be found that are built on ethereum's blockchain and you can even accumulate ETH just from playing.
- Decentralized markets. These markets can be whatever you can imagine, where the trading of goods happen live on ethereum's blockchain.

Ethereum boasts about having the largest and most active community in the entire world. It includes developers, investors, miners, ordinary users, multi-billion companies and much more. Due to the large involvement with "daps" and people's interest in the way they work there are thousands of different tutorials and guides which can be used by anyone to make a decentralized application. This enables companies with no experience of blockchain development to quickly grasp the concepts and start developing on ethereum.

Monero (XMR)

Monero is different from most other cryptocurrencies as it possesses one distinct characteristic that makes it unique. Monero is the most secure, private and untraceable cryptocurrency currently in the market. Similarly to all other cryptocurrencies, all transactions are confirmed by distributed unison and recorded on the blockchain in an immutable way. Monero utilizes three main techniques to keep its users private:

- Ring signatures
- Ring confidential transactions
- Stealth addresses.

This way Monero's users enjoy the perks of a decentralized platform similar to bitcoin without all of the privacy issues. Origins, amounts, and destinations of transactions are all concealed and no one can track a user's transactions. At the same time, the fact that users remain completely anonymous while using Monero is the reason for which it is the cryptocurrency of choice for carrying out illegal transactions (this will be further analyzed in the "dangers of cryptocurrency" section).

Monero also has a really helpful and knowledgeable community with over 500 developers and 30 core developers. Many forums and IRC channels can be found with the majority of them being welcoming and active. Monero's Research Lab, as well as all of its developers, are constantly trying to achieve more anonymity and privacy, pushing the frontier of cryptocurrency privacy and security further than it has even been before.

Dangers / Illicit Uses Of Cryptocurrency

It must be obvious by now that cryptocurrencies have much to offer. Unfortunately, though cryptocurrencies have another side to them as well. Their decentralized nature is the reason for which there are many instances where their use for illicit activities can be observed. Through coins such as Monero criminals can carry out illicit transactions without the fear of being exposed or getting caught by law enforcement.

Dark-Net Marketplaces

Studies show that Bitcoin and Monero are being constantly used to purchase illicit goods such as drugs, weapons and stolen credit card numbers from different Darknet marketplaces. It is extremely difficult for Law Enforcement to track these activities as they take place in the Dark-Net. Thus they can not just take the website down as it is technically impossible. This is the reason for which Dark-Net marketplaces are flourishing and getting thousands of new members every day. Fortunately, there have been instances where law enforcement has been able to shut such websites down. It is important to analyze these cases to understand how these marketplaces operate as well as how to stop them.

