A Survey on Blockchain Technology

Different approaches and On-going Development

Navjot Sharma
CS-550 Advanced Operating System
Illinois Institute of Technology
Chicago, IL, United States
nsharma11@hawk.iit.edu

***Abstract*—This paper aims to write a survey on Blockchain technology, identify each Blockchain based on its domain like insurance, energy trading, ride sharing etc, Identify the pros and cons of different approaches to Blockchain, summarizing the progress of on-going development and discovering promising industries which will be disrupted by Blockchain in near future.**

***Index Terms*— Blockchain, Bitcoin, decentralized, P2P Distributed System, Proof-of-Work, Hash and Digital Signature.**

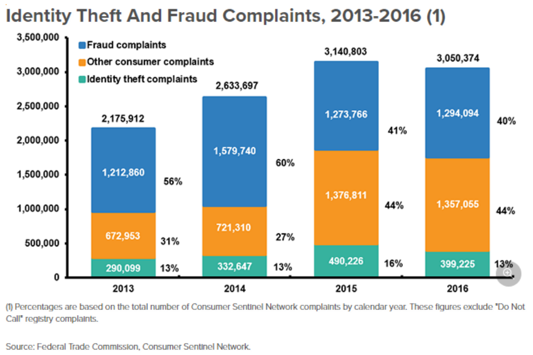
I. Background

It all started with a thesis by Satoshi Nakamoto first time, in the end of November 2008, called Peer to Peer Electronic cash system. This was a thesis on a US mailing list where cryptographers exchange information. This is the very beginning of Bitcoin. After discussions held on the mailing list for a while, the first block was created in January 2009 and the operation of Bitcoin and Bitcoin Blockchain was commenced. Since then, the Bitcoin system as first application of Blockchain technology has receieved recognition throughout the world and has proven to be decentralized solution for financial industries and has never been suspended and users have been increasing worldwide. It is believed that Blockchain has a potential to become an asset for not only the financial institutes but also the non-financial industries too, with its features, such as – No downtime, Falsification of information is hard, and inexpensive system.

II. Problem Statement

The conventional transaction system for currency transaction between persons or companies are centralized, i.e. all the information and data are often controlled and managed by a third party organization, rather than the two entities that are involved in the transaction. For instance if we need to make a digital payment or currency transfer, we require a bank or credit card provider as a middleman to complete transaction, similar is the case with other domains such as music, games, software etc. This problem was addressed by Blockchain technology.

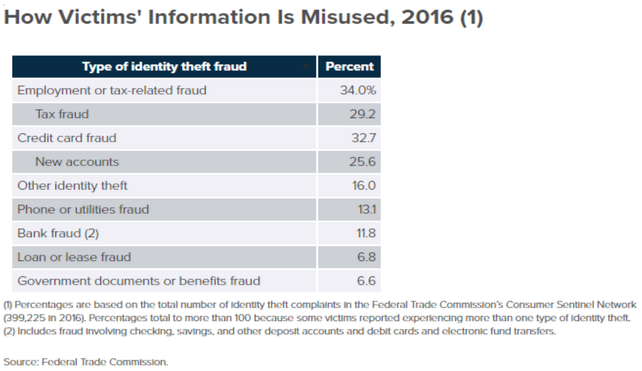
Unlike traditional databases that are stored and maintained on private and centralized servers, a Blockchain is decentralized, publicly distributed, and transparent. This public distribution means that the data being maintained is effectively unforgeable, incorruptible, and has no center point of failure. Identity protection is a common problem in today's digitized world. Seemingly every other week, headlines reveal some hacker has gained access to a centralized server resulting in the theft of millions of financial records, medical records, or identities. Below figures 1 and 2 shows the stats of Federal Trade Commission, for Identity theft and Fraud Complaints from 2013- 2016 and how victim's information is misused in 2016. This problem is likely to get worse before it gets better. As of 2016, there are 13 billion devices connected to the internet. Many of these devices hold our personal information, bank records, and credit card numbers. By 2020 this number is set to reach 40 billion leaving us more exposed than ever.


Identity Theft And Fraud Complaints, 2013-2016 (1)

(1) Percentages are based on the total number of Consumer Sentinel Network complaints by calendar year. These figures exclude "Do Not Call" registry complaints.

Source: Federal Trade Commission, Consumer Sentinel Network.

Figure 1


How Victims' Information Is Misused, 2016 (1)

Type of identity theft fraud	Percent
Employment or tax-related fraud	34.0%
Tax fraud	29.2
Credit card fraud	32.7
New accounts	25.6
Other identity theft	16.0
Phone or utilities fraud	13.1
Bank fraud (2)	11.8
Loan or lease fraud	6.8
Government documents or benefits fraud	6.6

(1) Percentages are based on the total number of identity theft complaints in the Federal Trade Commission's Consumer Sentinel Network (399,225 in 2016). Percentages total to more than 100 because some victims reported experiencing more than one type of identity theft.
(2) Includes fraud involving checking, savings, and other deposit accounts and debit cards and electronic fund transfers.

