Technical Analysis of the Blockchain and the Cryptocurrency Market

Viktor Bakayov
viktor.bakayov@student.uva.nl
University of Amsterdam, The Netherlands

January 10, 2018

Abstract

The emerging of Bitcoin open a whole new field - decentralized applications (DApps) and smart contracts. The underlying technology - the blockchain provides the fundamentals (security, trust, immutability) for defining, pushing forward and shaping the Smart Economy. The technologies are in active research. Novel approaches emerge for achieving consensus and ways of decentralizations. Currently, the biggest issue is how to scale such networks for enterprise and world-wide usage. Unfortunately, due to the hype about blockchain the money invested in such technologies surpass way much their actual advancement. Nevertheless, the new projects emerging every day can have a great impact on the society and can redefine the IT industry. This analysis is to explore the current technology advancements in blockchain and give overview of the most popular and promising cryptocurrencies.

1 Introduction

Today, the cryptocurrencies are gaining popularity with every day. While still the average person have a very limited knowledge of cryptocurrencies, banks, governments and many companies are aware of its importance and are actively researching them, release papers or are about to start so-called blockchain-projects.

Cryptocurrencies emerged as a side product of another invention - the bitcoin. It's unknown creator, Satoshi Nakamoto, never intended to create a currency, moreover digital cash, but he wanted to solve something that many before him failed. He wanted to build a decentralized peer-to-peer digital cash system, with no server or central entity that prevent double spending. However, to solve this one usually would have exactly a central authority (a server) to declare the correct state of balances, keeps track of transactions etc. Satoshi Nakamoto manage to achieve consensus without such central authority with the so-called blockchain. His success gave the birth of cryptocurrencies.

The blockchain paved the road for a new way of crowdfunding - An Initial Coin Offering (ICO), and the creation of decentralized applications. There are numerous applications such as fraud reduction, distributed storage, smart contracts, payments, trading platforms, managing digital identities and many more which take advantage of the blockchain characteristics and build on it. No matter what the project's goal is it would create its underlying crypto tokens, that are not just the currency used in the network, but they are a unit of its business model. We are sitting at the dawn of a new economy as there are more than 1300 cryptocurrencies with a total market cap of more than $746 billion dollars as of 9th of January 2018 [19]. Three years ago most blockchain projects were just replicas of bitcoin, or clones. Today, however it is a totally different environment and we have many projects that are beginning to solve real-world problems.

The purpose of this paper is to analyze the cryptocurrency environment, the top few projects and what is their product, but also emphasize on how they utilize the blockchain and/or the underlying network.

2 Blockchain Specification

The blockchain is a distributed, immutable, public ledger, which records transactions between different parties in a secure, efficient, verifiable and permanent manner. The blockchain has 4 key properties: Trusted, Verifiable, Traceable and Reproducible. The trust is achieved by mistrusting single ill-behaving nodes but trusting the collective whole. A high redundancy value decreases the changes that a malicious group could manipulate results, but comes with a performance penalty. The blockchain is verifiable and allowing the interested parties to check if the data source is really the entity that it claims to be (signed transactions) and that the published data was not altered (data hashes as part of the transaction). The blockchain also allows to trace a transaction back to the origin, and if needed to reuse or reproduce each step.

2.1 Blocks and Transactions

The blockchain can be characterized by two kinds of records: blocks and transactions. It holds the history of all transactions in the network and they are publicly accessible via some blockchain explorer. This gives unique transparency but does not hurt security. Each block holds various number of valid transactions and among other things, a reference to the block (in form of a hash) that came immediately before it. Each block has to have one predecessor and one successor. The linked blocks form a chain.

2.2 Transaction Validation and Consensus at Large Scale

In order to generate a block all transactions and blocks must be validated, an important procedure to prevent ¨double spending¨ and correct balances. The validation is done by achieving consensus, a sort of an agreement, between the participants in the distributed system. Once the validation is done a new block is created and added to the blockchain. Currently, this is done through several methods all employed by different blockchains.

2.2.1 Proof of Work (PoW)

The Proof of Word method tries to find an answer to a very difficult and computationally expensive mathematical problem which is unique to each block. This is done by a process called "mining". Each miner (the entity performing the computation) tries to guess a valid hash value. For the further analysis, we would take the Bitcoin network as a typical representative of the Proof of Work approach. The hash function in the bitcoin network takes as parameters various block header properties: the block version number, a value called 'hashMarkleRoot' which is a hash of all transactions in the block, the timestamp of the block, the hash of the previous block, a value called 'nounce'. The 'nounce' is a completely random number between 0 and 2 to the power of 31 which is brute forced in order to luckily find a hash smaller than the target hash, which is calculated based on the difficulty. When the miner successfully guesses it is appended to the hashed contents of the block, and then rehashed [12]. If the hash meets the requirements set forth in the target hash, then the block is added to the blockchain and broadcasted to all other participants. The validity of the newly created block now can be effortlessly verified by other miners and the transactions inside will be approved. Miners' incentive is the award of newly-mined bitcoins or transaction fees for successfully finding blocks. However, approaches which rely on economies incentives poses fundamental problems, as if there is a less financial gain for the participants the network improvement may be stalled or prevented. In addition, PoW suffers two fundamental disadvantage - waste of energy and substantial confirmation latencies (minutes or tens of minutes) making PoW both expensive and time-consuming.

The collective computing power of the miners provides security and trust to the Bitcoin. Hashing the information gives the very useful property that if a single entity is modified, it would result in a completely different hash. As the ledger is replicated and distributed over the miners, tempering only one blockchain version will not be enough and so would be rejected by rest of the network. For one to successfully temper with a transaction, one should control more than half of the network for the modification to be accepted (51% attacks). In addition, the attacked should successfully beat all others to propose a modified (not-valid) version of the chain. If an attacked desires to make a modification of a transaction in previous mined block (not last), he would need to change the transaction's block and furthermore mine all future blocks in be the first to mine the last block in order to propose the malicious version of the chain. As the network grows and more participants are included this is practically infeasible in commercial deployments and ultimately the blockchain is considered very secure. However, the 51% attack is assuming zero latency, but on working conditions is 49.5% on the bitcoin network and even can go down to 33 % . To beat such attacks the PoW systems should have high operational costs, as costs of attacking the system (acquiring 51%) are almost equal to what is spent to run the system. Thus high security can only be achieved with high operational costs - a fundamental PoW flaw. In addition, networks can be counter intuitively highly centralized. In bitcoin network a 51% attack can be successfully done by just controlling 3 of the biggest mining pools (22% AntPool; 18% BTCPool; 15% BTCToop) [20].

