MUNESCO

Forum: Finance (EB2)

Issue: The establishment of scalability. security and stability of cryptocurrencies with an emphasis on Bitcoin.

Student Officer: Deniz Önalır, Defne Kaya

Position: President Chair, Deputy Chair

Introduction

"No digital currency will soon dislodge the dollar, but bitcoin is much more than a currency. It is a radically new, decentralized system for managing the way societies exchange value. It is, quite simply, one of the most powerful innovations in finance in 500 years."

(MICHAEL J. CASEY and Paul Wigna, WSJ, January 2015)

The Bitcoin protocol at its core is primarily tasked with synchronizing a ledger of transactions between different participants in the network.
Participating nodes collaboratively work to establish an agreed upon record of transactions. If there is consensus on the contents of the ledger, then in fact, there is complete agreement over the ownership of all funds.

Bitcoin bundles together the security of the currency with an incentive system that supports those who participate. Designed as a decentralized P2P system, it gains a higher level of security and stability as more resources are devoted to its operation. Thus, the rewards given to participants in exchange for their work promote the system's long term security.

Consensus mechanisms for synchronizing data in distributed systems have been known for quite some time, but Bitcoin, which was introduced by a pseudonymous creator named Satoshi Nakamoto [2008], had successfully overcome a previously unsolved challenge: How to achieve consensus in an open "permissionless" system, i.e., one in which any- one can freely partake. The ledger maintained within Bitcoin is supported by a data structure known as *the blockchain*. Each individual block is a collection of transactions that was approved by the system. Blocks are organized in a chain structure—as each block contains a cryptographic hash of its predecessor. If the system is to be secure against manipulation, records on the blockchain must become immutable after some time, otherwise transfers of money could be reversed or rerouted.

The main challenge in establishing consensus in the permissionless setting is assuring that attackers cannot launch *Sybil attacks* [Douceur, 2002] in which they freely enter the system under multiple assumed identities and subvert the pro- tocol. Such attacks are feasible since the internet at its core does not provide any verification of identity.
Conventional consensus protocols, that only provide guarantees of

security as long as adversaries do not control a sufficient number of nodes in the system are susceptible to such manipulations. 1 Subverting the protocol in this way implies that the attacker can double-spend, i.e., use money repeatedly in several transactions by reverting payments after they had already been accepted.[1]

Definition of Key Terms

Bitcoin: a type of cryptocurrency (= a digital currency produced by a public network rather than any government).

Ponzi Scheme: a way of deceiving investors (= people who give money to a company hoping to get more back) by using the money they give to pay interest to existing customers rather than investing it.

Cryptocurrency: A digital currency produced by a public network, rather than any government, that uses cryptography to make sure payments are sent and received safely.

Mining: Mining is finding a special code in your CPU or GPU that is defined by the blockchain. The problem is, the code changes its place constantly and the prize given to the founder of this code is decreasing day by day (50BTC in 2009, 25 BTC as of 2014). Decentralization is the situation of the code changing its place non-stop and prevents the user from finding it, therefore increasingits value by rarity.

Wallet: The cryptocurrency wallet is secured both with public and private encryptions; while the private encrypting keeps the money secure, the public encryption lets the wallet receive money from outside. But the difference from standard bank accounts is that the money is not actually kept on the wallet but is in a ledger.

Decentralized Currency: A decentralized currency is a currency that is not official back by any government or organization**.**

Background Information

The Bitcoin is a digital, cryptocurrency delivered as an open supply software program in 2009 by way of pseudonymous developer Satoshi Nakamoto. The Bitcoin's traits seem to make it a top candidate for global reserve forex because of its fast monetary transactions to anywhere in the global with little or no cost manipulation or export/import controls.

However, this primary candidate has its own negative aspects. The first is that virtual currencies, unregulated will be Petri dishes for corruption and cash laundering. They could wipe out decades of advances towards fraud and unlawful activities. Another critical element to don't forget is the worldwide reserves of bitcoins already with the international locations.

Bitcoin and other cryptocurrencies have enormous potential and bring in conjunction with them extensive potential for crook activities and ethical behaviors.