Source: Federal Trade Commission.

Figure 2

III. History and Purpose of Survey

This technology was originated in 1991 as Digital timestamps, which were basically like Notary, and used to timestamp the digital documents so that no one could tamper with them, and it was not used after that, until in 2009, it was adapted by Satoshi Nakamoto, to create a digital cryptocurrency called Bitcoin. And then, in 2015 Ethereum was launched which was build on Bitcoin design with smart contracts.

This paper aims to write a survey on Blockchain technology, identify each Blockchain based on its domain like insurance, energy trading, ride sharing etc, Identify the pros and cons of different approaches to Blockchain, summarizing the progress of on-going development and discovering promising industries which will be disrupted by Blockchain in near future.

This decentralized environment for transaction has been enhanced for various domains as below:

- Insurance
- Energy trading
- Ride sharing
- Supplychain
- Banking
- Education
- Healthcare, etc.

We'll be discussing about the advantages and disadvantages of the Blockchain solutions available in few of these domains.

IV. Research Approach

The research approach for this project paper follows below steps:

a. Blockchain Working and Its Components.
b. Properties of Blockchain
c. Different Approaches in Different Domains
d. Pros and Cons based on different Approaches for evaluation
e. On-going Development and Research Challenges.
f. Future of Blockhcain

Details are as follows:

a. Blockchain Working and Its Component

Blockchain is a digital ledger in which transactions made in Bitcoin or another cryptocurrency are recorded chronologically and publically, it enables transaction between individual participants without involvement of a third party.

Components of a Block:

- ➢ Data- the data stored in a block depends on the type of Blockchain, for example in case of Bitcoin; data is sender, receiver and the amount to be transferred.
- ➢ Hash- It can be considered as a fingerprint and identifies a block and it is always unique, such that once a block is created its hash value is calculated, and if something changed in a block then it cause the value of hash to be modified, this means the whole block is changed.
- ➢ Hash of previous block- used to create the chain of blocks, hence the name Blockchain. It makes the block secure by creating a chain, if one block changes, this makes the next block invalid, because it doesn't have the value of a previous block.

Only hashing cannot help to make the Blockchain secure, because with today's technology we can very easily tamper with one block and recalculate hashes for other blocks to make the blocks valid again. So, the question arises how Blockchain secure themselves? The answer is using Proof of Work- POW and Being distributed i.e. Peer-to-peer P2P network.

As shown in Figure 3 below, Proof of Work provides the guarantee of the continuity of data and enables sharing of the Blockchain data among nodes adding delay or slowing down the creation of new blocks and mitigating the issues with Hashing. In Bitcoin it takes 10 mins to calculate the required POW and add new block to the chain.

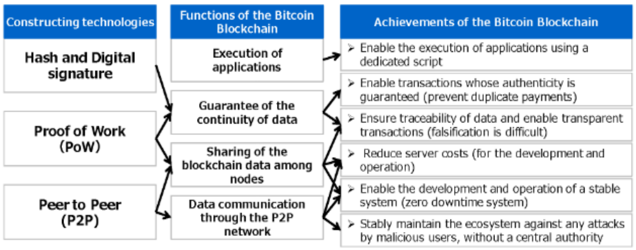

Constructing technologies
Functions of the Bitcoin Blockchain
Achievements of the Bitcoin Blockchain
Hash and Digital signature
Proof of Work (PoW)
Peer to Peer (P2P)
Execution of applications
Guarantee of the continuity of data
Sharing of the blockchain data among nodes
Data communication through the P2P network
➢ Enable the execution of applications using a dedicated script
➢ Enable transactions whose authenticity is guaranteed (prevent duplicate payments)
➢ Ensure traceability of data and enable transparent transactions (falsification is difficult)
➢ Reduce server costs (for the development and operation)
➢ Enable the development and operation of a stable system (zero downtime system)
➢ Stably maintain the ecosystem against any attacks by malicious users, without a central authority

Figure 3

b. Properties of Blockchain

- Decentralized- P2P –means that not one single entity has control over all the processing
- Public- Open to everybody to access and use.
- Fault tolerant- provide protection from failure, since there is no single point of failure.
- Enables the transfer of value
- Distribute Database- means not all the processing of the transaction is done in the same place
- Cryptographically secure Design

Figure 4 represents the structure of centralized, distributed and decentralized systems.

