Blockchain, a Small Techie Overview

Romain Claret
romain.papers@protonmail.com
1st September 2016

Abstract. Blockchain is more a buzzword than a framework. Most of the people think to understand it or part of it, then propagate their beliefs to the people without any understanding of it. As a result, it ends up categorized as some mystical technology that nobody understands because of the propagated misunderstandings. This paper will try to help to overview what is Blockchain and help you to make your opinion about it.

1 Introduction

Everybody heard of it or even pronounced the name at least once, and almost everybody has their personal understanding of it. Blockchain is Bitcoin; Blockchain is Ethereum; Blockchain is safe; Blockchain is anonymous; Blockchain is destroying the finance industry; Blockchain is the next big thing; Blockchain is a lifestyle, etc. In the end, what the heck is it? Short answer: all the above claims are *true*. Blockchain is a framework to process any form of decentralized transactions, and its part the **digital censensus** family. However, in our case, we will overview the technical aspect of the framework so that you can get a techie point of view about it. I won't go into too many details on the subject of digital consensuses, or what are in my opinion on today's privacy paranoia. I will just invite you to read my other papers treating those subjects. I should also say that most parts of this paper are coming from a research paper I am also the author of, which ended up into a Project named **Overclouds**, whose goal is to create an anonymous and decentralized internet data sharing service right through the browser.

2 Is blockchain worth it?

It is important to note that with the incoming quantum computers (predicted to appear wildly in about twenty years [2030ish]), the security, the anonymity, and the mining structure must change from todays perspectives. As for today, the blockchain technology is at its hype, meaning that we see it as the best thing in the world. However, from now the hype will decrease, and maybe a new technology will emerge, or the blockchain technology will evolve or reshaped to go in a direction we do not expect yet. **Yes**, from todays perspective, the timeframe is pretty significant, it is worth the interest.

3 Whats next in crypto-currency?

As of today, considering that the technology of blockchain will not change, and is still in use for crypto-currency, it could take three types of path.

3.1 One of the paths

A neverending death and birth of crypto-currencies. Indeed, once the mining is no more profitable, the security sharply decreases because miners are verifying the transactions and are playing the role of consensus for validating transactions. Miners are mining as long as the devices allow a profit (power consumption, device rentability, etc.). Best case scenario, the hardware technology continues to involve, as well as the required computational power. (Note that we are currently brute-forcing the solutions.) Moreover, based on the model of crypto-currency of Satoshi Nakamoto, Bitcoin, at some point in time, the maximum amount of coins will be reached, and the network will not generate coins (rewards) anymore. At this point, the only income of the miners will be the transaction fees. If the transactions fees are not high enough to motivate the miners to continue mining (and verifying/validation the operations), the currency will die due to the lack of security. So the miners will move to new profitable crypto-currencies (note that they could have an advanced hardware for mining at this point, which will help them to start pretty well).

3.2 The second path

A constant source code adaptation of the original crypto-currencies to make it compliant with the market evolution. For example, increase the maximum amount of coins, make public keys quantum proof, etc. Indeed, currently, the **ECDSA**[11] is not quantum proof, which is the current hashing algorithm (we have already SHA3[8] which is quantum proof, just to be safe). The problem is ECDSA, which during a transaction sends the public key, and theoretically, a quantum computer can guess the private key from it. However, the address is still secure because it is the hashed public key. However, the second path is **killing** the concept of a stable currency based on expendable raw material stock, and the social and economical results are pretty hard to define. A secondary question would be about the creation of raw material from nowhere? What will happen, if tomorrow, we find a new gold mine, which holds the same amount of gold already retrieved (doubling by this mean the maximum quantity of gold available), and with a retrieving difficulty level a lot decreased, so it becomes again profitable to mine?