---

[1] *http://www.wsj.com/articles/the-revolutionary-power-of-digital-currency-1422035061*

Cryptocurrencies use cryptographic protocols, or extremely complex code systems that encrypt sensitive data transfers, to secure their units of exchange. Cryptocurrency developers build these protocols on advanced mathematics and computer engineering principles that render them virtually impossible to break, and thus to duplicate or counterfeit the protected currencies. These protocols also mask the identities of cryptocurrency users, making transactions and fund flows difficult to attribute to specific individuals or groups.

Cryptocurrencies are also marked by decentralized control. Cryptocurrencies' supply and value are controlled by the activities of their users and highly complex protocols built into their governing codes, not the conscious decisions of central banks or other regulatory authorities. In particular, the activities of miners – cryptocurrency users who leverage vast amounts of computing power to record transactions, receiving newly created cryptocurrency units and transaction fees paid by other users in return – are critical to currencies' stability and smooth function.

Importantly, cryptocurrencies can be exchanged for fiat currencies in special online markets, meaning each has a variable exchange rate with major world currencies (such as the U.S. dollar, British pound, European euro, and Japanese yen). Cryptocurrency exchanges are somewhat vulnerable to hacking and represent the most common venue for digital currency theft.

Most, but not all, cryptocurrencies are characterized by finite supply. Their source codes contain instructions outlining the precise number of units that can and will ever exist. Over time, it becomes more difficult for miners to produce cryptocurrency units, until the upper limit is reached and new currency ceases to be minted altogether. Cryptocurrencies' finite supply makes them inherently deflationary, more akin to gold and other precious metals – of which there are finite supplies – than fiat currencies, which central banks can, in theory, produce unlimited supplies of.

Due to their political independence and essentially impenetrable data security, cryptocurrency users enjoy benefits not available to users of traditional fiat currencies, such as the U.S. dollar, and the financial systems that those currencies support. For instance, whereas a government can easily freeze or even seize a bank account located in its jurisdiction, it's very difficult for it to do the same with funds held in cryptocurrency – even if the holder is a citizen or legal resident.

On the other hand, cryptocurrencies come with a host of risks and drawbacks, such as illiquidity and value volatility, that don't affect many fiat currencies. Additionally, cryptocurrencies are frequently used to facilitate gray and black market transactions, so many countries view them with distrust or outright animosity. And while some proponents tout cryptocurrencies as potentially lucrative alternative

investments, few (if any) serious financial professionals view them as suitable for anything other than pure speculation.[2]

The source codes and specialized controls that support and secure cryptocurrencies are complicated. Nevertheless, laypeople are capable of understanding the essential ideas and being educated cryptocurrency clients.

Practically, most cryptocurrencies were derived from Bitcoin. Like customary monetary standards, cryptocurrencies' express an incentive in units – for example, you can state "I have 2.5 Bitcoin," similarly as you'd say, "I have $2.50." A few ideas represent cryptocurrencies' esteems, security, and integrity.

Blockchain

A cryptocurrency blockchain records and stores every exchange and action, approving responsibility for units of the money at any given point in time. As the record of a cryptocurrency whole exchange history to date, a blockchain has a limited length – containing a limited number of transactions– that increments over time.

A cryptocurrency exchange in fact isn't settled until the point that it's added to the blockchain, which normally happens within minutes. Once the exchange is concluded, it's typically irreversible – dissimilar to customary installment processors, for example, PayPal and credit cards, most cryptocurrencies do not have built-in chargeback capacities, however some current cryptocurrencies have simple refund features.

During the lag time between the transaction's initiation and finalization, the units aren't available for use by either party. The blockchain thus prevents double-spending, or the manipulation of cryptocurrency code to allow the same currency units to be duplicated and sent to multiple recipients.

Private Keys

Every cryptocurrency holder has a private key that authenticates their identity and allows them to exchange units. Users can make up their own private keys, which are formatted as whole numbers between 1 and 78 digits long. Once they have a key, they can obtain and spend cryptocurrency. Without the key, the holder can't spend or convert their cryptocurrency.