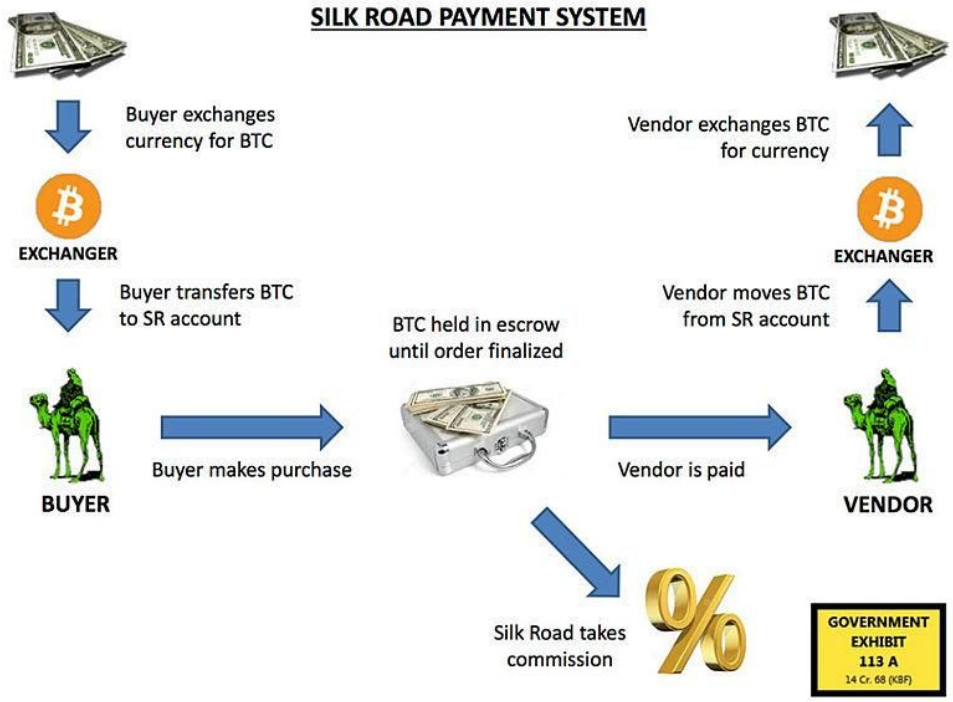
Silk Road

If one wants to analyze Darknet Markets, Silk Road is impossible not to mention. In fact, it is the reason for which Darknet markets came into existence in the first place. Founded in February 2011 by "Dread Pirate Roberts" (Ross William Ulbricht) Silk Road quickly became a worldwide phenomenon accumulating more and more fans.

By 2013 the site had around 10,000 products for sale with 70% of these products being drugs. Other products available on the website were fake documents, guides, and counterfeit items. Based on data the FBI collected by imaging Silk Road's server on July 23, 2013 there were approximately 1,229,465 transactions completed on the site with revenue of 9,519,664 Bitcoins and a commission of 614,305 Bitcoins for the site. This involved a total of 146,946 buyers and 3,877 vendors being involved with the site. In today's rates that would mean a revenue of approximately 77.3 Billion US dollars and a commission amounting to 5 Billion Dollars just for the site's staff.

Ross Ulbricht wanted to create an unregulated from law enforcement platform where users could interact with sellers freely. In order to achieve this anonymity was crucial. This is why he understood the need for using cryptocurrencies and in particular, Bitcoin and Monero for the funds exchanged to be kept private. He came up with a payment system that would then be used as the basis for most other darknet marketplaces to follow. This payment system used "escrow" as a form of reassurance to both buyers and sellers that everyone would get what they were supposed to.

Silk Road's payment system could be described as the following:



It is of great importance to note that the seizure of Silk Road V.1 in 2013 (many more were created after that by silk road fans) was not due to some vulnerability of Bitcoin or Monero. The reason for which Silk Road reached its demise was clearly human error. One could say that there are many different events that weakened Silk Road more and more but the most important out of those events was Ross Ulbricht's arrest. His arrest was made possible as law enforcement was able to connect his alias "Dread Pirate Roberts" with accounts he had previously made on different forums and sites that directly collected his pseudonym with his real name and personal information.

The lesson to be learned from Silk Road's case study is that the biggest asset which can be used to combat the illicit use of cryptocurrency is human error. Furthermore, it is important to note that Silk Road constitutes the birth of a new wave of platforms used to perform transactions of illegal goods and created the payment system employed by all major darknet marketplaces to date.

Operation Bayonet

"Operation Bayonet" is an operation that took place on June 2017 by the Dutch Police. The objective of the operation was to take down one of the largest markets at that time, "Hansa Market" and identify as many of its members as possible.

"Hansa Market" was home to many different types of services and goods. Notably, the most popular services provided were the selling of illicit substances, hacked accounts, and credit cards as well as different stolen and counterfeit products. At its height, Hansa's 3,600 dealers offered more than 24,000 drug product listings, from cocaine to MDMA to heroin. It was the largest darknet market in Europe and no one believed it would be taken down.

