Blockchain and Its Applications – A Detailed Survey

Supriya Thakur Aras
Department of Computer Engineering
Maharashtra Institute of Technology,
Pune, India

Vrushali Kulkarni, PhD
Department of Computer Engineering
Maharashtra Institute of Technology,
Pune, India

ABSTRACT
Blockchain is being termed as the fifth disruptive innovation in computing. In simplest words, it is a distributed ledger of records that is immutable and verifiable. Since its advent in 2008, blockchain as a concept has been used in various ways. The largest impact or application is seen as a multitude of cryptocurrencies that have sprung up. However, with time, it has become clear that blockchain as a technology is likely to have an impact much wider than just the cryptocurrency domain and much deeper than simple distributed ledger storage. This detailed survey intends to bring together all the key developments so far in terms of putting blockchain to practice. While the most common adoption of blockchain is in finance and banking domain, there are experiments being conducted by many big players in various other domains. This paper will explore the various domains where blockchain has had an impact and where future implementations may be expected.

General Terms
Blockchain

Keywords
Blockchain, Cryptocurrency, Distributed Ledger

1. INTRODUCTION
Blockchain technology or the distributed, secure ledger technology has gained much attention in recent years. This paper presents a detailed survey of blockchain technology literature and its applications. The sources of blockchain literature examined for this survey include research papers, books and book chapters, journal papers, specific cryptocurrency sites and wikis, conference papers, company 'Point of View's (PoVs), whitepapers published by various organizations implementing and experimenting in Blockchain. Blockchain being a much hyped and experimented technology a lot of literature is found in content hosted on proprietary forums such as company websites, web articles, etc. This survey is extensive and covers the various aspects of blockchain including consensus algorithms and their variations as well as currently implemented and possible future applications. This survey will not cover the details of technical aspects of blockchain, however, references that cover these aspects may be found in bibliography.

2. BLOCKCHAIN OVERVIEW

2.1 Blockchain Technology
A very significant plus of the blockchain technology is that it solves two of the most dreaded problems of currency based transactions, which have so long necessitated the requirement of a third party to validate the transactions. These are popularly known as the Byzantine Generals' Problem and the Double Spend Problem.

With advent of Blockchain, cryptoeconomics has evolved. This very aspect has been highlighted in works of Pilkington [1]. The paper explains how blockchain as a concept can be applied to a non-tokenized scheme. The paper also talks about blockchain taxonomy and how hybrid solutions become an obvious choice and moving from permissionless to permissioned blockchain becomes imperative to solve certain kinds of problems where trust is paramount and a public permissionless ledger seems both a risk and an overhead.

For a long time, the terms Bitcoin (cryptocurrency which has been the first and the most successful of the blockchain based cryptocurrencies) and Blockchain have been used interchangeably. Swan [2] explains how these terms were used to mean one of the three things – firstly the underlying blockchain technology platform, secondly the Bitcoin protocol i.e. the software which actually runs on the Bitcoin blockchain's network computers and makes transactions possible and thirdly the Bitcoin digital currency itself (denoted as BTC) which is the source of value. The three things listed above can be visualized as the layers of the Blockchain stack. Blockchain technology forms the lowermost layer with the Bitcoin protocol in the middle and the digital currency forming the top layer. Swan's book [2] considers the evolution of Blockchain technology in three generations. The digital currency application is considered the Blockchain 1.0, the application of blockchain to smart contracts and Distributed Applications (DApps) is considered the Blockchain 2.0 and finally the application beyond currency and economics is detailed as the Blockchain 3.0.

Peters and Panayi [3] provide a comprehensive overview of emerging blockchain architectures, their distinction from traditional databases and role of blockchain in electronic exchanges.

3. BLOCKCHAIN TAXONOMY
The original idea of blockchain implementation propounded by Nakamoto [4] has been that of a public decentralized ledger. So has been the implementation of most popular blockchains e.g. Bitcoin, Ethereum. In theory, based on who can access the blockchain network and how the permissions to write to the blockchain network are assigned, four types of blockchains can be defined as shown in Table 1.

