CS498A - Under Graduate Project: Blockchain Technology

August 2017 - Ongoing

Nikhil Vanjani
(14429)
Department of Computer Science and Engineering, IIT Kanpur

Abhishek Verma
(14026)
Department of Computer Science and Engineering, IIT Kanpur

Dr. Arnab Bhattacharya
Department of Computer Science and Engineering, IIT Kanpur

Dr. Piyush Kurur
Department of Computer Science and Engineering, IIT Kanpur

1 Introduction

In this project, we are trying to explore blockchains at a fundamental level and to understand how they solve or have the potential to solve various problems. At the time of writing this report, we have formally studied half of Aravind Narayanan's Course on Bitcoins and Cryptocurrencies[1], have read whitepapers of Bitcoin[2], MaidSafe[3], Factom[4] , went through some resources on UCB's Blockchain group's website[5] and miscellaneous blogs. In this report we would focus on some of the major challenges with blockchains.

There has been a buzz about blockchains in the recent years after the breakthrough of the Bitcoin blockchain in 2008 and subsequently various blockchains are emerging. But to say that blockchains are ready to take over the world by storm would be nothing less than an exxageration. The evolution of blockchains seeems similar to that of Internet. The initial designs were to solve some specific problems, but then people realized and are still realizing that its potential is much more than just those problems. So now people are trying to build solutions based on blockchains and the technology is evolving around it. This requires to solve various other problems as well and people are trying to figure out if its possible to solve those somehow using blockchains and cryptography. In the latter sections of the report we will try to explain few of these fundamental challenges.

2 History

Blockchains as a technology had its seeds sown long back in 1970s when Ralph Merkle designed the ***Merkle Tree***[6] data structure, which is at the core of blockchains. More specifically, distributed blockchains are immutable, append only, public ledgers. Subsequently, there were some attempts to build solutions using it but nothing much significant until Bitcoin came about in 2008.

Bitcoin is basically a digital currency, the transactions of which are recorded in a distributed ledger, called the bitcoin blockchain. Before we go into the specifications of Bitcoin, it should be noted that this was not the first attempt of creating digital currency. There were other attempts as well, though not based on blockchains, the most prominent being David Chaum's idea of digital cash[7]. Subsequently, PayPal emerged in 1998 which maybe called the last breakthrough before Bitcoin.

The primary reason behind Bitcoin's success as compared to all other attempts is that it provided a monetary incentive model for users in the network to validate transactions and also to approve only the correct transactions.

3 Use Cases of Blockchains[14]

With the emergence of various applications of blockchains, we feel the use cases can be categorized as follows, though more cases may emerge as well:

- **Bitcoin Currency + Bitcoin Blockchain:** Bitcoin[2]
- **Bitcoin currency + non-bitcoin blockchain:** Sidechains like Blockstream[8], Truthcoin[9]
- **Non-bitcoin currency + bitcoin blockchain:** Factom[4], Namecoin[10]
- **Non-bitcoin currency + non-bitcoin blockchain:** Ethereum[11]

- **Non-blockchain consensus:** MaidSafe[12]
- **Blockchain-neutral smart services:** PeerNova[13]

4 Major Challenges with Blockchains

In this section, we present our understanding of the major challenges. Of course this list is not complete and there are various aspects that we are yet to explore.

4.1 Scalability

The challenges associated with scalability seem to be three fold- speed, cost, space.

- **Speed:** At present, Bitcoin blockchain requires around 1 hour to arrive at distributed consensus which is impractical for scaling up various applications, like monetary transactions, uploading data records, etc. Other blockchains as well require some time, may be lesser than bitcoin but it still is impractical. Exchanges like Mt. Gox and Instawallet attempted to resolve this problem through Green Addresses but these systems relied on trusting the service provider that they won't attempt double spending attacks. But such exchanges could not stand the tide of time and their trust was eventually broken. So, the need is still of a trustless, ie, decentralised system to arrive at distributed consensus quickly. Silvio Micali, in a recent paper proposed Algorand which tries to solve this problem. We look forward to read this paper.

- **Cost:** In the model of blockchains, there are some entitites known as miners who validate transactions. Bitcoin is based on Proof of Work (PoW) concept, ie, miners need to guess a certain random string which will meet the conditions of the hash output. This guessing requires a lot of computational power and the model is such that the miner who guesses the fastest gets to mine the block. On an average whoever has the highest hash rate would be able to guess it. So, as of today, bitcoin blockchain consumes a lot of power due to this competition. The hash rate is increasing day by day and miners will only mine till the point of time when they are reaping profits out the business. To cut down on cost, there have been various alternate proposals like Proof of Stake, Proof of Capacity, Proof of Activity, etc.