"Operation Bayonet" was carried out in a different fashion than most other similar law enforcement operations. After a tip by a cybersecurity company whose name remains anonymous, Dutch police forces were able to locate Hansa's "developer server" hosted by a company based in The Netherlands. In contrast to the actual market, the developer server did not operate via tor. Through this new finding, they immediately discovered the identity of the two creators of the marketplace and by cooperating with German authorities the two German Nationals were apprehended. After the successful arrest of the two men something unexpected happened. The FBI contacted Dutch law enforcement to inform them that Alpha Bay’s servers were located in the Netherlands. AlphaBay was at that time the largest darknet market in the world with far more traffic and popularity than Hansa.

That was the moment where they had an unprecedented idea. They theorized that if AlphaBay was taken down the former users of the market would immediately start looking for substitutes, mass immigrating to the next largest site. Thus they decided to pull out an

incredible scheme. By arresting Hansa's admins and shutting down AlphaBay they had full access to Hansa (after interrogation about the credentials). They changed some parts of the code in order to collect more users data and managed to decrypt all pgp messages by saving the messages before being encrypted. They decided that it would be better to operate the website for a month and collect as much information about the users/sellers as possible. Doing so was not difficult as the two men had left everything unencrypted and with no real protection. Through this scheme they managed to get thousands of credentials and identify Hansa's and Alphabay's users/sellers.

Although Bitcoin was used as the token for the transactions it appears like again its anonymity was not breached and human error was the main reason that contributed to the success of the operation.

Ransomware

Ransomware software is notably one of the worst malicious uses of Bitcoin. Among malware creators, it is believed to be one of the most destructive types of viruses. It employes cryptography and creates a pair of two unique keys, a public and a private key. Once the virus is deployed the public key is used to encrypt the target's system and can only be decrypted using the attacker's private key.Once a system has been compromised, the hard drive's contents become encrypted and the user is unable to access them. The attacker usually threatens the victim that if a specific ransom is not paid in Bitcoin the contents of the hard drive will be published online. The typical way this attack is carried out is by disguising itself as a legitimate file that the user is tricked into downloading or opening.

WannaCry is the biggest in scale ransomware infection ever performed. In 2017, more than 200,000 computer systems were infected in more than 150 countries. It lasted for a period of four days and caused unimaginable damage. The main target of the attack were hospitals and health services around the world. They included the National Institute of Health in Colombia, Britain's NHS and numerous Indonesian hospitals. By targeting such institutions it completely shut down the hospitals' machinery and the only option was to pay the ransom. Other businesses were targeted as well and more than $200,000 were sent to the attackers. Even police precincts were forced to pay the ransom as there was no way to regain access to their systems.

Law enforcement was unable to trace the identity of the people holding the funds as all transactions were made via bitcoin. The hackers who are presumed to be "Lazarus Group", a North Korean hacking group that was responsible for the 2014 Sony Pictures cyberattack and the 2016 Bangladesh bank heist wanted to find a way to be as anonymous as humanly possible. This is where Bitcoin came in handy as it ensured their anonymity.

Many blame the NSA for the attack as the attackers used a tool called "EternalBlue". This tool was developed by the NSA and had found a vulnerability in Windows systems which could be exploited to gain access. The hackers were able to gain access to this exploit as it was stolen from the National Security Agency and leaked by a group calling themselves "The Shadow Brokers". The virus was so destructive as it was capable of copying itself from one system to another with no human intervention needed. The attack was stopped four days after it first appeared as law enforcement was able to find a kill switch created by the attackers themselves if anything went wrong and managed to stop "wannacry" from spreading and infecting more devices.

Human Trafficking

Human trafficking has existed for thousands of years. One would assume that nowadays this phenomenon would be almost extinct and nothing more than a bad chapter of human history. Unfortunately, this is far from the case as an estimated of over 45 million men, women and children are victims of this modern-day slavery. In fact, human trafficking following the narcotics business is one of the most booming industries with a staggering worth of $150 billion. Its main aspects are:

- Forced sexual exploitation
- Organ Harvesting
- Forced Marriages
- Forced Labor
- Murders
- Forced Abortions for Stem Cell Harvesting
- Child slavery.