3.3 The third path

A crypto-currency under the control of its creators. I am looking strongly toward Ethereum here. They created a lot of rumble into the blockchain community by taking the decision to hard fork the chain after the DAO hack. They went into a dangerous road by applying a third party power over transactions meant to be ruled by the consensus. For me, at this stage, they have shown me that they don't have the same values than me about unalterable consensus driven transactions. The DAO hack was not possible because of Ethereum's core or blockchain architecture; it was a problem coming directly from DAO's smart contract. I will end on this, in my opinion, the hacker played with the consensus rules. In the real world, if someone makes a mistake, the mistake cannot be undone, we can find fixes for it, but at the end, *it have to be part of the history.*

4 Predicted evolution in blockchain

Smart-contracts, as described in 1997 by Nick Szabo [18]. It only needed the technology to hold the structure, and with the help of blockchain this concept came to life with the first version of **Ethereum**[20] (2013a) and more recently (2016) the Homestead version of Ethereum [6]. The particularity of Ethereum is that it uses the currency as fuel to run smart contracts on the EVM (Ethereum Virtual Machine) using the power of each node on the network to do a calculation, and creating a consensus on the output. This technology evolution has allowed, for example, a startup company named *Slock.it* to create an alternative currency called *DAO* that allows IoT (internet of things) devices to interact with the crypto-currency. It allows, for example, to control a lock, in a hotel. The door could be then locked until a client paid the door to open. It's interesting to note that for DAO all the coins are already available, the interest here is to let people trade a defined amount of raw material, without the ability to create new.

4.1 What is next then?

To answer shortly, I don't know yet. I think that it hard for anybody to make a claim in this area. In my opinion, I would say, an IoT-based blockchain with an embedded digital consensus. You can read more about this in another paper I made. However, again, it is personal.

5 How blockchain verifies transactions?

We have currently three *famous* protocols to verify that identity A can do an operation to identity B. But of course, other protocols also exists, and a lot still have to be found and described.

5.1 Proof-of-Work

The most famous and used today, introduced with Bitcoin, read as PoW[7, 10]. This protocol is aiming at reducing the risks of DDOS attacks and family abuses by requiring that the clients/nodes have done some computational work (processing time and power) before validating a transaction. It was a solution developed mainly for our financial world. Without going into too many details, the client has to find via brute-force a password for the transaction, which was randomly generated by the network.

5.2 Proof-of-Stake

What is a stake? It is globally something that holds. In our case, it is more like a flag that can keep a land (a claimed property).

Read as PoS[12] . Usually, in blockchain PoW, miners validate the transactions that came first depending on their CPU power. Note that the more CPU power you have (GPU, FPGA, ASIC, etc.) the larger is your influence. POS is the same thing but with different paradigms: In one of them, Stakeholders validate with

something they own (raw material as an internal currency). Moreover, in a simple manner, everybody has a certain chance (proportional to the accounts balance) per amount of time of generating a valid raw material. Another paradigm would state that we are not working with the amount of raw material owned, but with their age (for example, the raw material is multiplied by the time that it was unused) which gives a weighting factor. However, with this paradigm, a collision attack[21] (using several alternated copies to create a new copy) is pretty important, because we could have a super linearity by accumulating aged raw materials. There are other different types of approaches but we will not details them all because they are not the best of consensus algorithms. (elitism, identity, excellence, storage, bandwidth, hash power, etc.)

Ghost Protocol From the full name, Greedy Heaviest-Observed Sub-Tree protocol, introduced by Yonatan Sompolinsky and Aviv Zohar[17], it allows the PoW consensus to work with much lower latency than in the blockchain protocol from Satoshi Nakamoto [16], and of course keeping it secure. Indeed, in blockchain based PoW, a miner is rewarded for each block found so the other miners can continue to mine on top of it. However, when a miner produces an orphaned block (a block that exists in the chain), they are not rewarded for their work, plus the consumed power was in vain because the work is unused by the consensus. Here comes the solution, Ghost, which includes orphaned blocks. It introduces the notion of rewarding orphaned blocks to miners and increasing the security of the consensus with increased validations of a block in the blockchain.

Casper Now there is a friendly ghost in town; it is Casper[5]. This protocol is based on Ghost and is planned to be included into Ethereum for the Serenity[4] release (final), however, the Metropolis version must go out be- fore. We should also note that they released the Homestead version on 14th March 2016 (about a month before this Report release). It will work on the smart contracts.

Now, on the security side By using raw material (sort of digital assets) defined by the consensus PoS avoids a Sybil[9] attack. Which is a technique where the attacker is trying to compromise a system by creating multiple duplicate or false identities. It is resulting into including false information, which as a result can mislead the system into making not intended decisions in attackers favor. By the way, PoW protects itself against a Sybil attack by using computational resources that exist in an extra protocol. However, in PoS traditional approach, we have two major problems. The first is Nothing-at-Stake, and the second are Long range attacks.

