Let's Talk Cryptocoin

Yana Garipova

Spring 2018, University of Minnesota

Introduction

This is a written work on cryptocurrencies. Cryptocurrency is a child of mathematics and computer science. It is very practical on the surface and complicated from a technical point of view, what makes this topic one of the most interesting ones to work with. Extreme popularity among people and controversial feel of it make cryptocurrency one of the most exciting topics nowadays. On the other side of the coin, there are many papers and forums already published, so it would be challenging to write a unique, thought-provoking paper but worth a try.

This written work provides an overview of the original bitcoin and the ingenious technology behind it (free course for the reader). Next, the paper attempts to identify some major weaknesses of the system and briefly describe what other projects developers have done to eliminate those issues. Moreover, this text attempts to answer whether bitcoin actually works the way it was meant to and some other minor questions a reader would hopefully find interesting. Then, the paper presents a design for a new coin which would utilize Proof of Action (a certain combination of PoW and PoS), what I expect to be efficient in terms of energy conservation and even money distribution.

Due to the massiveness of the topic and the time constraints, some future work is expected for this project. It will include the actual programming and launch of the coin, analysis of its performance and modifications to improve it.

Thus, the goal of this project is to achieve a firm understanding of cryptocurrency technology and present an alternative coin idea.

Bitcoin, Litecoin, Ethereum, and what makes a coin?

The original Bitcoin and its aftermath

Bitcoin is an alternative payment system, which takes decentralization, security, and privacy as a priority.
Decentralization means there is no third party participating in a transaction, such as a bank. Since there is no bank to solve disputes, the system relies on cryptological methods to ensure that: no trust is needed between the payer and the payee, that the users stay pseudo-anonymous, and the network is efficient and secure[1].
Bitcoin system is a good competitor for the current financial system for a few reasons. First, it minimizes the quantity of information shared. That is, the payer pushes the money instead of giving the credit card information to be charged[2].
Secondly, Bitcoin system has low transactions fees, what it great advantage especially for international transfers or very small transactions amounts.
None of the Bitcoin components are actually new; people thought of these algorithms and wrote papers even 40 years ago[7]. However, nobody has created The Bitcoin before.
Below we will attempt to explore these protocols and explain why they are generating so much discussion among people and answer the question whether the system is it actually working the way it was meant to. Now, let us get into the details of how the system works.

Participants: Nodes

There are nodes, full nodes, and miners on the network. A node is a light-weight wallet that can be supported in a smartphone.
What it does[2]:
1. Assigns private keys/password and creates public keys for the client;
2. Generates the address;
3. Creates transaction messages and signs them;
4. Sends transactions to the server (full node);
5. Keeps the balance (just within the application not explicitly available for public);

Address Creation

Many of Bitcoin features are based on public/private key encryption algorithm ECDSA (Elliptic Curve Digital Signature Algorithm). Address creation is one of them[2]. Bitcoin wallet contains a set of private keys (100 of them). The public key is computed from the private key, and the Bitcoin address is computed from the public key.

The public key is computed from a private key, knowing that a private key number d is symmetrical to the public key number e with respect to the modulus n [9].

How is the address computed from the public key?

We take the public key of two integers, 32 bytes each, and add one byte to the left of it. The whole thing is our x. Then, we apply hashing functions *RIPEMD160(SHA256(x))*, which altogether is called *HASH160(x)*. It gives us 20 bytes of output and we add a Network ID (main or test) byte on the left. These 21 bytes are the first component of the Bitcoin address. Then, the same 21 bytes are being shuffled with SHA256 twice. We take 4 first bytes from that result and write next to what we already had. That gives 25 bytes of a unique Bitcoin wallet address.

Digital Signatures

Every transaction message has to be signed by a unique digital signature, such that is cannot be copied for future use and proves that the sender and only the sender authorized the transaction. A digital signature is a transaction message encrypted with a private key of the sender, thus it is always unique. Private key is multiplicative inverse of public key modulo *(p-1)(q-1)*, where $pq=n$, p and q are prime numbers and n is the modulo integer of the encryption step[9]. We know that this system is safe because n is large (must be larger than our text to be encoded written in a number format), and splitting it into primes to find the private key is a very time-consuming task even for a super computer[9].