Following the trail of these human trafficking businesses, has been difficult for law enforcement. In recent years their job has become even more difficult as criminals have started using different cryptocurrencies and the darknet to cover their tracks. Deputy Superintendent of Jamaican Police Carl Berry says:

"They are asking for payment in bitcoin and other cryptocurrencies, a new factor which creates problems for law enforcers."

By using bitcoin they are now able to hide behind a “mask” without being afraid of being exposed or arrested. The only thing they need to do is simply find someone wishing to buy one of their "products", agree on a price and then deliver anonymously.

This recent shift in means of transactions should not come as a surprise. Criminals are always trying to advance and anonymize themselves from law enforcement. Hense whenever a new technology comes out which can be of assistance to them they will eventually use it.

Bitcoin Mixers/Tumblers

Bitcoin mixers can be characterized as platforms that split bitcoins and then reassemble them. There are various tumblers on the darknet and their service fees range from 1-3 percent. The way they work is quite simple.

Firstly the "dirty" funds are sent to a hidden tor wallet. This type of transaction is usually referred to as "hop" and it can be done many times. The more it is done the more obfuscated the funds are as additional layers are placed between the original and destination address.

It is now time to deposit the funds to the mixer's receiving address. Once that is done the tumbler will split the bitcoins to numerous small transactions, sending small chunks to different unrelated wallets. Then these unrelated wallets send the value of the original transaction (minus the fees) to a new clean address.

The funds are now ready to be used and even deposited to official exchanges to be converted to fiat currency.

Unrelated exchanges

Unregulated exchanges are another common way for large amounts of cryptocurrency to be laundered. Unregulated exchanges are considered all exchanges that do not carry out "Know-Your-Customer and Anti-Money-Laundering (KYC/AML)" procedures, such as identity checks and allow the anonymous exchange of funds on their platform.

This is perhaps the easier way as the only thing the user must do is trade small chunks of bitcoin manually with different unregulated exchanges. This resembles "hopping" in a way as the user adds an additional layer of privacy each time. Once this is done the user can take his "clean" funds and convert them into fiat currency.

Of course, there are multiple other ways through which money laundering can be achieved such as through bitcoin casinos. The two examples listed above are the most widespread and common techniques used.

Online Banks

An online bank, not to be confused with online banking is a banking institution that can only be accessed through the internet. Online banking on the other hand is a web portal through which you can carry out your everyday banking operations but has a physical store as well.

After the financial crisis of 2008, the general populous started losing faith in banking institutions as they believed they were the ones responsible for the collapse of the financial system as well as the loss of their funds. This type of uncertainty was then used by open-minded individuals who sought to find a way to use this widespread sentiment for their gain. This is how online banks were created.

Banks, on the one hand, alternative revolutionary institutions on the other, where funds could be securely stored without any fear. This new generation of banks had to choose a target audience that would better appeal to their message. Millennials were the obvious answer. This generation of technology thirsty individuals have learned and been

used to having everything in the reach of their hands. Their mobile device must have everything they need in life, and access to their bank is one of those things. Online banks have focussed on offering quality, user-experience through their digital banking services. For them, the most important aspect of their business is customer service and satisfaction as well as the visually satisfying appearance of both their web platform and credit cards. This can be easily confirmed by examining some samples of credit cards provided by online banks.

Obviously, appearance is not the only reason for which there has been such a rise in the popularity of digital banks. In order to understand the deeper reasons behind this increase in demand for said services, it is eminent to analyze the pros and cons that come with them.

Benefits of Online Banks

High Yield Interest Rates and Lower Fees

The main advantage of using an online bank is the minimal to no fees that come with it. It is known by now that the central difference between online and traditional banks is the fact that online banks have no physical infrastructure. Hence, there is no need to spend funds for maintaining the multiple physical branches that would come with a traditional bank. This enables online banks to pay higher interest rates or annual percentage yields (APYs) on savings by having minimal to no fees at the same time. The most popular of these digital banks offer interest rates up to 2%. A major difference to conventional banks where the majority of them offer an APY of 0.01%.