Table 1: Blockchain Types

Based on access to blockchain	**Based on access to blockchain data**
Permissionless – Anyone with computing power can join	Public – All who access can modify
Permissioned –Approved users only	Private – Only specific users can write / modify

However, it is observed that the terminologies Public and Permissionless are used interchangeably and so are Private and Permissioned.

An increasing number of use cases can be found for permissioned/ non-public blockchains. Buterin [5] explains appropriately why certain real life situations demand non-public blockchains. He further classifies the non-public blockchains into Consortium blockchains and Fully-Private blockchains. Based on the investment capacity and privacy need organizations may choose to go for private or consortium blockchain as an alternative. Consortium blockchains may be the option of choice when different organizations have common goals to achieve, wish to share the cost and are willing to share their data.

Depending on the use case, one needs to select an appropriate architecture from those defined in the Table 1. Xu et al. [6] provide a further detailed taxonomy which can help in choosing architecture for a blockchain system. This paper classifies various blockchain based system configurations against multiple parameters such as performance, cost efficiency and flexibility. Various dimensions of a blockchain system such as blockchain configuration, storage, computation, degree of decentralization are considered in coming up with the taxonomy.

3.1 Public /Permissionless blockchains

Public blockchains are open for all. Anyone can join them to post transactions and to participate in the mining and consensus process of adding new block of transaction to the blockchain [7]. These blockchains usually use Proof of Work (PoW) or Proof of Stake (PoS) for consensus mechanism. Having more number of participants works well for this model, as it further reduces the possibility of a 51% attack.

As per Buterin [5] public blockchains enhance the notion of trust and also protect the applications from the developers themselves. There is usually sufficient incentive (e.g. in Bitcoin, at least at the moment) and also significant saving as compared to third party dependent systems in terms of minimal transaction costs to opt for public blockchain to record transactions. An agreed disadvantage of public blockchains [1,2,3] is that it is wasteful in terms of computing power especially when PoW is involved.

3.2 Non – Public /Permissioned blockchains

Permissioned blockchains are built usually by organizations for their specific business need [5]. Such blockchains are likely to have interfaces with existing applications of the organization. Organizations may opt for consortium blockchains where limited trusted members mandatorily need to sign off a transaction. In fully private blockchains, the write permission over the blockchain is given to a central organization. The former are referred to as partially decentralized by Buterin [5].

Much value is seen in private blockchains due to the flexibility offered by increased control over the rules of transaction, which may be altered by overall consensus. This becomes easier in a private or consortium blockchain than a public one. There is also increased accountability as all the nodes are named. The Bitcoin blockchain as of date approximately takes 10 minutes for a transaction to be confirmed and is considered to be secure after ~6 blocks are added after the said block. In addition to cryptographic puzzle solving time, network delays add to the transaction commit time. This disadvantage is not applicable in a private blockchain scenario, as network delays are limited. They may however not be completely eliminated and may still exist, given that even private blockchain nodes may exist over network in a cloud environment.

Increasing applications of permissioned blockchains are seen, handling a variety of asset types, not necessarily cryptocurrencies. An example of this is seen in Accenture [8] using blockchain for storing feedbacks in the Akshay Patra Meal Provisioning for school children in India. Since the non-public blockchains are often connected to other applications, they can be used to store merely the encrypted hash i.e. a digital representation of assets or equivalents stored on other systems or even physical assets such as land, educational certificates, artwork, etc. Increasing number of banks are utilizing or experimenting with blockchain to use it to store fiat currency digital representation or even securities that can be traded.

4. BLOCKCHAIN PROTOCOLS

Blockchain eliminates the need for third party to conduct transactions on one's behalf. This implies that the consensus mechanism has to exist in the network itself. How a given blockchain network implements its consensus mechanism, determines the strength of the network. A foolproof consensus mechanism, suitable for purpose (of the blockchain in question) is essential to maintain sanity and coherence of data among the participating nodes of the network. The consensus mechanisms of blockchain aim to eliminate mainly two known problems with digital currency - Remove the problem of double spend and Eliminate Byzantine Generals problem.