When formed, the transaction message with its signature and the public key is passed to all the full nodes in a gossip-like manner to be verified[2]. In other words, a wallet shares this information with a full node it knows. The full node shares it with some other full nodes on the network that it knows. Even if the system is large, it does not take much time to a network to receive the information. However, this leads to another problem: if there are many transactions happening at the same time and full nodes receive them in different

orders, how do we agree which one is first? It is especially important when dealing with double spending - if an attacker creates two transactions for two people when he/she only has money for one? The original solution on that will follow after the brief introduction of full nodes on the network, miners, and their functions.

Participants: Full Nodes

Every full node includes the functions of a wallet, plus, they hold the history of the entire network's of transactions and verify the validity of the new ones.
They need to check that all the transactions are indeed authentic: they take the digital signature of a transaction and decrypt it using the public key of the sender to see if it returns the original transaction message. Full nodes also check if a transaction is not double spent by counting all the inputs/outputs of that address using the old records. Full nodes also check many other things according to Bitcoin restrictions[4].
In other words, full nodes are servers that communicate with light-weight clients and other servers. Full nodes are important and needed for the network[6]. Bitcoin offers software which one can freely download in order to turn their computer into a full node. Though it comes will all the data of all the transactions ever made, what is space consuming, there are some features to deal with it:
https://bitcointalk.org/index.php?topic=1377345.0
https://bitcoin.org/en/release/v0.12.0wallet-pruning)

Participants: Miners

The Miner nodes compose the blocks from the transactions they received and solve them, i.e. find the hash to store the information[2]. (By the way, miners are just people who bought a piece of hardware and keep it plugged in and running). They need to find a random number nonce by brute force, such that *SHA256(previous block id, the current block's transactions, nonce)* gives a certain number of leading zeroes[1]. In other words, they have to find an input for a given output and it takes about 10 minutes on average. In other words, what miners do is to append to the blockchain. Miners' activity keeps the network running, so they get awarded by the system with a few bitcoins and transactions fees from the block they solved. Since the awarded number of bitcoins they get decreases twice every four years, sooner or later miners' only profit will be the transactions fees. Thus, transactions fees are creating an

incentive for miners to keep mining and prefer transactions with a higher fee to include in the block over the cheaper one.
Consequently, mining ensures that distribution of the new money in the system is even, the transactions are put in order, and the network is active.

Blockchain

The blockchain is called this way because the new block's hash depends on the previous block. Once a block has been solved, it is broadcast to the full nodes for confirmation[1]. Once it has been confirmed, it is added to every node's ledger. At this point, the transaction is in the blockchain and has become a history.

Even though the blockchain system was originally designed for the purpose of cryptocurrency, it is recognized as an ingenious system and now is being implemented to other projects, such as maintaining of the common database between different companies [10]. It is mostly blockchain's merit that makes enthusiasts believe that cryptocurrency is the currency of the future. Why is this so?

Because the Blockchain is a stunningly secure system, that does not let to make any changes to a block: if you want to hack a block, you have to hack all the blocks in the chain before that one, which is practically impossible. If you decide to hack the first block, then in order to succeed (with your evil plan), you have to build new blocks way faster than the rest of the network and win the race. This works because of another important part of the Bitcoin system: the Proof-of-Work.

Proof-of-Work

Appending a new block to the blockchain requires a lot of CPU power. There is a competition between the miners on the network, such that miners try to solve different blocks containing possibly a few of the same transactions. If two pools of miners solve different blocks at the same time, the blockchain forks. The practice shows that one subchain will grow faster than another one. The entire bitcoin system is based on the notion of Proof of Work, i.e. trusting the longer chain. The original bitcoin paper[1] states that the network is secure as long as the honest nodes have the majority of CPU power, thus the honest chain will be the longest. If an attacker does get hold of the major-

ity of power somehow, then he will make you read this engaging conversation: https://bitcoin.stackexchange.com/questions/658/what-can-an-attacker-with-51-of-hash-power-do
Since there are many people mining at the same time, driven by the incentive to receive the reward and support the network, but not all of their work gets accepted, a lot of extra energy simply goes to waste. Thus, the Proof-of-Work system is highly unsustainable[2], what might provoke dislike towards the system in modern American society.