It might seem like the difference in APY is not important. In larger amounts, though this difference in numbers can be huge. A balance of $10,000 deposited for 10 years at 0.01% will earn $10; at 2.25%, it earns just over $2,500. Thus it is obvious that this feature of online banks is more than compelling, especially in customers with large account balances.

At a conventional bank, you are also more likely to be charged with a wide range of fees, such as those for keeping an account open with a low balance, making direct deposits, or paying by check or debit card.

Convenience

Convenience might seem like something obvious but it is important to measure. By having an account in an online bank you can access this account wherever you are whenever you want. The only things that are required are an electronic device such as a mobile phone or laptop and a working internet connection. The physical limitations posed by traditional banks such as the need for a physical branch in your area or atm and time have been eliminated.

Toll-Free ATM Access

It has been stated that online banks eliminate the need for having a physical branch. This stands true, but there are cases where the need for physical access is needed. The most important and usual case is when someone wishes to convert their digital money into cash. This process takes place through ATM machines. Conventional banks usually have some type of fee which reduces money from your balance each time you withdraw cash. Online banks eradicate this problem by giving their customers access to huge ATM networks that offer fee-free withdrawals. These ATMs can easily be located through the bank's mobile application.

Disadvantages of Digital Banking

Server Down-time

When dealing with online-only services there is always a chance of having technical difficulties. In the case of online banks, there is the rare potential for the servers of the bank to go down. This might be due to a variety of technical issues. When this happens the customers are unable to use the app or website portal. On this occasion, their databases will probably become unreachable as well, meaning that the funds will be completely frozen.

Difficulty of Depositing Cash

When the entire notion behind online banks is centered on the fact that physical relation between customer - bank is no longer needed it is difficult to imagine how an

operation such as depositing cash takes place. Reality is that it is sometimes tedious and requires too many steps. The two easiest and simplest ways to deposit cash are either through an ATM or another bank. If the ATMs network used by your bank of choice allows cash deposits through ATM machines then that would be the easiest way to carry out said task. If on the other hand there is no such possibility one would have to deposit the funds to a third party traditional bank and from there transfer the funds to the online one.

Lack of Checking Options

A sad reality about online banks is that despite the extremely high APY that they offer, there is no range in available checking accounts. In fact, most online banks do not even offer checking accounts with a minority of them having some options.

Security

Security is a major issue that must be addressed. There are two types of security issues that might possess a serious threat to customers of said banks. Bank security and individual security. When a service is strictly online and there is a monetary gain in exploiting it there will be many people trying to achieve exactly that. It is of utmost importance for banks to always keep their systems' security up to date and always implement all possible security updates and protective measures. There have been numerous instances in the past where hacking groups have managed to gain access into banking institutions' customers' databases with the most recent one being a breach in "Capital One's" data-server where the information of more than 100 million people were sold online. Furthermore, there have been 3,494 successful cyberattacks against financial institutions, according to reports filed with the Treasury Department’s Financial Crimes Enforcement Network making it obvious that such institutions do not exempt themselves from falling victims of cyberattacks.

The other really important security-related issue that must be analyzed is individual security. Hackers always tend to want to exploit the weakest security link. It would be an understatement to state that individuals are more prone to attacks than the banks themselves as the security measures implemented by individuals are most of the time non-existent.

POSSIBLE SOLUTIONS

As there have been no previous attempts to really tackle any of the issues mentioned it is important for delegates to use this part of the study guide as reference and use their creativity in order to find the best possible solutions to the different issues.

Anonymity In The Blockchain

Due to the nature of cryptocurrencies there are limited things that can be done. By examining the ways through which the trails of cryptocurrencies can disappear it is obvious that bitcoin mixers play a huge role in making the illicit funds anonymous. Law enforcement agencies should try to locate the location of these websites' servers and eventually take them down.