Wallets

Cryptocurrency users have "wallets" with unique information that confirms them as the temporary owners of their units. Whereas private keys confirm the authenticity of a cryptocurrency transaction, wallets lessen the risk of theft for units that aren't being used. Wallets used by cryptocurrency exchanges are somewhat vulnerable to hacking – for instance, Japan-based Bitcoin exchange Mt. Gox shut down and declared bankruptcy after hackers systematically relieved it of more than $450 million in Bitcoin exchanged over its servers. Wallets can be stored on the cloud, an internal hard drive, or an external

2 https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/ by Brian Martucci

storage device. Regardless of how a wallet is stored, at least one backup is strongly recommended. Note that backing up a wallet doesn't duplicate the actual cryptocurrency units, merely the record of their existence and current ownership.[3]

Miners

Miners serve as record-keepers for cryptocurrency communities, and indirect arbiters of the currencies' value. Using vast amounts of computing power, often manifested in private server farms owned by mining collectives comprised of dozens of individuals, miners use highly technical methods to verify the completeness, accuracy, and security of currencies' blockchains. The scope of the operation is not unlike the search for new prime numbers, which also requires tremendous amounts of computing power.

Miners' work periodically creates new copies of the blockchain, adding recent, previously unverified transactions that aren't included in any previous blockchain copy – effectively completing those transactions. Each addition is known as a block. Blocks consist of all transactions executed since the last new copy of the blockchain was created, usually a few minutes prior.

Finite Supply

Although mining periodically produces new cryptocurrency units, most cryptocurrencies are designed to have a finite supply. Generally, this means that miners receive fewer new units per new blockchain as time goes on. Eventually, miners only receive transaction fees for their work.

This has yet to happen with any extant cryptocurrency, but observers predict that the last Bitcoin unit will be mined sometime in the mid-22nd century, if current trends continue. Finite-supply cryptocurrencies are thus more similar to precious metals, like gold, than to fiat currencies – of which, theoretically, unlimited supplies exist.

Cryptocurrency Exchanges

Many lesser-used cryptocurrencies can only be exchanged through private, peer-to-peer transfers, meaning they're not very liquid and are hard to value relative to other currencies – both crypto- and fiat.

Cryptocurrencies exchanges play an important role in creating liquid markets for popular cryptocurrencies and setting their value relative to traditional currencies. However, exchange pricing can still be extremely volatile – Bitcoin's U.S. dollar exchange rate fell by more than 50% in the wake of Mt. Gox's collapse, for instance.

Cryptocurrencies existed as a theoretical construct long before the first digital alternative currencies debuted. Early cryptocurrency proponents shared the goal of applying cutting-edge mathematical and computer science principles to solve what they perceived as practical and political shortcomings of "traditional" fiat currencies.

Cryptocurrencies technical foundations date back to the early 1980s, when an American cryptographer named David Chaum invented a "blinding" algorithm that remains central to modern web-based

3 https://www.bloomberg.com/news/articles/2018-01-18/imf-calls-for-global-talks-on- digital-fx-as-bitcoin-whipsaws

encryption. The algorithm allowed for secure, unalterable information exchanges between parties, laying the groundwork for future electronic currency transfers. This was known as “blinded money.”

After relocating to the Netherlands, Chaum founded DigiCash, a for-profit company that produced units of currency based on the blinding algorithm. Importantly, DigiCash’s control wasn’t decentralized, as is the case with Bitcoin and most other modern cryptocurrencies – DigiCash itself had a monopoly on supply control, similar to central banks’ monopoly on fiat currencies.

Wei Dai published a white paper on b-money, a virtual currency architecture that included many of the basic components of modern cryptocurrencies, such as complex anonymity protections and decentralization. However, b-money was never deployed as a means of exchange.

Shortly thereafter, a Chaum associate named Nick Szabo developed and released a cryptocurrency called Bit Gold, which was notable for using the blockchain system that underpins most modern cryptocurrencies.

However, Bit Gold never gained popular traction and is no longer used as a means of exchange.

After DigiCash, much of the research and investment in electronic financial transactions shifted to more conventional, though digital, intermediaries, such as PayPal. A handful of DigiCash imitators, such as Russia’s WebMoney, sprang up in other parts of the world.

In the United States, the most notable virtual currency of the late 1990s and 2000s was known as e-gold. e-gold was created and controlled by a Florida-based company of the same name.

At its peak in the mid-2000s, e-gold had millions of active accounts and processed billions of dollars in transactions annually. Unfortunately, e- gold’s relatively lax security protocols made it a popular target for hackers and phishing scammers, leaving its users vulnerable to financial loss. And by the mid-2000s, much of e-gold’s transaction activity was legally dubious – its laid-back legal compliance policies made it attractive to money laundering operations and small-scale Ponzi schemes. The platform faced growing legal pressure during the mid- and late-2000s, and finally ceased to operate in 2009.