While much work has been done on blockchain protocols, there are some key algorithms explained in brief here whose variations are being used and further developed to suit various applications of blockchain. Cachin et al. have explained blockchain consensus mechanism and various consensus algorithms in their research paper [9].

4.1 Proof of Work

PoW protocol requires all nodes on the network to solve cryptographic puzzles by brute force. For example, in case of Bitcoin blockchain, the new transactions are tentatively committed and then based on the PoW output, a selected block created by the winning node is broadcast to all the nodes, at specific synchronization intervals. Once the block is transmitted using peer to peer communication to all other nodes, the same is included in the blockchain and any tentative transactions are rolled back [10]. By rule of probability, the consensus is achieved as 51% of power rather than 51% of people count. Effectively the computing power used by all other nodes except the winning node, is wasted.

4.2 Proof of Stake

Proof of stake protocol of block verification does not rely on excessive computations. It has been implemented for Ethereum and certain altcoins. Instead of splitting blocks across proportionally to the relative hash rates of miners (i.e. their mining power), proof-of-stake protocols split stake blocks proportionally to the current wealth of miners. The idea behind Proof of Stake is that it may be more difficult for miners to acquire sufficiently large amount of digital currency than to acquire sufficiently powerful computing equipment. It is also an energy saving alternative [1, 11].

A variation of POS is the Delegated Proof of Stake (DPOS) algorithm. Delegated proof of stake (DPOS) is similar to POS, as miners get their priority to generate the blocks according to their stake. The major difference between POS and DPOS is that POS is a direct democratic while DPOS is representative democratic. Stakeholders elect their delegates to generate and

validate a block. With significantly fewer nodes to validate the block, the block could be confirmed quickly, making the transactions confirmed quickly. Meanwhile, the parameters of the network such as block size and block intervals could be tuned by the delegates. DPOS is implemented by Bitshares [11].

4.3 Practical Byzantine Fault Tolerance

An approach to deal with the Byzantine Generals problem is the Federated Byzantine Agreement (FBA). In this approach, it is assumed that the participants of the network know each other and can distinguish which ones are important and which ones are not. PBFT (Practical byzantine fault tolerance) is a replication algorithm which utilizes this principle. Hyperledger utilizes the PBFT as its consensus algorithm. There are designated validator (primary) nodes that are each associated with a group of nodes. The primary is responsible for multicasting requests to other replicas in its group. A service operation would be valid if it has received approvals from over 1/3 different replicas. Additionally, if a client does not receive the replies, it will send the request to all replicas instead of only sending it to the primary in case the primary is faulty. A primary is responsible for ordering the transaction and each replica commits the transaction in the same order. It has been seen that PBFT or its variations map well to the needs of various organizations like banks, supply chain or payroll systems.

4.4 Comparison of Blockchain Consensus Algorithms

Table 2 provides a quick comparison of the popular blockchain algorithms.

5. BLOCKCHAIN APPLICATIONS

Bitcoin has been the mainstay to many of the other applications of blockchain. Many projects have been implemented to overlay the Bitcoin blockchain as noted by Swan and Crosby et al. [2, 12]. This not only makes the Bitcoin more powerful and popular, but also reinforces the notion that Bitcoin is here to stay. Some examples are MasterCoin, NXT, Open Assets, ColoredCoins, etc.

Pilkington in [1] also explains how the concept of blockchain can be extended beyond digital currency to any asset that has a definite value associated with it. The paper explains some of the popular cryptocurrency applications like Ethereum, Ripple, Gridcoin, etc., and also lists possible future applications in various domains such as digital identity provisioning, voting, commodity trading, etc. Interesting insights on Blockchain impact to Financial Domain can be obtained from the Edgeverve Infosys Finacle Report, Feb 2017 Blockchain Technology From Hype to Reality[13]. As per this report derived from a survey of over 75 financial institutions, nearly 50% of the banks surveyed have already invested in Blockchain technology or were likely to do so in 2017.