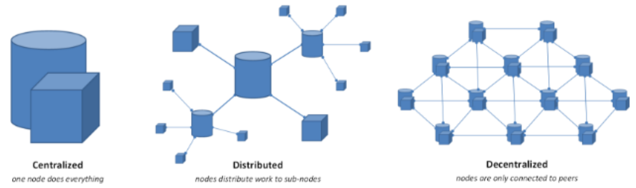

Centralized
one node does everything
Distributed
nodes distribute work to sub-nodes
Decentralized
nodes are only connected to peers

Figure 4

c. Different Approaches in Different Domains

There are number of non- financial domain applications for Blockchain along with financial ones, these are as below:

- Finance: Stock exchange, Peer-to Peer Banking, Remittance Services and Bitcoin trades are few approaches to Blockchain in Finance domain.
  - Stock Exchange- BitShares, Overstock
  - Peer-toPeer Banking- ROSCA which is a rotating savings and credit association (ROSCA). A group of individuals who agree to contribute for a defined period in order to save and borrow together. This is a form of combined peer-to-peer banking and peer-to-peer lending and usually between immigrant communities in a developed country or communities in a developing country.
  - Remittance Services- e.g. Bitpesa, Abra, Toast
  - Bitcoin trades- itBit, Coinffeine

- Insurance: In the insurance sector, blockchain makes it easier to share information, providing greater line-of-sight to data and security through records that cannot be altered when written. Labor-intensive, repetitive and error-prone client onboarding, underwriting and claims settlement processes will be transformed through the use of a unified platform to store and share all documentation. Below are few approaches in Insurance domain:
  - P2P insurance Social Insurance Network- Guevara, Friendsurance
  - Digital ID- ONENAME, OpenID Connect

- Ride Sharing: Instead of having a centralized organization acting as a clearinghouse, everyone who wants to drive others around would attach that piece of metadata to their profile that is part of a Blockchain. There would be locations served and other information such as reviews of the driver that could be added to the profile. Then, when someone requests a vehicle, the Blockchain could filter out possible matches and deliver them to the rider who can request a ride. Then, transactions between the driver and rider can be processed on the peer-to-peer network.
  - Real-time ridesharing is an approach to this domain.- La'Zooz and Arcade city are example applications.

- Supplychain Management: Blockchain can increase the efficiency and transparency of supply chains and positively impact everything from warehousing to delivery to payment.
  - Peer-to-Peer Market- OpenBazaar
  - Supply Chain- SkuChain, Fluent, Provenance, Blockverify.

- Energy Management: It allows customer to buy and sell energy from each other in a centralized way.
  - TransactiveGrid and Ethereum are the application used for Energy management that uses Blockchain technology.

- Government Sector: Government sector is disposed to frauds and corruption, hence using Blockchain can help here, for Voting, Budgeting and to manage basic income.
  - Voting-Democracy.Earth follow.myvote.com- for voter registration, verification and counting
  - Budgeting- Consensys- already in function in Dubai.
  - Basic Income management- Circles for universal basic income.

- Medical: There are number of ways Blockchain is helping medical industry for example by providing access to large sample of anonymised medical record or genetics data.
  - Genetic Storage- Genecoin
  - Medical Records- BitHealth, Gem, Tierion
  - DNA recording- DNA.Bits

- Asset Management: It is used for asset management, such as Land registration using application Factom, because small developing countries, sometime the farmers are tricked and they end up losing their own land, if the only paper documentation they have is lost.

V. Evaluation and Results

The evaluation of this project is comprised by the following:

- Comparison of different type of Blockchain technology solutions available based on the domains like insurance, energy trading, ride sharing, supplychain, banking, education, healthcare, etc.
- For the sake of comparison we will also be identifying their pros and cons
- We will also be summarizing the progress of the on-

going development in this area.

Based on the above approaches there are different advantages and disadvantages of Blockchain technology.

- Pros:
  - There is no need for middleman/intermediaries, everything is out open for everyone to access. It has empowered users, since they are in control of all their information and transactions.
  - Also the transaction cost overhead has been greatly reduced.
  - 1 Bitcoin = **6925** USD nowadays, which has increased over time , and is expected to become $20260 in next two years.
  - Transactions are verified by huge P2P network and are irreversible, therefore there is no single point of failure.
  - The transactions are faster as compared to the interbank transactions which generally takes days for clearing and final settlement for off working hours.
  - Anything with a value to it can be transferred and saved safely and confidentially - without any modification
  - Cryptocurrency is not affected by economic crisis – (money in bank can be frozen in such crisis)

- Cons:
  - Lot of resistance, because people are currently employed by the institutions that serve as intermediaries
  - Scammers take advantage of anonymity of conducting transaction, e.g. can offer to multiply your bitcoin or Ransomeware malware
  - Still possible to Hack or manipulate system with strong will.
  - People still are unaware of cryptocurrency as a valid payment method like money
  - Energy consumptions is high, because the Bitcoin Blockchain network's miners are validating transactions by attempting 450 thousand trillion solutions per second, which requires large amount of compute power.
  - Even though it offers saving in transaction costs and time but the high initial capital costs cannot be avoided.
  - If companies need to migrate to Blockchain application system, it need to replace the existing systems, for which they need to strategize the transition.