Nothing-at-Stake The principal problem is that smart nodes have no discouragement from being Byzantine[13]. Indeed, signatures are very easy to produce, and they will not lose any tokens for being Byzantine. Another problem is that nodes with digital assets could never spend. A solution to this would be to have a security layer on deposits, which would cancel Byzantine deposits. To achieve this, we would need to store information about nodes and their immoral behaviors (which are decided by the consensus), so the consensus would be able to punish them. Now, this works only if the transactions are not hidden (with the

proof of malicious actions). Also, we should note that this security layer would ask more power for the consensus during the use of punished accounts. And slowing down the consensus is not acceptable because it acts as the authority and by this mean should be the cheaper to operate in power. Punishing the attackers with power consumption is fair. Compared to PoW, where attackers are not receiving compensations for their computational power (which is a disincentive). The PoS security layer is trying to disincentive attackers by removing their digital assets. It could be an interesting social experiment, however, in our humans economic point of view, attackers should be well disincentivized.

Long Range Attack In this type of attacks, the attacker controls accounts with no digital assets and is using them to create competing versions of transactions. This attack is touching both traditional PoS, and the deposit security layer (as long as authentication ends in the genesis block). The solution here would be to force nodes (and clients) to authenticate the consensus (for example with its state) by signing with the nodes that have something at stake currently, and nodes must have an updated list of nodes with deposits. It is usually called the *weak subjectivity* method [1].

PoS vs PoW? PoS compared to PoW is much cheaper to secure, and the transaction speed is greater. We could also note that it could be the stepping stone into *scaling the blockchain technology.*

5.3 Proof of Activity

The protocol from Bentov, Lee, Mizrahi, and Rosenfeld [3] which is implemented into PeerCoin (and its clones), is considered as a hybrid of the PoW and PoS. The nodes are doing PoW work by mining blocks and at the same time with the PoS (meaning that the blockchain includes both types of blocks).

The procedure

- The PoW miner mine.
- Once a block is found, the network is notified and creates a template. (multiple templates are possible)
- The block hash is used to find random owners by using its hash as numbers to determine owners (nodes from the network).
- Turn by turn each chosen owners sign the key with the key of the block. If a chosen owner is unavailable, the process paused. (it is not a problem this concurrently miners are still mining and generating new templates with different owners)
- At some point in time, blocks will be signed, and the reward will be given to the miner and the owners.

Continues data exchange To reduce the data traffic, each template does not include a transaction list during the signing process itself; it is the last owner (signer) that is adding it when creating the block.

6 Attacks on blockchain

Blockchain is designed to be controlled by the consensus of nodes. It means that it can not be owned nor controlled by a third party (in **my** definition at least). Until now this goal has been achieved. However, experiences showed that the system is not perfect.

6.1 The 51% attack

Most interesting way (in a social experiment point of view) of rewarding for the attackers. Indeed, if the attacker controls at least 51% of the consensus, it is possible to manipulate transaction by validating malicious transactions. Pool owners can do this. Note that as it is today (for actives crypto-currencies), it is no more possible to mine on your own and be profitable, miners are forced to join pools and distribute the work and rewards between them. Meaning that it creates a vicious circle, the more miners are in a pool, the more power it has. The more power it has, the more reward are generated. Finally, this results in attracting, even more, miners because they also want a bigger and easier reward for mining, which leads to the security risk of malicious pool chiefs who will control the currency and the transactions. All around the internet people are always saying that it is dangerous, in fact, they are asking others to stop making a profit for the good of others, which is a selfish human thinking. Can't wait to see it as a case of a figure.

6.2 Spam attacks

The idea here is to make many transactions to the victim's wallet (to its address), paralyze the legit transactions and by this mean its incomes. Indeed, the network will have to process all the spam transactions as well as the legit transactions, meaning that the delay is added before receiving the legit transactions. In some cases, like for Wikileaks[19], which is depending on this kind of funding to live, it is pretty bad. Plus, since many transactions appear in a block, its value increase and miners will jump on it to get the reward, meaning that the legit transactions are a bit behind because they have a lower reward. However, usually, the current crypto-currencies have an anti-spam solution. They have a minimum fee, and they increase the fee after each new transactions.