Another common way for criminals to launder their funds is through cryptocurrency exchanges that do not require any form of identification. These exchanges are not limited to shady, darknet platforms. There are numerous legitimate and popular websites where identification is not required to exchange funds. The legitimate exchange which is most commonly used by criminals is "Local BTC". Local BTC is a peer to peer marketplace that shares many common features with ebay. It is a platform where sellers connect with buyers with the intention of buying and selling bitcoins. A legal framework must be established where all buyers and sellers provide the appropriate identification to the website, both for security reasons and ameliorating user experience by ensuring a safe and friendly environment for all.

Reducing Bitcoin Fees And Transactions Delay

Although fees in the bitcoin network are low, when large amounts are being transferred the fees can become quite high. Another issue which is prevalent and directly connected with the fees in the network is the delay of transactions. The confirmation of a single bitcoin payment can take from 30 minutes to whole days, depending on the fee paid. This can be frustrating for both everyday users and especially for businesses trying to carry out payments.

The solution to this issue is the “Lightning Network”. It is a payment protocol that operates on top of cryptocurrencies such as bitcoin and enables fast, fee-free transactions. A mass adoption of the lightning network by raising awareness among businesses and individuals could offer a solution to the issue.

Security In Online Banking

It is critical for online banks to keep their systems secure and protect customer data. The existing regulations on this topic are more than enough to push banks to constantly updating their security measures and keep up to date with the different advancements in the field of cyber security.

The ones who risk compromising their credentials are the people themselves. There are multiple ways through which attackers manage to gain such user data but the most common and easiest to tackle are “Man In The Middle” attacks. This type of attack is carried out by hackers when the victim tries to access the web portal of the bank from a public area such as a public wifi network at a coffee shop. Banks have already implemented security measures to secure customers from “Man In The Middle” attacks by encrypting all forms where users can submit data. Unfortunately this is not enough to secure people from being deceived. Hackers create fake clones of the real banking websites and redirect all network traffic to the illegitimate website where they can see all the information being submitted by the user. The only real way through which this can be addressed is by encouraging online banks to add their own VPN software to their services. This way when a customer tries to login to his bank account all of his traffic will be redirected through an encrypted tunnel where the attacker will be unable to view any sort of critical data.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

United States

The United States is one of the countries whose intentions are still not completely clear as far as cryptocurrencies are concerned. There seems to be a generally positive stance towards the use of the blockchain in the financial sector, having at the same time many concerns on the unstable nature of the coins as well as their use for illicit activities. This can be verified by the Securities and Exchange Commission's warning to investors about cryptocurrency investing risks, the halting of several initial coin offerings and many comments on the need for more regulations. At the same time the Commodity Futures Trading Commission became the first U.S. regulator to allow for cryptocurrency derivatives to trade publicly, marking a milestone for cryptocurrencies. Summing up the country seems to be quite sympathetic towards the use of cryptocurrency but is alarmed by the volume of illegal transactions happening within these systems and highly supports the implementation of regulations.

Australia

Australia seems to be quite a cryptocurrency friendly country. This can be seen by the fact that members from both major political parties (Coalition and Labor) voted for the Reserve Bank of Australia to accept cryptocurrencies as an official form of currency. It seems like the Australian government believes that cryptocurrencies should not be seen as different from traditional fiat currencies and it is currently legal for any entity to buy, trade or mine cryptocurrencies.

The United Kingdom and the European Union

The United Kingdom stands united with the European Union on it's plans to regulate cryptocurrencies use in the future. At current time there seems to be no official stance on cryptocurrencies, prompting EU members to develop their own legislative frameworks and stances towards the use of crypto. In more detail:

- Finland has decided to make Bitcoin unbound from value added tax (VAT), by not viewing cryptocurrency as a currency but as a commodity.
- Belgium seems to follow Finland's steps by making cryptocurrency immune to value added tax.
- Cyprus has made no official comment on cryptocurrencies and has currently implemented no regulations.
- Germany seems to be open to Bitcoin and cryptocurrencies but have made some statements implying the need for the implementation of regulations such as the comment of Joachim Wuermeling, a board member of the German Bundesbank calling for global regulations on digital currencies. It is important to note that in Germany cryptocurrencies are legal but are taxed differently according to user. Exchanges, miners, enterprises and everyday users are taxed differently.
- Bulgaria as of recently has started to tax Bitcoin.