The mining difficulty is periodically adjusted to ensure that block generation occur at about 10 minutes as a precaution to ensure that the network is not flooded with conflicting (but valid) blocks. As the whole process is competition, between all miners and mining pools, who will find the next block first and collect the reward, they add more and more hashing power and so the mining difficulty is increasing ever since. The constant hardware increase and the fact that finding the correct hash is a computationally intensive procedure, have rendered the PoW method as extremely inefficient in energy consumption. The Bitcoin's current estimated annual electricity consumption is 32,56 TeraWatt Hour(s) [23], which is what more than 159 countries consume in a year [24]. Another comparison would be that the electricity required for a single bitcoin trade could power a house for a whole month [21]. However, this is still less than the gold mining (132 TeraWatts).

2.2.2 Proof of Stake (PoS)

While in PoW the creator of the new block will be the first miner to successfully mine the block, in Proof of Stake the creator is chosen in a deterministic way, depending on his wealth. There are several significant advantages over the PoW. First, the electricity consumption is greatly reduced as there is no need for the participants to run the hash procedures in order to secure the network. Because of this, there is also no need to generate new coins in order to motivate the participants to stay in the network and therefore there is no block reward, the creator will only take the transaction fees and in some cases more coins as reward. The processes is referred as 'minting'. The rewards and the posted collateral ensure a compliance with the protocol, but some protocols also have additional penalties. In PoS the risk of centralization is reduced as economies of scale are much less of an issue, discourages centralized cartels from forming and acting in ways that are harmful to the network, and the security is improved because it makes various 51 attacks more expensive [25]. Also, PoS algorithms can address scalability problems more easily (the concept of "sharding"), see Section 5. A fundamental undesirable implication of this approach is that the richer accounts will gain wealth much faster, ultimately making the rich richer.

In this method, a set of validators take turns proposing and voting on the next block, and the weight of each validator's vote depends on the size of its deposit (i.e. stake) [25]. There are many variations of consensus algorithms and reward distributions, but if we are to look from an algorithmic perspective, there are two major types: chain-based proof-of-stake and Byzantine fault tolerance (BFT) style proof-of-stake. In the first, a validator is pseudo-randomly selected for a given time slot and assigns that validator the right to create a single block on top of the current longest chain. In BFT proof-of-stake the validators are assigned the right to propose blocks,but through a multi-round voting process, they agree on whether or not any given block is part of the chain.

PoS based consensus algorithms are susceptible to ¨nothing at stake¨ attacks. In the case of a fork, whether that was accidental fork by having two valid blockchain versions, or in an attempt to rewrite history and reverse malicious transactions, the optimal strategy for any miner is to mine on every chain, so that the miner gets their reward no matter which fork wins. If we take the scenario that 99 % of the miners work on one version and the same 99% work on the other version we can have the clever 1 % person who decides to put his transaction in one of the version and wait for it to get confirmed to buy something. Then he would put his 1 % to the other blockchain which does not have the transaction or send the transaction to address that he controls , effectively double spending the money. Because now the second version has 100 % it will win over. A solution is to penalize the miners who act maliciously, for example working on several blockchain versions. Such nodes will be reprimanded and their stake will be reduced. Now they have something to lose.

2.2.3 Proof of Importance(PoI)

The proof of importance is somewhat similar to Proof of Stake, but still it has some important differences. In PoI each account is given an importance score that proxies its aggregate importance to the network, meaning it is taken into account how much an account transacts with others and with who the account transacts. This algorithm is implemented into the NEM network and they argue the people who actively help the economy and the NEM benefits will get the rewards, not only those who have higher stake.

The NEM coin uses an approach called vesting to build up trust in the network. In order for a person to be able to harvest a block, he would need 100,000 vested balance. Vesting is the process of building up value over time. In a 24h time interval, 10 percent of the account balance become vested. For example during the first 24h none of the coins are vested, after 24h 10 percent of the balance is vested, next 24h 10 percent of the unvested balance will become vested and so the cycle continue as long as the coins are kept in the wallet.[18] Having a greater vested coin value means either you have held your coins for a while or you have a very large amount.

Accounts with higher importance scores have higher probabilities of harvesting a block. if we are to compare with PoS, a key difference is that the account balances give larger weight to fewer nodes, whereas importance scores have less noticeably larger nodes, meaning much more even wealth distribution. Also while the vested balances are monotonically increasing, the importance scores are non-monotonic, demonstrating that accounts with lower balances are able to gain higher salience (i.e importance) in PoI than in PoS and also PoI gives less salience overall to richer accounts than PoS. [11] This contributes to giving similar opportunities to everyone as they main goal is to empower the regular token holder.

2.2.4 Proof of Work by Cooperation

For this approach, we would take the Neo blockchain as a case study. Neo currently implements a Delegated Byzantine Fault Tolerance (dBFT) algorithm for consensus. In this algorithm, the nodes which validate the transactions are called bookkeeping nodes. Participants are able to designate bookkeeping nodes but certain requirements should be made, such as having special equipment, dedicated Internet connections, and a certain of amount of GAS, a network dividend to Neo. If two-thirds of the nodes on the network can agree with a bookkeeper's version of the blockchain, a consensus is achieved and the proposed version of the blockchain is validated. If consensus fails, an alternate bookkeeper is called and the process is repeated.[8] The network as a whole consumes fewer resources and can handle higher transaction volumes. However, the NEO network was criticized to be too centralized as only 7 nodes participated the validation, ran from the development team. Many view this kind of centralization to be counter-intuitive to the purpose of the blockchain. NEO's team argues that a decentralized model can still be built around this system by allowing the community to vote in the validation (bookkeeping) nodes.