This survey proved that blockchain is being tried in almost all important domains such as healthcare, finance, supply chain management, reputation management, etc.

5.1 Social Inclusion

As internet has become an accessible global platform to bring the world together, thanks to the mobility revolution, it is possible for the people in remotest parts of the world to access internet resources across the world. Cryptocurrencies enable people with no access to physical banks to perform global transactions with others across the world. As sited by Pilkington [1], thanks to Bitcoin, sellers like Indian handicraft work artisans have now found a global marketplace to sell their work. This takes away the hassle of fiat foreign currency availability and conversion. Bitcoins are an easily accessible, usable global cyptocurrency which provides value for their work.

Table 2 Comparison of Blockchain Consensus Algorithms

Algorithm	Pros	Cons
Proof of Work E.g.: Bitcoin, Litecoin, Dogecoin, Namecoin	• Considered very secure, as less prone to Sybil attack unless a mining node acquires • 51% of the pools computing power. • Miners get rewards (as Bitcoins) • Prevents unlawful forking of the chain	• Quite slow at the moment, only 1 block added in 10 mins • Driven by rewards assigned to solving the hash, may run into problems as rewards dwindle • Consumes lot of electricity (mining likely to be centralized where electricity is cheap!) • Decisions are not final till 6 blocks are confirmed
Proof of Stake E.g.: Nxt, Mintcoin	• Less wasteful in terms of energy consumption • Less chance of hardware centralization • Potentially faster than Proof-of-work protocol • Possibly reduced possibility of selfish mining attack (assuming already rich miners are less likely to attack!)	• Miners are encouraged to hold on to their stake rather than converting it into at currency • Economic penalties for fraudulent attempts
Practical Byzantine Fault Tolerance E.g.: Stellar, Ripple	• Can tolerate 1/3rd of the nodes to be faulty or adversarial • Fast and efficient • Trust is decoupled from resource ownership, so small group can keep a powerful organization in check	• Parties must agree to the exact participation of groups • Comes at the cost of anonymity

5.2 Cryptocurrency

Currency that is in use across the world is largely fiat currency or currency whose value is assured by a government guarantee, e.g. Indian Rupees, US Dollar, Great Britain Pound, etc. These currencies are not backed by physical assets. Commodity money is backed by a tradable resource, like Gold and Silver. Its value is at least as much as the value of the commodity itself. [14]

Cryptocurrency such as Bitcoin does not fit into any of the above categories. Cryptocurrencies are a medium of exchange that uses cryptography to secure transactions. They are a poor store of value compared to traditional fiat currencies and have lower price stability due to lack of government intervention. However, cryptocurrencies are a more efficient medium of exchange as blockchain technology is uniquely positioned to tackle speed and cost.

At the time of writing this paper in Dec 2017, over 1300 cryptocurrencies existed, with a total market capitalization of $ 431,029,932,585. Bitcoin is the most successful and most widely circulated cryptocurrency with a market cap of nearly $24,747,300,000 [15]. There are many cryptocurrencies being created and used for specific purposes. It may be noted that the value of the cryptocurrency is measured using the fiat currency.

5.3 Private Data Storage

A generic extension of blockchain transactions to transfer stuff other than cryptocurrency is suggested by Zyskind et al. [16]. In their proposed system, the transactions are used to carry instructions for storing, queuing and sharing data. With increased number of mobile applications seeking complete access to user data such as contacts, messages, photos and a variety of other personal data, Zyskind et al. [16] have provided the implementation architecture of a system which uses blockchain along with an offline storage mechanism in order to manage permissions explicitly for each line item, rather than giving complete access permission indefinitely. Offline storage such as LevelDB or any cloud storage can be used to limit the amount of data stored in the blockchain. This could however result in a limited third party dependency, but makes the solution more scalable.

Organizations may choose technology upgrade to adopt a more reliable data privacy solution, for their data.

5.4 Reputation Management

A successful implementation of reputation management can be found in Accenture's [8] Akshay Patra Midday Meal Program Management project. This project used a private blockchain implementation to gather real time, direct feedback from schools that is not manipulated by intermediaries. Thus blockchain has provided the required transparency to the meal chain, to help in audits and invoicing. This has also saved the manual effort of collecting, collating and transmitting the feedback.