There are number of on-going Research and development happening worldwide for Blockchain today, few highlighted ones are as below:

- Blockchain Thunder: The technology enables users and vendors to send and receive payments without touching the main block chain. Even in the prototype phase, Thunder has the potential to facilitate secure, trustless and nearly instant payments, unleash the power of micro transactions and allow the network to handle heavy loads, and increase user privacy.
- DIGITAL ASSET RESEARCH LAB: Blockchain recently partnered with the Centre for Cryptocurrency Research and Engineering (IC3RE) at Imperial College London to launch the Digital Asset Research Lab, a leading international centre for ongoing research and application activity related to cryptocurrency and block chain technology.

Even though the research is in right direction, but there is still couple of challenges to it, these are as follows:

- Add new functionality to Blockchain- for example storing more info
- Require different settings than original Bitcoin
- Business solutions
- Make it scalable – size of transaction
- Using Blockchain to develop more utilities.

VI. Future of Blockchain

Blockchain with its popularity and efficient functionality has a promising future. It has already started to disrupt most of the non- financial industries; I have identified few other industries that Blockchain will be disrupting in coming years:

- Forecast- It will change the way how we do research, consulting analysis and forecasting
  Example= Augur, used to place bets in a decentralized way, bet on anything from sports, stocks to elections.
- IOT- Internet of Things: Samsung and IBM want to create a decentralized network of IOT devices using Blockchain and this will eliminate the need for central location to handle communication for IOT devices and devices could communicate directly, update s/w, manage Bugs and monitor energy usage.
- Cloud Storage: Use Blockchain to make cloud storage more secure from hacks. Storj.io -> Decentralized cloud storage
- Public Benefits: Public benefits don't reach the lower level to the public and gets lost in the upper level due to corrupted public sector; Blockchain will help to mitigate this problem. Govcoin- UK based company, helping the Government to distribute public benefits using Blockchain
- Real-estate- Realtors ask for lot of commission fee and there are frauds with this domain too, with Blockchain in place the buyer can directly contact the seller of the property without the third party

hindrance. Ubiquity is one example of ongoing application development.

- Charity: Bitgive- To make sure that there is no corruption, and the needy get what they deserve.

VII. Conclusion

In conclusion we can say that, Blockchain technology runs the Bitcoin cryptocurrency and is a decentralized environment for transactions, where all the transactions are recorded to a public ledger, visible to everyone. The goal of Blockchain is to provide anonymity, security, privacy, and transparency to all its users. However, these attributes set up a lot of technical challenges and limitations that need to be addressed. For the sake of this survey, various non-financial domains have been identified along with the applications that are already implemented in those domains and after carefully considering all those application we came up with the future industries that will be disrupted by Blockchain. We have also identified the on-going Research and development and the the challenges associated with the research today.

Acknowledgment

Thank you for the TA Hariharan Devarajan, for helping choose this interesting project topic. Thanks to Prof Sun for his valuable inputs during presentation. Thank you both for the patience and detailed information you have provided.

References

[1] Statistics for Identity theft/cybercrime as identified by Federal Trade Commission (FTC) https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints

[2] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[3] Swan M. Blockchain: Blueprint for a New Economy. " O'Reilly Media, Inc."; 2015

[4] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Consulted. 2008;1(2012):28. https://link.springer.com/chapter/10.1007%2F978-1-4614-2110-8_2

[5] Meti- Survey on Blockchain Technologies and services - Information Economy Division Commerce and Information Policy Bureau http://www.meti.go.jp/english/press/2016/pdf/0531_01e.pdf

[6] Thesis by Satoshi Nakamoto – Bitcoin: P2P https://bitcoin.org/bitcoin.pdf

[7] Identity theft management https://medium.com/@philfrancis77/blockchain-the-byzantine-general-problem-and-the-future-of-identity-management-6b50a2eb815d

[8] Blockchain implementations: https://medium.com/@gaurangtorvekar/7-blockchain-technologies-to-watch-out-for-in-2017-4b3fc7a85707

[9] 19 Industries The Blockchain Will Disrupt https://futurethinkers.org/industries-blockchain-disrupt/

[10] IBM Blockchain Blogs https://www.ibm.com/blogs/blockchain

[11] Medium blogs: https://medium.com