Recently the City of Zion (CoZ) (an independent, international group of open source developers working on NEO blockchain) proposed a new approached - validation by coopetition. NEO will begin its decentralization by allowing well known commercial projects and communities to run consensus nodes, forming an initial confederation of actors with a strong interest in guaranteeing the security and success of the network. With this approach it can be ensured that all participants are equal in the network by design. Their power won't depend on how much money they have, or how cheap their electricity may be.

The taken approach is to conduct a rigorous vetting campaign to choose 7 initial consensus nodes. Some of the requirements would be to provide outstanding availability and excellent performance, rigorous security protocols, availability in case of emergency maintenance or that entities and the organizations behind them to be legally liable.

Once 7 consensus nodes are run from 7 different entities, then the voting process may begin to add additional nodes in order to increase the fault tolerance. Relatively big amount of GAS must be staked to be certified for the nodes to vote you in. These nodes will be run by people of different nationalities using different service providers in different countries and under different operating systems. This means that no jurisdiction, service provider or software flaw can affect the failure limit of the network. This approach could be the new standard as it eliminates the major PoW and PoS disadvantages as each entity is dedicated to increase the value of the entire blockchain, and if they don't or misbehave, or are offline they can be easily voted out. This approach allows for verifying and validating the participants and ensuring they are in fact who they say they are.

2.2.5 Stellar Consensus - SCP Quorum Slicing

The Stellar coin employs a method called federated Byzantine agreement (FBA) and uses stellar consensus protocol (SCP) that builds on the FBA in terms of its memberships list.The SCP protocol have the four key properties for consensus: decentralized control, low latency, flexible trust, and asymptotic security. For details, please refer to [1]. SCP uses open membership where everyone can join, rather than determined membership list. FBA achieves robustness through quorum slice — individual trust decisions made by each node that together determine system-level quorums. The key difference between a Byzantine agreement system and a federated Byzantine agreement system (FBA) is that in FBA each node chooses its own quorum slices [17]. There is no central authority, and each node decides which other participant they choose for information. Good quorum share nodes and lead to quorums that overlap. If two quorums are disjoined they can independent agree on two contradictory statements and undermine consensus. Each note is responsible for making good choices, which goes down to ensure that the slices are large enough and that the notes they contain are important enough not to risk their reputations by lying.

Reaching consensus goes through several voting steps. First, a node goes through initial voting showing its openness to the possibility of accepting a certain outcome. That node will not accept an outcome contradiction the one agreed, however, it might end up accepting something else if enough of other notes vote otherwise (peer pressure). Due to quorum intersection, slices influence one another and can lead to accepting an outcome which is different than initially voted. This is due to a blocking set of nodes, which contains at least one node from each of the node's slices and so it can block action in all quorums that contain the node, ultimately causing the node to accept a different outcome. When every member of a quorum votes to accept one particular outcome, the quorum ratifies this agreement. Confirmation messages are the final step of the voting process and imply system-wide agreement. This messages may convince additional nodes to accept the outcome, and no matter what events subsequently transpire, every responsive, accurate node will accept the statement. A system will agree on a statement only if sufficient messages are delivered and processed. The SCP protocol solves the main challenge - the risk of the system getting blocked and losing liveness. It is possible to neutralize blocked statements if they get stuck in the voting process with a ballot-based approach [17].

3 The Gap and Issues

Still, there is a huge gap between Blockchain and real business market. ICO is engulfing this gap by market capitalization, meaning there is a lot of money pouring into the technology, but yet the technology is not ready (see Figure. 1). Vitalik Buterin, the founder of Etherium and a blockchain pioneer, stated: "Need to differentiate between getting hundreds of billions of dollars of digital paper wealth sloshing around and actually achieving something meaningful for society". Hopefully, in the second half of 2018, this gap will close by already mature technology/strategy and start its big commercial adoption. Currently, the crypto market is desperate to get in on the ground floor of the first asset that actually gets used for something on a massive scale.

As every controversial and not yet proven technology the discussions whether it will succeed is ever growing. According to the CEO of JPMorgan, Jamie Dimon, the only digital currency that will see mainstream adoption are those which are government backed and there will be no real non-controlled currency in the world. He clarifies that the blockchain technology will develop, but the decentralized nature of cryptocurrencies will not last. [22]

Apart from project which goal is to scam people, there are now concerns of "unrealistic" projects. Such projects does not have strong fundamentals, don't have good tech or are just unrealistic. Might be remarkable tech on paper but the realization of it a whole new story. They would eventually run into a wall that they can't quite overcome. And the problem is that a lot of them have money. It is hard to fail, when you loose few millions per year and you have $1 billion of capital.

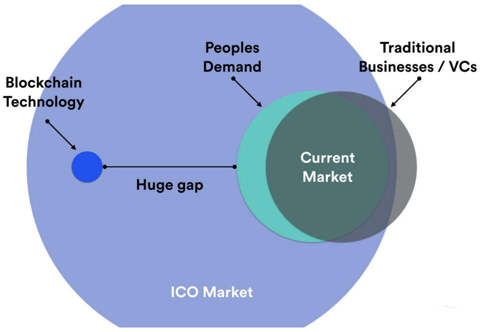

Figure 1: The Gap Between Technology and Market Needs

4 Smart Contracts

A smart contract is a set of instructions, terms, conditions and rules which reside in the form of a code on the blockchain and that everyone involved agrees. It a formal agreement between two parties, much like a normal contract, but rather than being written and interpreted by legal entities, it is written in code and being interpreted by computers. Due to the immutability of the blockchain one can be sure that the contract will execute exactly as coded - therefore no breach of agreement/contract can exist. The blockchain will execute transactions after the involved parties have executed their promises, and therefore such a system eliminates mistrust.