6.3 DDOS on exchange platforms

The profit behind this type of attacks is to either steal wallets or ask a reason to release the servers. The crypto-currency is only affected by the depreciation of its value in "real" money because they are not able to trade, and they are more likely to switch to another exchange platform or currency.

6.4 Developers

Ethereum proved that the developers of a blockchain solution have the power to apply a third-party power over the network, and rule the transactions by using hard forks. What I mean is that human factor is a stake here, a right amount of money for someone could make the difference.

6.5 Special dedication to Mining malwares

It is funny to see that hacking is evolving with the hype. Instead of having zombie computers doing nothing waiting for DDOS attacks or whatever they are used to, they are now mining coins (generally connected to a pool). How smart is that? I think that this is amazing!

7 Blockchain != Digital Consensus

I will end this paper with a point that is important for me. Blockchain is **not** *the* digital consensus, but is *a* digital consensus. So many people are misunderstanding this part, and it drives me nuts!

The blockchain technology is being very popular nowadays; it sometimes can put eye cups on our field of decisions.

Blockchain have indeed proved that it works as a consensus. However, a consensus with highly fault tolerant networks and overcome the Byzantine (Two Generals Problem) is not something that only blockchain have.

For example, Maidsafe[14] uses another technology to obtain a consensus[15]. Instead of using the whole network to validate a transaction, they give the consensus role to a random group of nodes.

7.1 Comparing

They both have pros and cons of course.

- blockchain
  - Pros: Shared global record of all transactions.
  - Cons: The speed. The chain can be gigantic (Bitcoin more than 105GB at the moment), and the file must be synced between all networks nodes[2].

- MaidSafe
  - Pros: Bandwidth speed limitations only. Low data storage consumption.
  - Cons: Small groups of nodes are playing the role of consensus for transactions. Nodes could never be aware of transactions that happened elsewhere if they are not related to them at any point in time.

References

[1] Proof of Stake: How I Learned to Love Weak Subjectivity - Ethereum Blog.

[2] Ayeowch. GLOBAL BITCOIN NODES DISTRIBUTION.

[3] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld. Proof of Activity: Extending Bitcoins Proof of Work via Proof of Stake. 42(240258):1–19, 2013.

[4] V. Buterin. Slasher Ghost, and Other Developments in Proof of Stake, 2014.

[5] V. Buterin. Understanding Serenity, Part 2: Casper, 2015.

[6] DR. GAVIN WOOD. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER HOMESTEAD DRAFT. 2015.

[7] C. Dwork and M. Naor. Pric-

ing via processing or combatting junk mail. *Advances in CryptologyCRYPTO'92*, pages 139–147, 1993.

[8] J. Foti. FIPS PUB 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY. 2015.

[9] G. Lawrence Paul Sundararaj1 D. R. Anita Sofia Liz2. Anti-Sybil Mechanism against Bogus Identities\nin Social Networks. *International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)*, 01(02):123–127, 2014.

[10] M. Jakobsson and A. Juels. Proofs of work and bread pudding protocols (extended abstract). *Secure Information Networks*, pages 258–272, 1999.

[11] D. Johnson, A. Menezes, . £, and S. Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA).

[12] S. King and S. Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. *Ppcoin.Org*, 2012.

[13] L. Lamport, R. Shostak, and M. Pease. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, 1982.

[14] MaidSafe. MaidSafe.net announces project SAFE to the community, 2014.

[15] L. Nick. CONSENSUS WITHOUT A BLOCKCHAIN, 2015.

[16] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.

[17] Y. Sompolinsky and a. Zohar. Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains. *Eprint.Iacr.Org*, pages 1–31, 2014.

[18] N. Szabo. Formalizing and Securing Relationships on Public Networks. 1997.

[19] TheBitcoinNews. Bitcoin Spam Attacks, 2015.

[20] Vitalik Buterin. A Next-Generation Smart Contract and Decentralized Application Platform. 2013.

[21] X. Wang, D. Feng, X. Lai, and H. Yu. Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. 2004.