5.5 Education

Blockchain can be the transformational force in education as well. Sharples and Domingue [17] have suggested the use of blockchain to provide a verifiable, easily shareable and permanent record of such educational records and rewards. It also talks about the possibility of having an 'Educational Reputation Currency', which is initially distributed to participating institutes based on any existing metric. This currency can then be propagated successively in the blockchain and may be awarded to promote learner reputation.

One limitation not completely addressed in this paper is how the creation of such a reputation currency shall be controlled. For example, in case of Bitcoin blockchain, Bitcoins are created whenever a block is added to the blockchain. The added Bitcoins are awarded to the node that added the block. The quantity of Bitcoins created is also defined by the Bitcoin algorithm. At the time of writing this paper, every added block adds 25 Bitcoins to the winning node's account. Using an external third party ranking of educational institutes may create a bias and participants may question fairness. A successful implementation of blockchain to award educational certificates has been done by Sony and University of Nicosia [18, 19]

5.6 Banking

The impact of blockchain as a technology was first felt by the banking and trading sector. So much so that Bitcoin and its underlying technology, the blockchain, were initially seen as the biggest threat to banking businesses worldwide. However, in past few years it has been seen that banks have deep dived to make this technology work for them in a favorable manner and are experimenting various ways to use blockchain in their business.

Some experts however still do believe that blockchain will lead to the end of several long standing businesses and professions [20]. Typical banking processes like approval of a loan or derivative is a time consuming process due to multiple back end steps involving contract negotiations with multiple parties. Blockchain provides the necessary transparency and speed via smart contracts, to this requirement. Multiple banks are already experimenting Blockchain-as-a-Service offering from technology companies such as R3, IBM and Microsoft [9, 20, 21].

The potential role of blockchain in banking is dealt with in great detail in [3]. Panayi et al. discuss automation of various niche aspects of banking like client account reconciliations, data loss reporting, Over the Contracts (OTC) contracts/products and clearing settlement, cash management by government, etc.

5.7 Finance – Payroll and Settlement

Public service transactions may be as trivial as buying a train ticket or more complex ones such as marriage registration, property buy and sell, patent management, etc. Typically public service transactions require a series of actions to validate the authenticity of the transacting party (or parties), verification of the data provided by the transacting party (or parties), conduct the required transaction and finally provision of the required service followed by recording of the end to end transaction. This translates into significant turnaround time for the transacting parties.

A digital blockchain ledger can reduce this turnaround time to minimum as the most important asset ownership validation and verification is performed taking advantage of the intrinsic nature of the blockchain.

Sestoft [22] proposes a distributed system – Autonomous Pension Fund that would be a self-sustaining running autonomous contract based system to manage life based pension funds without a central trusted pension fund. Since a large number of activities related to life based pension such as receiving payments from active customers, making payments to beneficiaries and payments of taxes on pensions are mainly processing of contract regulated payments, Sestoft opines that

they can be executed using Self Executing Contracts and a cryptocurrency. Sestoft has proposed use of Ethereum for the algorithm. A prerequisite here is the fact that such an autonomous system will need event insurance relates life-event triggers from other trusted bodies, so that self-executing contracts can act on them.

A key challenge noted by Setsoft [22] for the Autonomous Pension Fund system is the long term nature of the engagements with the customer/beneficiaries till their death. It is challenging for people to have faith in an autonomous system to keep its promises and more so to keep faith in the technology and its sustenance for that long a period. The latter challenge about faith in longevity of the technology itself, equally applies to most of the blockchain applications.

5.8 Blockchain for Public Services

5.8.1 Taxation

As ideated in [23] PWC, UK, report, taxation is one area where blockchain can potentially make a big contribution. The report relates the key attributes of blockchain namely provenance, transparency and traceability to the exact needs of a modern taxation system. A huge advantage of cutting on administrative cost can result from the use of blockchain especially in transaction taxes such as VAT, withholding Tax, stamp duties, etc. In a sharing economy, blockchain could be used to achieve compliance and transparency for tax payments, thus shifting the responsibility of collecting tax from tax authorities to participants of the sharing economy.