Numerous application can be created following the same model, for example providing rules for fair gambling and betting, or exchange of non-digital assets such as oil, real estate and gold, or move funds in accordance with instructions given long in the past. The initial plan was to build a separate blockchain for each particular application, but as described this would require a lot of resources to maintain and validate the blockchain. With smart contract and the rules defined inside, one can define the functionality of a blockchain, and run it on an existing smart contract blockchain. On that networks, many applications are running simultaneously.

4.1 Smart Contract Platforms- Ethereum and Neo

4.1.1 Ethereum

The leading and most developed decentralized application (DApps) that runs smart contracts is Ethereum. Writing smart contracts on the Ethereum network is done with the Solidity programming language. Its goal is to simplify the language of smart contracts, but also many consider as a disadvantage as one have to learn a new language. The Ethereum network showed that decentralized application (dApps) is feasible and it is the new decentralized future. Today there are around 900 dApps [16]. In the beginning of December 2017 the first semi-popular smart contract - *CryptoKitties* (a game similar to Pokemon) congested the Ethereum network leading to longer conformation times and increase the pending transaction queue to the 20k-30k transaction range [7]. Currently, Ethereum uses proof-of-work based consensus algorithm with a plan to run a proof-of-Stake consensus algorithm called Casper to solve many of the current problems.

Casper will mainly address the current scalable issues, ¨nothing at stake¨ problem and will disincentivize censorship. This means if a miner loses a block, the other miners won't benefit (as in PoW), but rewards for everyone are highest if everyone can participate in the validation. Casper favors availability over consistency (CAP theorem) and also have harsher incentives. A validator will be penalized (by reducing its stake) for being offline, and have strong enforcement that he would follow the rules.

4.1.2 Neo

The alternative commercial ready platform is Neo. There are two aspects of the difference between the two - technical and economic model. The Neo dBFT consensus algorithm is very fast. Currently, it takes 15 seconds to generate a block (even can be tuned to go faster- 5s, 3s), resulting in being able of processing 1,000 TPS with 10,000 TPS potential. For comparison, the VISA network can process 45,000 TPS. The Ethereum network can handle the modest 15 TPS. Also, the NEO has a very good finality. Depending on the risk model, usually exchanges wait for several or few hundred confirmations for the transaction to be accepted, but in NEO just one is enough. Also, the Neo contracts can be written with a mature programming language, such as C#, Java, Python, JavaScript, Kotlin and more, with plans to support C, C++, GoLang. A compiler will compile the code to a bytecode and run it on the NEO virtual machine. This is my opinion is a big plus, as most of the developers can write smart contacts without the need to learn a new language. The dBFT and the smart contract contributes to a much faster transaction per second rate and to a greater scalability. Also, currently the tools for debugging and testing smart contacts are lacking, however, NEO provides major support for debugging at Neo VM level.

With Neo the economic model is different. Neo uses two tokens and separates stake and utility. By holding Neo , you are holding a stake in the blockchain, you can vote for joining the consensus process or how much the transaction fee should be. By holding GAS token you can pay for the utility- deploy a smart contract, pay for a transaction, network fees etc. When you need to pay for some utility, you don't need to reduce the percentage of your stake. There are scenarios when use of chain (performing many transactions) have the negative impact of diluting the user stake, and possibly reducing the weight of the stakeholder's vote. As NEO has good fundamentals, it still have a lot to catch up.

4.1.3 Smart Contract Security and Exploits

Smart contracts are pretty difficult to get right. Testing and certifying smart contract is an important part of the underlying ecosystem. Several security breaches happened so far. The DAO (Decentralized Autonomous System), which goal was to codify the rules and decisionmaking apparatus of an organization, was the first big breach in the field. 3.6m Ethers were stolen, worth 72 million dollars at the time (20 $ per token), and 2,7 billion now (750 $ per token). The smart contracts code is usually publicly available, making it possible for everyone to look for exploits. The attacker exploited a function called ¨SplitDAO¨ which was vulnerable to the recursive send pattern. The problem was that the function updates user balances and totals at the end, so if we can get any of the function calls before this happens to call SplitDAO again, we get the infinite recursion that can be used to move as many funds as we want [2]. The attacked moved the coins to a child DAO, which had the same structure as the DAO. Because of this, he could not withdraw any funds for 28 days, as that long was the funding period. A critical update in the form of a soft fork was done locking out several addresses, preventing moving any Ether out of the DAO or its children. Essentially, this seals the Ether into the addresses for all time, and they can never be claimed. A hard fork was proposed in order to restore and give back the tokens back to the DAO investors. Eventually, it was decided to hard-fork the blockchain. As this was controversial, having miners and investors supporting both versions, this lead to break Etherem into two separate active blockchains (Ethereum and Ethereum Classic), each with its own cryptocurrency.

On 20th of July, a breach was done on the Parity Multisign Wallet and allowed an attacker to steal 150k ETH (30M USD). The account was used to store funs from past token sales. The way the contract was written was to extract the constructor method into a separate library and the wallet contract would forward all unmatched function calls to the library. This causes all public functions from the library to be callable by anyone, including *initWallet*, which can change the contract's owners. However, the *initWallet* had not checks to prevent to be called after the contract was initialized. The attacked exploited this by called this method via transaction and changed the owner of the contract to an address controlled by him. A subsequent transaction was issued transferring the tokens by invoking the ´execute´ function. later that year, yet another hack was performed locking out 514k ETH ($155M). The Parity contract is from two parts, one of which contains the majority of wallet logic and is deployed only once. It is acting like a dependency, or like a library, for when creating a new wallet by a second lightweight contract. The hacker (who claims to have done this accidentally and to have no intention to do so) similarly acquired ownership of the library contract and invoked the ´kill´ function which destroyed the contract and rendered all dependent contracts completely unavailable. It is unknown whether the person issuing the transaction was a hacker or a developer who accidentally destroyed the contract, but in any case he performed two transactions, making this ´killing by accident´ story less likely. There is no way to unblock the funs without another hard fork.