The People's Republic of China

China is one of the countries with the most firm stance against cryptocurrencies. Bitcoin and all other cryptos are essentially banned in China. Financial institutions such as banks and payment processors are prohibited from interacting and accepting Bitcoin. All cryptocurrency exchanges are banned and the government has reportedly prosecuted miners. This crackdown on miners might be perceived as something quite odd as in 2017, more than 50% of the miners worldwide were from china. After further inspection though this move by the People's Republic of China on the complete ban of cryptocurrencies seems natural as the government's administration has repeatedly tried to censor online activity, eliminate anonymity and crack down on corruption and illegal transactions.

The Republic of Korea

South Korea is one of the oddest cases of them all. That is due to the fact that initially South Korea was considered as a safe-haven for bitcoin enthusiasts and miners that had fled from China. In the beginning of 2018 everything changed when top government officials started discussing the implementation of cryptocurrency regulations. On January 23 2018 the South Korean government enforced a law forbidding anonymous accounts to trade cryptocurrencies. The New York State's Department of Financial Services also reported being requested by South Korean authorities to deliver customer information on accounts associated with six South Korean banks with branches in New York.

Russian Federation

Russia's stance on cryptocurrency is not as simple as stating they are either for or against cryptocurrencies. In September 2017, the chief of the central bank of Russia Elvira Nabiullina said that the central bank was against regulating cryptocurrencies as currency and would not equate them with foreign fiat currency. That means that cryptocurrencies should not be used as payment for goods and services. On the other hand, President Vladimir Putin among others has continuously stretched the dangers of cryptocurrencies and the need for strong legislative actions in the near future in order to crack down on money laundering and illicit transactions. On January 25 2018 the Finance Ministry published a draft of a legislation which would define tokens, establish ICO procedures and determine the legal framework for cryptocurrencies and mining. Presidential candidate Titov Boris said in a press interview "The Finance Ministry's proposals present a much tougher regulation than in Japan, Switzerland, Belarus [and] Armenia; that is, in all countries that have adopted some form of legislation. It would be better not to adopt anything than to adopt such legislation.

Research Questions

In order to gain a deeper insight into the topic and explore the variety of fields were cryptocurrencies could be used you could read the following articles:
https://blockgeeks.com/guides/blockchain-applications/
https://hackernoon.com/10-uses-for-blockchain-that-will-change-the-world-c5b96cf7c976
https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx

The delegates could also find different uses of the blockchain for the UN. An example for how the UN has used and is planning to use the blockchain could be found here:
https://www.coindesk.com/the-united-nations-wants-to-accept-ethereum-and-bitcoin-and-soon

Lastly the delegates are urged to read the original whitepaper of bitcoin in order to understand exactly what it's goals are and what Satoshi Nakamoto had envisioned about his creation.

https://bitcoin.org/en/bitcoin-paper

BIBLIOGRAPHY

Andreas M. Antonopoulos (April 2014). Mastering Bitcoin. Unlocking Digital Crypto-Currencies. O'Reilly Media. ISBN 978-1-4493-7404-4.

Oscar Williams-Grut and Rob Price (26 March 2017). "A Bitcoin civil war is threatening to tear the digital currency in 2 — here's what you need to know". Business Insider. Retrieved 2 July 2017.

Jordan Pearson (14 October 2016). "'Bitcoin Unlimited' Hopes to Save Bitcoin from Itself". Motherboard. Vice Media LLC. Retrieved 17 January 2017.

Empson, Rip (28 March 2013). "Bitcoin: How an Unregulated, Decentralized Virtual Currency Just Became a Billion Dollar Market". TechCrunch. AOL inc. Archived from the original on 9 October 2016. Retrieved 8 October 201

"Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Banking, Housing, and Urban Affairs Subcommittee on National Security and International Trade and Finance Subcommittee on Economic Policy" (PDF). fincen.gov. Financial Crimes Enforcement Network. 19 November 2013. Archived (PDF) from the original on 9 October 2016. Retrieved 1 June 2014.