In countries like India which are moving towards uniform taxation via GST (Goods and Services Tax), blockchain can help in tracking the end-to-end collection and expenditure of taxes by the government. While the tax provenance aspect is very important and so also is the utilization of tax earnings.

The biggest challenge however, in this would be to achieve digitization of currently non-digital sellers who rely on paper records rather than digital ones. Pilots in this area in various countries are likely to be seen in future.

5.8.2 Healthcare

Over the past decade, healthcare is turning increasingly digital with more and more doctors, hospitals, healthcare machineries going digital to store their patient records. Digitization of medical data enables easy retrieval, sharing on need basis for better decision making based on historic cases and is also very crucial for legal purpose record keeping. However, medical data digitization also exposes it to a bigger risk of patient privacy violation.

A blockchain based Healthcare Data Gateway (HDG) is proposed by Yue et al. [24] They propose the use of a private blockchain cloud to guarantee that the medical data cannot be changed by anybody including the patient himself and/or the physicians. Medical data is diverse in kind, i.e. it could be numeric, textual, image data (scans, x-rays, photos, etc.), video data (transcripts, recordings, etc.), etc. To remove the complexity of storing varied data types Yue et al. [24] propose an Indicator Centric Schema (ICS) based data model. In this model, a single table shall be used to organize all data for a given patient and would include simple relevant fields like timestamp, indicator, type, value and category. The ICS also can be extended to include a Purpose Centric Access Control model which would include say requestor, indicator, timestamp, purpose and retention duration.

Such a model is extensible for use in other similar applications of blockchains where data of different types needs to be stored. A segregation of frequent and infrequently accessed data into separate blocks of the blockchain may also be done.

Xia et al. [25] have also proposed a blockchain based system MeDShare, for sharing medical data among cloud service providers. MeDShare would provide data access control, provenance and auditing. The proposed system also used smart contracts for data behavior detection from data access patterns, and blocks malicious users.

5.8.3 Voting

In the year 2014, a Danish political party was the first to use blockchain technology for voting [26]. Online voting platforms such as 'Followmyvote' [27], which enable digitally secure blockchain based voting have also been created.

5.8.4 Insurance

Cognizant Technology Solutions give an end-to-end view of how blockchain can transform insurance in their perspectives [28]. Travel insurance, crop insurance, property and casualty insurance and most importantly health insurance are all set to change with the use of blockchain technology. A multiparty shared network with insurers, hospitals, funeral homes, a department of health and the beneficiary forming the nodes of the blockchain, can be created. This setup will provide the necessary disintermediation and speed required for the insurance and claim process to be streamlined and to eliminate frauds.

5.8.5 Smart Cities

A possible application of Blockchain to smart cities is suggested by Sun et al. in [29]. Authors relate a smart city to a sharing economy where information and communication technologies are utilized to enhance opportunities of sharing of resources. Author proposes using a blockchain based framework for sharing of resources across various services to ensure data immutability, accountability, proper asset utilization and to reduce transaction costs.

6. OTHER RELATED WORK

Blockchain has its inherent challenges and limitations. Due to peer to peer network operation, it is high on energy usage and hence wastage per unit computation. While all the network nodes compete to add the block in case of a Proof of Work based blockchain system, only one node succeeds in adding its transactions block each time. As a result, while other blocks contributed to transaction validation and verification process, thus reinforcing it, their efforts are effectively are wasted when the given transaction block is not added.

Wang et al. [7] have assessed many such pitfalls as they have evaluated blockchain against a maturity model. They evaluate blockchain for four technology maturity parameters as defined by ACM Computing Classification System (CCS 2014) and against the five stages of the Capability Maturity Model (CMM). Blockchain's merits over traditional distributed databases are often debated. A school of thought is that distributed databases are a cheaper option with less power wastage. Peters and Panayi [3] provide a lucid distinction between the two.