5 Blockchain Scalability Issues

Undoubtedly, the biggest issue and field of research currently is how to scale the blockchain being able to validate thousands of transactions without compromising the security or the decentralization. There is a decentralized, scalability, security (DSS) trilemma, much like the CAP theorem, but nobody has officially proven this. The main scalability issues in the cryptocurrencies are the time taken to put a transaction into the block and the time taken to reach a consensus. We discussed how miners in PoW are incentivized to include the transaction in the next block and the more advanced consensus algorithms which partially solve the problem. Here we discuss other approaches which can be taken to scale. A summary of the scaling effort is in the table below.

Upgrade	Description	On/Off Chain	Scaling Improvement
Increase gas limit	Miners increase gas limit	On-chain	2-8x
Parallel Process Transactions	Transactions can be processed simultaneously instead of one by one	On-chain	2-8x
Proof of Stake	Changing consensus algorithm from Proof of Work to Proof of Stake	On-chain	2-5x
Payment channel networks	Parties exchange signed transactions off chain, allowing infinite transactions with only an initial and closing transaction on chain	Off-chain	10-100x+
TrueBit	Off-Chain smart contract computation/ execution through a verification game	Off-chain	10-100x+
Plasma	Tree hierarchy of blockchain where only fraud proofs are reported up the tree	Off-chain	10-100x+
Sharding	Validators only need to validate some, not all, of the network's transactions	Off-chain	10-100x+

Table 1: Scaling Techniques

First, we are to briefly describe the scaling effort on the Bitcoin network. Two solution have been proposed. First is to increase the block size from 1 Mb to 2 MB, which will lead to more transactions fitting in a single block. The disadvantage, as viewed from the miners eyes, is that a low blocksize limit encourages higher transactions fees and also will eventually require higher fees for fast confirmations. That is miners have to interest to increase the block size. The second solution is called Segregated witness (SegWit). In this proposition the transaction signatures are moved towards the end of a transaction, reducing the size a transaction taken on a block. As a result more data can fit in a block than the maximum block size. The block limit would effectively increase from 1 MB to around 4 MB (70%). The Segregated Witness suggestion was activated through a soft fork in August 2017. The 2 Mb block size advocates argued that this is not the easiest approach and there was a lot of uncertainty if this is safe or not. The community was split on how to scale the bitcoin and that was a long time debate. After the New York Agreement (NYA) where a lot of community people met, it was decided to proceed with a compromising agreement called "Segwit2x". That is a combination of the two proposed solution, essentially stating to first adopt Segwit and than double the block size. The idea was first abandoned due to not enough supporters as the original signatories of the New York Agreement weren't comfortable with the hard- fork coming so soon after SegWit's activation and because of lack of consensus, but was eventually revived and forked at block number 501451 on Dec. 28 2017. However, there is still an ongoing dispute which version to call itself bitcoin (old vs new), and it is the community and miners who will decides which one is the "real" bitcoin. Currently the new version goes by the name "SegWit2x [Futures]". This is not the first hard-fork performed on the Bitcoin. There are now 5 popular versions of bitcoin: Bitcoin, Bitcoin Gold, Bitcoin Cash, Bitcoin Diamond and SegWit2x, but the list is extensive and goes to 14 hard-forks as of December 2017.

There are few notable efforts made to scale up. First in the table above is Ethereum based and suggest to increase the gas limit of a block. This would increase the total number of transactions per block, as miners can only add transactions whose gas requirements add up to something which is equal to or less than the GAS limit of the block. A massive speedup can be achieved by having separate payment channels network, performing several micropayments on them and recording only final/important part of it on the main chain. That is - state channels, a mechanism in which operation that would normally be done on the blockchain get conducted off of the block. The transaction capacity would increase and the fees will decrease. Making a payment will be done instantaneously because only few transaction are required on-chain, and the bulk of transaction will be off-chain without fees. Lighting network [10] will be designed for Bitcoin and Raiden p2p network [14] is the Etherium analogy. Such architectures are refereed as "layer 2". They are both in early development phase. Such services are intended to be free, however a small fee may be introduces because someone needs to host, facilitate this second layer. Another, issue is that it erodes the decentralized operation of these coins.

Similarly, like using state channels, TrueBit [15] uses a layer outside the blockchain to do off-chain computations to enable scalable transactions among Ethereum smart contracts [6].

The Casper algorithm (the Ethereum update) is going to implement a new technique called "sharding". A transaction is broke down into shards and nodes work on individual shards side-by-side. Each shard only processes a small part of the state and does so in parallel [6]. Next to the main chain, there will be running a shard chain. The advantage is that only a small pieces of proof of collations (transactions are wrapped into collator, similar to a block) have to be recorded on the main chain. In addition, the validators only have to verify the shard they are watching for [9]. For more details please see [9].

On-chain transactions take a lot of resources of the network and take the most time to process. Nearly all scaling solution rely on the idea to switch from a model where all transactions hit the ledger to a model where only part of the transactions are recorded. The bulk is done off-chain (often with a side chain or hierarchy of chains on top of the main chain), or that users can privately exchange messages which cryptographically sign the transfer. Often transactions are to be grouped and batched before being communicated to the blockchain and often transmit only the final result to the network as one transaction.

6 Decentralized Application, Platforms, and Solutions

The blockchain opened a new realm and unlocked a new technology sector. Its first implementations - the Bitcoin showed the concept is solid and surpassed everyone's expectation. Now there are many blockchain projects which try to solve real problems and have a practical use and applications. In this section, we are to discuss the most popular projects and the ones which can have the greatest impact on the society.

6.1 Bitcoin

Bitcoin paved the way for the cryptocurrency world, with its revolutionizing decentralization 10 years ago. However, the constant research and the fast technology development have rendered the Bitcoin obsolete technology. Now it is considered to have high latency (more than 10 minutes for first confirmation, up to an hour to be certain) and poor scalability (max. of 7 transactions per second). The network recently has suffered from increase transaction fees. The fee is varying and it is dependent, on how fast you want to confirm your transaction (in best case to be included in the next block), but the average transaction fee on 21st of December 2017 was 55 $ [4].In comparison, if you would make the same transaction on the same day via the Litecoin network (another cryptocurrency) it would take 1.43 $ [5] with an average block time of 2 minutes.