- **Space:** There are two primary issues related to space and storage. Firstly, in blockchains like bitcoin, a block can have maximum size of 1MB and each transaction has a minimum size. Also, a block is mined in 10 minutes, and consequently one can carry out transactions only at the rate of 7 transactions per minute. The protocol implementation of micro-payments might be a viable solution for this problem, but micro-payments in their own essence are losing out practicality on bitcoin blockchain due to high transaction fees. People are coming up with alternate solutions to micro-payments. Secondly, as more and more people adapt the blockchains, more transactions get recorded on them and the total size of blockchains increase. For instance, the size of bitcoin blockchain is in excess of 100GBs, which makes it impossible for each user to store the complete blockchain. This was anticipated by the developers beforehand and hence there are two types of nodes in bitcoin- fully functioning nodes and non-fully functioning nodes. Fully functioning nodes store the complete blockchain and get to mine blocks as well, whereas non-fully functioning nodes can store only part of blockchain, say the blocks which contain their own transactions and they are unable to participate in mining activity as they don't store the pool of transactions yet to be mined. Researchers anticipate that due to the increasing size of bitcoin blockchain, there are only thousands of fully functioning nodes on the network and that this figure might be gradually dropping which is a bad sign as it makes pooling majority of computational power in the network easier. Apart from mining issues, storage issues are common problem for scaling up any blockchain and people are yet to figure out how to do that using a blockchain. There are alternatives like MaidSafe, which implement decentralized consensus but blockchain data structure is not at its core. The consensus is achieved using something knwon as Close Groups.

4.2 Network Bootstrapping and Evolution

Bootstrapping the network is something which is done quite innovatively in most of the blockchains. What they do is to put an upper limit on the total number of cryptocurrencies ever in the network and the number of cryptocurrecnies usually is either constant from the beginning or its rate of generation decreases with time. This helps to prevent inflation as the demand 'might' keep increasing forever but the supply has an upper cap. To ensure that this 'might' happens, the early investors in the new blockchains keep themselves invested in it for long time as that is the only way to increase their profits.

This investment of their helps to eastablish trust in the system and in turn boothstrap the network to grow. But putting an upper cap on total number of coins points to a challenge of how the system will evolve. To predict how it will evolve is challenging because the system is constantly changing. People are uncertain about what will happen when the mining rate becomes so low in bitcoin blockchain that the primary source of revenue for miners will be the transaction fees. Will the transaction fees be too steep ? Nowadays people are trying to understand and predict how such networks will evolve from a game theoretic perspective. The theory is catching up but is not yet up to the mark. This is one of the major hurdles the technology faces for widespread adaption.

4.3 Forks and Regulators

At times it so happens that a hacker exploits some vulnerability in a blockchain code or in a service built on top of a blockchain and the hacker is able to gain access to users' wallets and rob them. Such instances have fuelled philosophical debates in two aspects. Firstly, whether hard fork should be created or not. While the creation of hard fork may help to revert the robberies but it goes against the principles of blockchains, ie, it no longer remains immutable. Secondly, if someone thinks hard forks should be done, who should lead the process of spreading awareness among the network users to perform the hard fork in the blockchain to an earlier point of time ? Obviously, there will be some actors who will have enough influence on others so as to successfully propagate it into the majority of the network users. So in a way there still are some sort of regulators or regulatory body of the blockchain, which is principally against the idea of decentralization. These both are open debates and some blockchains happen to have created hard forks while some happen to have prevented that from happening and tried to find an alternate solution. Surely it would be impossible to avoid such occurences as there are always zero days out there. Nonetheless, it would be interesting to explore ways to decreases instances where such decisions need to be taken.

5 References

[1]: Bitcoin and Cryptocurrency Technologies
[2]: Bitcoin White Paper
[3]: MaidSafe White Paper
[4]: Factom
[5]: Blockchain at Berkeley
[6]: Method of Providing Digital Signatures *RC Merkle*
[7]: Blind Signatures for Untraceable Payments *David Chaum*
[8]: Blockstream
[9]: Truthcoin
[10]: Namecoin
[11]: Ethereum
[12]: MaidSafe: Consensus without a Blockchain
[13]: PeerNova
[14]: Use case discussion