Is there anything else to it?

Even though bitcoin is a well thought system, it has dark sides, some of them were mentioned before. There are many skeptical opinions about the bitcoin, and some of them are very reasonable.
First question is, why do we need this new system?
The crypto coins provide great security (no more credit card theft) and, as mentioned above, their transactions fees are up to 10 times cheaper than the banks' ones, what is a big advantage, especially for international transfers. However, using applications like Venmo with certain banks, one can transfer money with no charge. Also, assuming we do not count every 20 cents, what are the other differences between the current banking system and the bitcoin?
Cryptocurrency is a decentralized system ran by all the users, when applications like PayPal or Venmo are run by a company. Cryptocoin supporters claim that decentralized technology does not have any regulations that could be implemented by a company. In other words, the cryptocurrency system has no censorship[2]. With a crypto coin, people can purchase anything that is sold with the crypto coin. Furthermore, as fearsome as it sounds, bitcoin income is untraceable and easily tax avoidable. This makes people think of bitcoin as "dirty coin"; it makes governments implement harsh regulations like in China or Indonesia...[7] Due to its features, Bitcoin is considered controversial among society. But in fact, the bitcoin does not provide any new offers in particular; what we are all afraid of has been bought and sold for years with cash.
Another argument supporting the bitcoin system is that the decentralized technology has a lower chance for internal abuse. However, according to this article[3], despite the idea of decentralization, the majority of bitcoins is owned by a minority of people, what allows them to control the price. Even though the percentage changes every 10 minutes, the previous statement will remain true

for quite awhile. As price instability is one of the major disadvantages of the bitcoin, a little more about it will follow later.
Despite the ingenious system behind it, Bitcoin has many other complications, such as:
1. Proof of Work is not sustainable;
2. Bitcoin language has a strict protocol, for example, it uses no "for loops" and has many other limitations.
3. Privacy. Bitcoin is not fully anonymous;
4. Bitcoin price is highly unstable.
Let us see what people have done to deal with these issues.

1: Proof-of-Work vs Proof-of-Stake: Other Coins

As mentioned before, the Proof of work is unsustainable. Amount of energy consumed by PoW every year equals to about 7 percent of Niagara Falls' energy[2]. For that reason, another method called Proof-of-Stake has been proposed. In PoS, voting depends on how much coins you have. *SHA256(previous block id, current time, unspent output)* is less than miner's coin balance times the difficulty[2].
Even though this process is a good idea in terms of energy consumption and no need for mining hardware, PoS originally had other complications. For example, the more money you have, the easier it is to mine. Thus, the new money distribution is very uneven. Also, with PoS it is very easy to build multiple branches, what requires trust and makes the system a subject to attack. By now a significant amount of work has been done to improve the Proof of Stake. For example, NXT is a platform that successfully implements Proof of Stake in their blockchain[2]. It also allows users to create their own tokens. People have also thought of combining the two methods. For example, Peercoin is a hybrid of PoW and PoS. It uses both PoS to save energy and PoW to reach consensus. Distributing money using PoS is called minting and the creators of Peercoin plan to completely replace mining with minting.
There is also an idea of delegated proof-of-stake and the creators claim this is the best way to reach consensus ever found[5].

2: Programming and Protocol Limitations Issue: Ethereum

Ethereum is a platform where a new coin/decentralized system "contract" can be written and tested. This platform does not have limitations like bitcoin does

in terms of programming and memory storage. Ethereum has its own coin - Ether. It uses proof of work to validate transactions. Differently from Bitcoin, Ethereum nodes keep the balance for other nodes, instead of going through transactions and counting balance every time[2].

3: Privacy: Other Coins

Bitcoin is not fully anonymous since the records of all the transactions is available to anybody and we can track ownership of bitcoins. If someone finds out that a certain address belongs to you, they can see all your history of transactions. There is a coin Monero that improves it. Monero uses bitcoin's system to check a transaction for double spending, but then deletes links of ownership assosiation[2].
For more exciting solutions, the reader can turn to Coin join or Zerocash cryptocurrencies.