7. BLOCKCHAIN CHALLENGES

Regulation is the biggest challenge for non-fiat currency. The rate of technical innovation is surpassing the rate at which regulations catch up. The currency evolution has seen a transformation in the order from fiat currency to e-money to virtual currency to cryptocurrency [9]. Cryptocurrency is the first decentralized version of currency. Some regulatory

bodies hold the opinion that cryptocurrency does no fulfill the functions of money primarily due to its value volatility. [30]

It is a challenge more from the governance perspective rather than from the cryptocurrency user's perspective. There are already reports of Bitcoin being used for illegal activities, drug rackets, money laundering, etc. Trevor Kiviat [14] highlights the difference between at currency and cryptocurrency and the challenges associated with cryptocurrencies regulation. IRS of USA have framed laws for taxation of Bitcoin holdings while Russia is considering banning Bitcoin due to the usage of this unregulated currency for unethical purposes. China also has banned Bitcoins while Australia has passed a resolution to accept Bitcoin transactions. [31, 32]

The Economist (2015) article - The magic of mining [33] highlights a very important challenge of power consumption associated with mining and provides with some examples of how increasing power is being invested in mining activities to earn Bitcoins.

Bitcoin's increasing adoption has led to concerns about the ability of the underlying blockchain technology to scale. Since Bitcoin is a self-regulating system that works by discovering blocks at approximate intervals, its largest transaction throughput is effectively capped at maximum block size, divided by the interval [34]. In their paper, Wei Xin et al. propose various strategies to improve private blockchain scalability. The have recommended and experimentally shown that optimization of parameters like block construction, block size, time control and transaction security can lead to better performance and lower error rates.

In the light of the fact that several international electronic primary financial exchanges have begun to announce they will explore the adoption of blockchain technology in their trade processing and reporting for execution and clearing, Peters and Vishnia [35] examine the current status of regulatory requirements and the challenges faced by market participants in meeting them.

An interesting tradeoff is revealed by the work by Rimba et al. [36] on cost of storage and computation of business processes on a standard cloud environment vs. blockchain environment. As per the results of this experiment costs of a single business process (Incident Management) were higher on Ethereum blockchain than on Amazon SWF. However, the experiment is done for a limited scope of a single business process and the results may not be generalizable, given the day to day advances in blockchain technology towards its optimization.

One key limitation of Blockchain technology is the scalability issue due to size of the public or permissionless blockchain. Blockchain optimization and scalability is an area of much research. In [37], Gencer et al. propose a service oriented sharding technique to achieve blockchain scalability and extensibility.

8. CONCLUSION

In a plethora of blockchain based applications and experiments, faith on the longevity of blockchain technology, is increasing. Scalability and consensus algorithms are areas of growing research in order to make blockchain more adaptable for businesses of larger scale. Areas like taxation, education, insurance are yet to see a major overhaul via blockchain adoption and these can be the focus areas of future research in blockchain. Acceptance of cryptocurrency by governments and establishment of regulations governing them are very important to ensure ethical use of cryptocurrency. The public blockchains also provide an opportunity of mining interesting patterns of cryptocurrency usage, user behaviors and monetary networks across the globe.

9. REFERENCES

[1] Pilkington Mark. 2016 Blockchain Technology: Principles and Applications, Research Handbook on Digital Transformations, Social Science Research Network

[2] Swan Melanie. 2015. Blockchain: Blueprint for a new Economy, OReilly Publications

[3] Peters G.W. Panayi E. 2016. Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money , Banking Beyond Banks and Money, Springer Sep 2016, pp. 239-278

[4] Satoshi Nakamoto. 2008, Bitcoin: A Peer-to-Peer Electronic Cash System, [Online] http://www.bitcoin.org

[5] Buterin, Vitalik. 2015, On Public and Private Blockchains. [Online] https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[6] Xu et al. 2017. A Taxonomy of Blockchain-Based Systems for Architecture Design. 2017 IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 3-7 April 2017