Bitcoin is widely regarded as the first modern cryptocurrency – the first publicly used means of exchange to combine decentralized control, user anonymity, record-keeping via a blockchain, and built-in scarcity. It was first outlined in a 2008 white paper published by Satoshi Nakamoto, a pseudonymous person or group.

In early 2009, Nakamoto released Bitcoin to the public, and a group of enthusiastic supporters began exchanging and mining the currency. By late 2010, the first of what would eventually be dozens of similar cryptocurrencies – including popular alternatives like Litecoin – began appearing. The first public Bitcoin exchanges appeared around this time as well.

In late 2012, WordPress became the first major merchant to accept payment in Bitcoin. Others, including Newegg.com (an online electronics retailer), Expedia, and Microsoft, followed. Dozens of merchants now view the world’s most popular cryptocurrency as a legitimate payment method. Though few other cryptocurrencies are widely accepted for merchant payments, increasingly active exchanges allow holders to exchange them for Bitcoin or fiat currencies – providing critical liquidity and flexibility.

As of January 2018, many cryptocurrencies suffered a major value loss going to $10K from $19K and many of the latecomers to this market lost their investments in a short period. Despite this major blow, some economists state that Bitcoin and Alt-Coins will rise back stronger until the end of 2018.

Timeline of Events

1998-2009 - The Pre-Bitcoin years

Although Bitcoin became the first cryptocurrency that was established, there had been previous attempts to start to enterprise at developing on line currencies with ledgers secured by means of encryption. Two examples of those have been B-Money and Bit Gold, which had been formulated, however, by no means, completely evolved.

2008 - Mr. Nakamoto

A paper called Bitcoin was posted to a mailing list discussion on cryptography. It was posted by someone calling themselves Satoshi Nakamoto, whose real identity remains a mystery to this day.

2009 – Bitcoin begins

The Bitcoin software is made available to the public for the first time and mining – the process through which new Bitcoins are created and transactions are recorded and verified on the blockchain – begins.[4]

Examples of Cryptocurrencies

Cryptocurrency usage has exploded since Bitcoin's release. Though exact active currency numbers fluctuate and individual currencies' values are highly volatile, the overall market value of all active cryptocurrencies is generally trending upward. At any given time, hundreds of cryptocurrencies trade actively.

1. *Bitcoin*
2. *Litecoin*
3. *Ripple*
4. *Ethereum*
5. *Dogecoin*
6. *Coinye*

Important Organizations and Countries Involved

United States of America: The country has legalised cryptocurrencies, and recently decided to tax the exchange between coins which made the Bitcoin suffer its recent blow.

4 https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto- currency-everyone-should-read/#7726787b3f27

Bangladesh: ’Anybody caught using the virtual currency could be jailed under the country’s strict anti-money laundering laws’’ – Bangladesh Bank, 2014.

Ecuador: The government has banned digital currencies since it ‘’supports the monetary scheme of dollarization’’.

Venezuela: The country is desperately in need of its own oil-backed cryptocurrency ‘’Petro’’ the succeed for every profitable source is destroyed in country, even farming.

China: Although private parts can hold cryptocurrencies, the banks can’t.

Bibliography and Useful Sources

- http://www.latimes.com/business/la-fi-bitcoin-price- 20180117-story.html
- https://www.bloomberg.com/news/articles/2017-12-21/tax- free-bitcoin-to-ether-trading-in-u-s-to-end-under-gop-plan
- https://www.reuters.com/article/us-venezuela-economy/enter- the-petro-venezuela-to-launch-oil-backed-cryptocurrency- idUSKBN1DX0SQ
- http://bitcoinbans.com/
- https://www.bloomberg.com/news/articles/2017-12- 22/bitcoin-plummets-toward-13-000-down-more-than-30- from-record
- https://www.nytimes.com/topic/subject/bitcoin
- https://www.theguardian.com/technology/bitcoin
- https://www.entrepreneur.com/topic/bitcoin
- http://www.wired.co.uk/article/bitcoin-101
- https://bitcoinmagazine.com
- History of Cryptocurrency, by Brian Martucci