4: Price Stability: Other Coins

Price fluctuation is one of the greatest flaws in the system of bitcoin. Many cryptocurrency enthusiasts would agree that price fluctuation is just a sign that something else is wrong[7], for example,
- percentage of ownership of bitcoins, as mentioned before;
- lack of faith in the currency (there is an opinion that the whole system is a fraud).

To address the issue, people came up with great projects. For example, there is a coin Digix - it is run on the Ethereum platform. 1 token is backed up with 1g of real gold and two-way exchange is possible. This is a great idea, probably the best stability we can get. Another coin called Tether is backed up with 1 dollar, (which in turn is also backed up with gold). It is connected to a bank account in Hong Kong, what does not eliminate 3rd party as the original bitcoin proposed.
Another smart solution for stabilizing price is NuBits. This coin is not backed up by anything. The server creates more Nubits if demand exceeds supply (price of goods high = price of coin low) and burns coins otherwise. This is probably the best solution proposed so far.

Other Coins

The Bitcoin is the original project, that inspired all other cryptocurrencies. Thus, they all share the same neat idea of privacy, security, and decentralization.
There are already over 100 different coins with unique goals/ideas and this number is growing. [https://coinmarketcap.com/] I would like to describe some other coins that especially stand out.
Litecoin is very similar to the Bitcoin, but it has certain differences. Its maximum number of total coins is planned to be 84 million instead of 21 million, though that would not affect the usage and pricing in general[11]. Litecoin uses a different hashing algorithm instead of SHA256, called Scrypt. Also, Litecoin processes a block much faster, what made it a very successful coin[11].
Banana Coin runs on Ethereum platform and its price backed by 1 kg of bananas per token. The main idea of Banana coin is to make people invest in the banana plantations and improve the supply of Lady Finger bananas in China. Even if it slightly sounds like a joke, it also shows a great example: cryptocurrency does not have to be thought of as something dark or illegal. On the contrary, it could be directed towards greater good.

Idea

Despite a large number of already existing coins, there are lots of ideas for new implementations. For example, if there was a coin that would "meet in the middle" between the secure, peer-to-peer system and the government control, it would dissolve the dark myths and clean the cryptocurrency's name. However, I believe the prices fluctuation and complex, energy-wasting mining process are the biggest concerns, so I will try to minimize these issues in my Y-coin.
Nubits is indeed a great idea to deal with price fluctuation. There are other options though. For example, what if the coin was assigned to online goods and services, such that it does not have to be exchanged with regular money? In that way, it can really be decentralized with minimum of 3rd party influence. For example, I can photoshop your picture for 3 tokens. If you want some tokens, earn them. Although it will not work hundred percent: people can still buy it from each other or just stop spending trying to save. How do we know? Well, this idea is not new. History knows examples of local barter tokens. For example, "My Sitter Circle" is an application simulating similar idea. People

will exchange tokens for watching over their kids. Of course, in this case, there is a lot of trust present and this is not a cryptocurrency, but it could be. I would like to implement this idea with the Y-coin. Theoretically, if there are many services available for different prices, it is less likely that the network will get stuck. The advantages are that you do not have to invest or lose money, only your precious time and services.
Many people claim how unsustainable the Proof-of-Work is. People proposed the Proof-of-Stake, which still has issues and is being under development. Delegated Proof-of-Stake is similar to democratic voting, involving witnesses. It is quite complex to implement. I would like to implement Proof-of-Action in the Y-coin. It is similar to Proof-of-Stake only the mining depends not on how much coins you have, but how active you are on the network. This algorithm is meant to simplify the mining, which does not require any special hardware or transaction fees (until all the money has been released)! It also ensures a fair new money distribution.