Bitcoin was more like proof-of-concept project that even its creator did not anticipate to gain such a popularity. There are two main reasons why the bitcoin is still the king of the cryptocurrencies. First, is that it is constantly boosted by the mass media, and with the ease the common person can stake his money, lured by the idea of quick and easy money, he would do it first on Bitcoin, simply not knowing that there are many more coins. The second reason is as first coin, the Bitcoin is massively adopted by the exchanges, making it possible to buy other alt coins with bitcoins only. However, the trends have become to shift now. Exchanges are opening fiat pairs (USD and EURO) and the bitcoin dominance has dropped from around 85 % in February 2017 to under 35 % as of December 2017 [13]. My opinion is that bitcoin will (hopefully) slowly fade and make room for the new better generation projects making 2018 a year of transition.

6.2 Ripple

Released 2012, Ripple goal is to provide secure, near free and instant global transaction without any size limitations with no chargebacks. The network is very fast, payments settle for 4 seconds, and handles 1,500 transactions per second, with the possibility to scale to handle the same throughput as Visa (50,000 transactions per second, as of July 15, 2017). The Ripple off-chain transaction processing system is called "Payment Channels". The Ripple uses a "Byzantine Consensus Algorithm" known as the "Ripple Protocol" for validation and consensus. The validation notes are more than 55 and they represent some of the top enterprise hosting providers in the world, such as Microsoft, MIT, and CGI. The use of the Ripple token (XRP) is completely optional, but rather the XRP holding incentive the company to make the product as useful as possible.

Unlike other altcoins, Ripple was recognized as a legal tender by several governments. Although there are no major banks using it yet, the SEB Swedish bank settled $180 million on the Ripple Blockchain [3].The market value of Ripple as of 2d of January is more than 83 billion dollars. Still, banks are reluctant to invest in blockchain technologies. But Ripple is an enterprise-ready solution, and maybe it is just a matter of time for the transaction payments to become digital, instant, universal and almost free.

6.3 Monero

Monero adds on existing cryptocurrency design by obscuring the amount of every transaction made as well as the sender and the recipient.The system utilizes ring signatures to maintain the sender's privacy. In a ring signature design, several decoy outputs are created alongside the real output. any of the decoys is as likely of being an output as the actual output because of which any unintended third party (including the miners) won't be able to know who the sender is. For more on link signatures please check - [27].

Since every transaction has a unique key image, the miners can verify against double spending by simply checking it out. Monero has transaction unlinkability, nobody but the sender know that the recipient is receiving the coins. A one-time public key is generated from the public view key of the recipient and the public spend key. Then a one-time public address called "stealth address" is generated from the one-time public key. When the recipient is scanning the blockchain for his transaction he uses his private spend key and then he can calculate a private key which corresponds to the one-time public key and collect his Monero.

So far we described how the sender and how the recipient is kept anonymous, but what about the transaction itself? Ring Confidential transactions were use that essentially hides transaction amounts in the blockchain. Since the value is not known, it is now not possible to be aware of any particular transaction. [28]

6.4 SiaCoin

Sia coin is decentralized network of computers, which taken together, comprise the world's cheapest cloud storage platform. It's goal is to provide fast,reliable and cost-effective service with incentivized storage. According to the website storing 1TB on Sia costs about $2 per month, compared with $23 on Amazon S3. What distinguished Sia from other decentralized storage solutions, like *Storj* and *MaidSAFE*, is the ability to create a smart contract to ensure the host is paid for their services (in the form of Sia coin), even if the client does not access their files. The files are encrypted, so that only they can access them, as well as they are highly replicated to ensure the client can access the file even if the host if offline. On the other hand, those contracts allow for punishing misbehaving hosts. For each minute their provided storage is offline, their balance will be reduced. Everybody can join to the sea network with few terabytes of storage and become a host. The profitability of being a host highly depend on the market evaluation of the coin and the demand for storage space on the network. For example, 6 TB of storage can earn around 10 $ per month.

6.5 IOTA, Raiblocks

There is new type of cryptocurrencies gaining popularity in the recent months, namely those of fast, feeless, minerless cryptocurrencies. IOTA and Railblocks are the most promising at the moment. Because of their fast transaction conformation and high throughput they are a great use case for machine-to-machine micro transactions in the IoT space. Their unique architectures address the scalability issues with the current blockchains and are advertised as "unlimited scalability". Both are "pre-mined", meaning their ledgers start with certain amount of coins and will never change.

IOTA

IOTA transaction validation uses a "pay-it-forward" kind of system. In order to put a transaction on the IOTA network, the client must perform heavily computation on two previous transactions on the network. The algorithm takes between few seconds to few minutes depending on the GPU hardware. Once the proof-of-work is successfully computed, your transaction get broadcasted over the network, where in turn will be confirmed by other participants. Once there are enough confirmations, the transaction will be deemed valid. In theory, the more transactions that occur over the network, the faster your transactions get confirmed. In IOTA rater then the transactions being attached to a blockchain structure, they are attacked to a directed-acyclic-graph (DAG). A core feature is the ability to securely transfer data through the DAG, making it possible to have secure and authentic channels between devices. The creators advocate numerous use cases with the tangle (DAG) architecture, but just one is trusted e-Voting. For only several days, the project gained massive market cap (close to 11 billion as of January 2018). For details about the tangle and the IOTA project please check the IOTO white paper: [30].

RaiBlocks

Railblocks operates on a peer-to-peer architecture they call “block lattice". Essentially, they have one block chain for each account which is controlled by the account’s private key, that is only they can add to. Each block chain is replicated to all peers in the network. Balances are modified through send and receive blocks. Transferring funs is by creating two blocks: one receive block on the recipient’s blockchain and one send block on the sender’s blockchain. Users do not have to be on-line to receive funs, as once a user access his wallet any outstanding funds will be automatically signed.