Orcutt, Mike (19 May 2015). "Leaderless Bitcoin Struggles to Make Its Most Crucial Decision". MIT Technology Review. Archived from the original on 18 October 2017. Retrieved 22 June 2017.

Golumbia, David (2015). Lovink, Geert (ed.). Bitcoin as Politics: Distributed Right-Wing Extremism. Institute of Network Cultures, Amsterdam. pp. 117–131. ISBN 978-90-822345-5-8. SSRN 2589890.

Katz, Lily (12 July 2017). "Bitcoin Acceptance Among Retailers Is Low and Getting Lower". Bloomberg. Archived from the original on 25 January 2018. Retrieved 25 January 2018.

Biggs, John (8 April 2013). "How To Mine Bitcoins". Techcrunch. Archived from the original on 6 July 2017.

Gervais, Arthur; O. Karame, Ghassan; Gruber, Damian; Capkun, Srdjan. "On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients" (PDF). Archived (PDF) from the original on 5 October 2016. Retrieved 3 September 2016.

Braue, David (11 March 2014). "Bitcoin confidence game is a Ponzi scheme for the 21st century". ZDNet. Archived from the original on 6 October 2016. Retrieved 5 October 2016.

Moore, Heidi (3 April 2013). "Confused about Bitcoin? It's 'the Harlem Shake of currency'". theguardian.com. The Guardian. Archived from the original on 1 March 2014. Retrieved 2 May 2014.

Dan Caplinger (4 April 2013). "Bitcoin's History of Crushing Speculators". The Motley Fool. Archived from the original on 7 January 2014. Retrieved 7 January 2014.

Ball, James (22 March 2013). "Silk Road: the online drug marketplace that officials seem powerless to stop". theguardian.com. Guardian News and Media Limited. Archived from the original on 12 October 2013. Retrieved 20 October 2013.

Stross, Charles (2013). Neptune's Brood (First ed.). New York: Penguin Group USA. ISBN 978-0-425-25677-0. It's theft-proof too – for each bitcoin is cryptographically signed by the mind of its owner.

"Informed Investor Advisory: Cryptocurrencies". North American Securities Administrators Association. April 2018. Archived from the original on 23 July 2018. Retrieved 23 July 2018.

Martin, James (2014). Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs. New York: Palgrave Macmillan. p. 2. ISBN 9781349485666.

"Anticounterfeiting on the Dark Web – Distinctions between the Surface Web, Dark Web and Deep Web" (PDF). 13 April 2015. Retrieved 1 June 2015.

Roger, Jolly. "Clearnet vs Hidden Services – Why You Should Be Careful". Jolly Roger's Security Guide for Beginners. DeepDotWeb. Archived from the original on 28 June 2015. Retrieved 4 June 2015.

Taylor, Harriet (19 May 2016). "Hit men, drugs and malicious teens: the darknet is going mainstream".

Miller, Tessa (10 January 2014). "How Can I Stay Anonymous with Tor?". Life Hacker. Retrieved 7 June 2015.

Mansfield-Devine, Steve (December 2009). "Darknets". Computer Fraud & Security. 2009 (12): 4–6. doi:10.1016/S1361-3723(09)70150-2.

Roberts, Jeff John (9 July 2018). "Another Crypto Fail: Hackers Steal $23.5 Million from Token Service Bancor". Fortune. Archived from the original on 10 July 2018. Retrieved 10 July 2018.

First U.S. Bitcoin ATMs to open soon in Seattle, Austin Archived 19 October 2015 at the Wayback Machine, Reuters, 18 February 2014

"Warren Buffett: Cryptocurrency will come to a bad ending". CNBC. Archived from the original on 19 March 2018. Retrieved 18 March 2018.

Sarah Jeong, DEA Agent Who Faked a Murder and Took Bitcoins from Silk Road Explains Himself Archived 29 December 2017 at the Wayback Machine, Motherboard, Vice (25 October 2015).