Y-Coin

A simple version of a coin could be simulated using socket networking on Unix or using a prepared platform, like Ethereum.
There is a server(full node) and a client (simple lightweight application).
Clients must be connected to a full node to communicate about the changes. Full nodes also include wallet function "local client." For a bigger network, a full node must be connected to some other full nodes to communicate, a feature of all cryptocurrencies. Client performs the wallet's functions:
1. Generates my address;
2. Creates transaction messages;
3. Signs them;
4. Keeps the balance;
5. Sends the transactions to the server it knows; 6. Receives the messages from the full node.
A server/ full node:
1. Receives transaction messages;
2. Validates them;
3. Broadcasts them to the other full nodes to validate;
4. Calculates its own and other full node's it knows activity record.
Then full node selects the best candidate it knows and shares with other full

nodes; if the new candidate from other node is better, then the full node takes it instead. Once all the nodes agreed on the candidate, that node will be able to create a block from transactions it received then mine it. The miner will get a reward in accordance with the bitcoin system, i.e. sooner or later the coin will have a limited amount. Once the block has been broadcast and added to the chain, the candidate's activity record resets.
The system needs to make sure that new users have as much chance as the old ones and it should not matter how much money they have. Thus, the activity record should depend on: how many light-weight wallets the node is connected to, how many transactions the full node received from these wallets, how many hours it spends by working as a server.
To summarize, first, with Y-coin you do not have to connect it to real money, it is supposed to be a token for different web services. Second, it utilized Proof-of-Action to reach consensus, which does not require mining hardware or transaction fees (at least in the beginning.)

Future Work

Any cryptocurrency project is an ambitious one, especially designing your own coin. Due to time constraints and massiveness of the topic, this project has a great opportunity for future development. Next, I would like to write the Y-coin server and client programs, test them and work on further improvement in terms of security, privacy, and price stability.

Inspiring Reading

Please contribute to bitcoin:
https://bitcoin.org/en/bitcoin-core/contribute/

All other coins are here:
https://coinmarketcap.com/

Can Full nodes shut down computer? How many of them does the network need? The answers are here:
https://bitcoin.org/en/full-nodewhat-is-a-full-node

Proof-of-Work vs Proof-of-Stake:
https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

Easy example of blockchain technology used in other system than cryptocurrency:
https://dzone.com/articles/why-do-we-need-blockchain

About all the blocks on the network and much more:
https://blockchain.info/

What if an attacker gets hold of most of the CPU power on the bitcoin network?
https://bitcoin.stackexchange.com/questions/658/what-can-an-attacker-with-51-of-hash-power-do

Conclusion

The Bitcoin's algorithms are not new, but it has "boomed" and changed the world. Apart from being a popular topic and activity, Bitcoin's technologies, especially blockchain, have been recognized and used in other areas of business. However, as anything revolutionary, the Bitcoin has its dark sides too. Price fluctuation, non-sustainability of network, intractability, and complicated design have earned the Bitcoin its skeptical opinions among people and governments' desire to restrict it. Bitcoin's strengths also created many enthusiasts of cryptocurrency, who developed other projects like crypto coins, platforms, and alternative algorithms. There are over hundred coins that deal with one or another issue, and I also decided to design a Y-coin and optimize it in terms of price stability and sustainable way to reach ordering consensus. Since the idea is very massive and ambitious, it has a great plan for future work. The plan includes writing the actual code, testing the network, and its further improvement.

References

[1] Bitcoin: A Peer-to-Peer Electronic Cash System. 2009

[2] Driscoll, S., Introduction to Bitcoin and Decentralized Technology. *PluralSight Courses*, 2016

[3] Suzuki K., Bitcoin Trap. *Money Voice*, 2018

[4]Developer Documentation. *Bitcoin Project*, 2018, bitcoin.org/en/developer-documentation.https://bitcoin.org/en/developer-documentation

[5]Delegated Proof-of-Stake Consensus.*Bitshares.org*, 2018 https://bitshares.org/technology/delegated-proof-of-stake-consensus/

[6]Running a Full Node.*Bitcoin Project*, 2018. https://bitcoin.org/en/full-nodewhat-is-a-full-node

[7]Odlyzko, Andrew. "Cryptocurrency Talk." 26 Apr. 2018.

[9] Garrett, P., *Cryptology and Number Theory.* Prentice-Hall, ISBN 0-13-030369-0.

[10] Sarfarz., A. Why Do We Need Blockchain? *Database Zone*, 2017.

[11] Fernando, J., Bitcoin vs Litecoin: What's the Difference?. *Investopedia*, 2018