Users send funds by creating two blocks: one send block on their personal blockchain and one receive block on the recipient’s blockchain. Users receive funds by “pocketing” any outstanding receive blocks into their personal blockchain. Users do not have to be on-line to receive funds. When the nodes sync, the consensus algorithm runs through the ledger to ensure that the cryptographic signature on the “send” and “receive” blocks are authentic.

The network has no central authority to manage the transactions. To prevent double spending, in the infrequent case when the network has to make a global decision, there is a balance-weighted vote to determine the outcome. Since not everyone can remain on-line a representative (someone with high balance value) will be chosen to act as a "representative". For details, see the White paper: [26]

6.6 Overview

In the cryptocurrency field everyday new projects are emerging out of the blue. Some are just mirroring and copy already existing projects but some bring something new to the table. The projects can be categorized into several categories, each with few subcategories. Please check Figure. 2 [29]. We are to briefly go through each category:

- **Currencies**: Most projects try to build a better currency with the intention to represent either a medium of exchange, unit of account or a store of value. In this category fall the project mentioned: Bitcoin, Ripple, Monero.

- **Developer Tools**: Other projects are used as building blocks for decentralized application. Such projects are Ethereum and Neo or ZepellinOS for secure contracts. Protocal design around scaling and interoperability are very hot topics. We mentioned projects such as Plasma and Lighting Network. The field is driven by providing all the necessary components for building a fully decentralized autonomous application and improving the network scalability, security and reliability. The dApps development stack comprises of few main layers: computation (Etherium, TrueBit), file storage (Storj,Sia), external data(Oracles- Augut), monetization (some token model), payments (state channels, Ox). TenX is a project that allow to convert and spend the virtual currencies in real life through a bank card. This deal with a common misunderstanding that you can’t buy real objects with virtual money.

- **Fintech**: As the proliferation of cryptocurrencies is ever increasing the need of exchanging one unit of currency for another is growing. Decentralized Exchanges are filling this niche. But also they can be lend (SALT) or accepted as an investment (ICONOMI).
- **Sovereignty**: The projects in this category provide the functionality necessary for a world where users aren't forced to trust in any individual or organization but rather in the incentives implemented through cryptography and economics.[29] For example, Civic provides secure ID Identification without multi-factor authentication such as a username, password, third-party authenticator, or physical hardware token but rely on the blockchain and biometrics on the mobile device.
- **Value Exchange**: A key design of the blockchain is to provide trust to parties which have no relationship or trust between them. This allow to exchange goods/services/storage/ computation/bandwidth/energy without a middleman (the necessary evil up to now to maintain order and trust), which will lead to lower costs. A notable examples are: Streamium (broadcast videos and charge the viewers), Filecoin and Sia (lend, share data storage), Golem (share computer power), Gridcoin (rewarding volunteer distributed computing), Steem (publishers to monetize content and grow community).
- **Shared Data**: This category is about collecting and sharing a lot of data by the numerous participants in the network. Then the data can be annotated, build different models and extract insights from it . FOAM project (in the same field as IOTA) allow you to track custodianship and provenance of items on a supply chain or in the IoT space to pay between devices such as drones that negotiate use of air space, or autonomous cars that pay for road usage. Similarly, Sweetbridge tackle down commerce, supply chains and interest-free loans.
- **Authenticity**: The immutability of the blockchain ensured that the data written to it hasn't been modified or tampered with. Therefore the digital assets can represent real-world goods (like train tickets) or data. Using blockchain for sensitive data, or markets for goods susceptible of fraud ensured the user of the item's integrity. Factom is a project to preserve, ensure and validate digital assets, and GUTS is the blockchain platform for honest tickets.

7 Conclusion

We might be entering a new era and the next iteration of the Internet - fully efficient and digitized society. Although, increased number of fraud projects was observer, there are still many which are destined to change the way we operate. Many ideas will fail, but only successful project on massive scale is needed to show the full potential of blockchain and the power of decentralization. The cryptocurrency field is yet to disprove the ill-believers and gain mainstream integration or will be drag down by major security breaches, strong government regulations or for unexpected reasons. Nevertheless, the underlying blockchain technology and decentralization approaches is real tech. and will find many applications in different fields.

References

[1] The stellar consensus protocol: A federated model for internet-level consensus. https://www.stellar.org/papers/stellar-consensus-protocol.pdf, 2015.

[2] Analysis of the dao exploit. http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/, 2016.

[3] Seb-new payment solution with blockchain technology. https://sebgroup.com/press/news/new-payment-solution-with-blockchain-technology, 2016.

[4] Bitcoin avg. transaction fee historical chart. https://bitinfocharts.com/comparison/bitcoin-transactionfees.html, 2017.

[5] Bitcoin, ethereum, litecoin, dash avg. transaction fee historical chart. https://bitinfocharts.com/comparison/transactionfees-btc-eth-ltc-dash.html, 2017.

[6] Blockchains don't scale. not today, at least. but there's hope. https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a, 2017.

[7] Cryptokitties: why the ethereum blockchain is congested. https://medium.com/eidoo/cryptokitties-why-the-ethereum-blockchain-is-congested-ecb219fd0fe0, 2017.

[8] Delegated byzantine fault tolerance (dbft). https://hackernoon.com/what-is-neo-and-what-is-gas-5b9828a1aa65, 2017.

[9] Ethereum sharding: Overview and finality. https://medium.com/@icebearhww/ethereum-sharding-and-finality-65248951f649, 2017.

[10] Lightning network. https://lightning.network/, 2017.

[11] Nem technical reference. https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf, 2017.

[12] Nonce. https://www.investopedia.com/terms/n/nonce.asp/, 2017.

[13] Percentage of total market capitalization (dominance). https://coinmarketcap.com/charts/#dominance-percentage, 2017.

[14] Raiden network. https://raiden.network/, 2017.

[15] A scalable verification solution for blockchains. https://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf, 2017.

[16] State of dapps. https://www.stateofthedapps.com/, 2017.

[17] A summary of the stellar consensus protocol white paper. https://medium.com/a-stellar-journey/on-worldwide-consensus-359e9eb3e949, 2017.

[18] Vesting nem. https://blog.nem.io/what-are-poi-and-vesting/, 2017.

[19] Cryptocurrency market capitalizations. https://coinmarketcap.com/, 2018.

[20] Hashrate distribution - bitcoin. https://blockchain.info/pools?timespan=4days, 2018.

[21] businessinsider. The electricity required for a single bitcoin trade could power a house for a whole month. http://uk.businessinsider.com/electricity-required-for-single-bitcoin-trade-could-power-a-house-for-a-month-2017-10, 2017.

[22] O. Capozzalo. Jpmorgan chase ceo: All crypto will be government controlled. https://cointelegraph.com/news/jpmorgan-chase-ceo-all-crypto-will-be-government-controlled, 2018.

[23] Digiconomist. Bitcoin energy consumption index. https://digiconomist.net/bitcoin-energy-consumption/, 2017.

[24] D. Galeon. Mining bitcoin costs more energy than what 159 countries consume in a year. https://futurism.com/mining-bitcoin-costs-more-energy-159-countries-consume-year/, 2017.

[25] GitHub. Proof of stake faq. https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ, 2017.

[26] C. LeMahieu. Raiblocks: A feeless distributed cryptocurrency network. https://raiblocks.net/media/RaiBlocks_Whitepaper__English.pdf, 2017.

[27] R. Mercer. Privacy on the blockchain:unique ring signatures. https://arxiv.org/pdf/1612.01188.pdf, 2016.

[28] S. Nother. Ring confidential transactions. https://eprint.iacr.org/2015/1098.pdf, 2015.

[29] J. Nussbaum. Mapping the blockchain project ecosystem. https://techcrunch.com/2017/10/16/mapping-the-blockchain-project-ecosystem/, 2017.

[30] S. Popov. Ioto white paper: The tangle. https://iota.org/IOTA_Whitepaper.pdf, 2017.

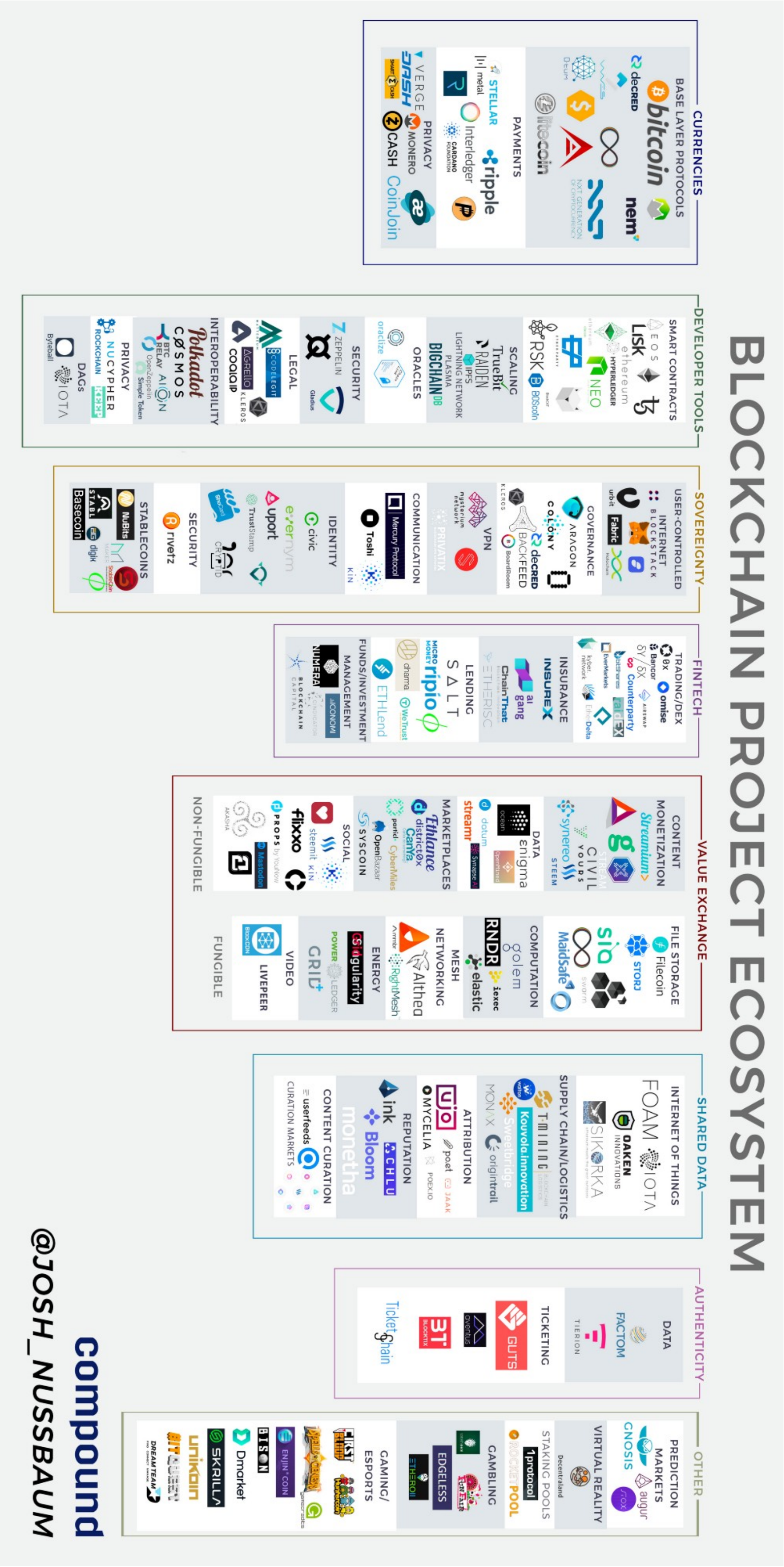

Figure 2: Blockchain Project Ecosystem