[7] Huaiqing Wang, Kun Chen and Dongming Xu. 2016. A maturity model for blockchain adoption. Financial Innovation, Springer, Open Access, DOI 10.1186/s40854-016-0031-z

[8] Kiran Balasubramanian. 2017, Accenture Labs and Akshaya Patra Use Disruptive Technologies to Enhance Efficiency in Mid-Day Meal Program for School Children. Accenture Newsroom. [Online] https://newsroom.accenture.com/news/accenture-labs-and-akshaya-patra-use-disruptive-technologies-to-enhance-efficiency-in-mid-day-meal-program-for-school-children.htm

[9] Cachin et al. 2017. Blockchain, cryptography, and consensus , IBM Research, Jun 2017, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201703/Documents/Christian%20Cachin%20blockchain-itu.pdf

[10] Decker, Wattenhofer. 2013. Information Propagation in the Bitcoin Network, 2013 IEEE Thirteenth International Conference on Peer-to-Peer Computing (P2P). [Online] http://dx.doi.org/10.1109/P2P.2013.6688704

[11] BitFury group. 2015. Public versus Private Blockchains Part 1: Permissioned Blockchains, BitFury.com whitepapers [Online]: http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf

[12] Crosby et.al. 2016. BlockChain Technology: Beyond Bitcoin, Applied Innovation Review, Issue No. 2 June 2016. [Online]. Available: http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf

[13] Edgeverve-Infosys team. 2017. Blockchain Technology From Hype to Reality: Edgeverve Infosys Finacle Report, Feb 2017. [Online]. Available: https://www.edgeverve.com/wp-content/uploads/2017/02/Blockchain_Technology_From_Hype_t

o_Reality_Infosys_Finacle.pdf

[14] Trevor Kiviat. 2015. Beyond Bitcoin: Issues in Regulating Blockchain Transactions,HeinOnline.org.

[15] Cryptocurrency Market Capitalizations, [Online] https://coinmarketcap.com/

[16] Zyskind et. al. 2015. Decentralizing Privacy: Using Blockchain to Protect Personal Data, 2015 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, July 2015 [Online].Available: http://dx.doi.org/ 10.1109/SPW.2015.27

[17] Sharples M., Domingue J. 2016. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. In: Verbert K., Sharples M., Klobučar T. (eds) Adaptive and Adaptable Learning. EC-TEL 2016. Lecture Notes in Computer Science, vol 9891. Springer, Cham,[Online] Available: https://doi.org/10.1007/978-3-319-45153-4_48

[18] Sony Global Education.2016. Sony Global Education Develops Technology Using Blockchain for Open Sharing of Academic Proficiency and Progress Records, 22 February 2016. http://www.sony.net/SonyInfo/News/Press/201602/16-0222E/index.html

[19] University of Nicosia. 2017. Academic Certificates on the Blockchain. https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain/

[20] Fanning, K et.al. 2016. Blockchain and Its Coming Impact on Financial Services, The Journal of Corporate Accounting and Finance, Wiley Periodicals, Inc. [Online].http://onlinelibrary.wiley.com/doi/10.1002/jcaf.22179/pdf

[21] Microsoft Azure Blockchain as a Service , https://azure.microsoft.com/en-in/solutions/blockchain/

[22] Peter Sestoft. 2017. Autonomous pension funds on the blockchain, IT University of Copenhagen, Dagstuhl seminar, Mar 2017

[23] Nicholson, Lynn. How blockchain technology could improve the tax system, PWC. [Online]. Available: http://www.pwc.co.uk/issues/futuretax/how-blockchain-technology-could-improve-tax-system.html

[24] Xiao Yue et.al.2016. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control, Journal of Medical Systems, Oct 2016, 40:218, Springer Science, DOI 10.1007/s10916-016-0574-6,

[25] Xia et.al. , MeDShare: Trust-less Medical Data Sharing Among Cloud Service Providers Via Blockchain, Jul 2017, IEEE Access, vol 5, pp 14757 - 14767 https://doi.org/10.1109/ACCESS.2017.2730843

[26] Blockchain Voting Used By Danish Political Party, 2014, https://www.cryptocoinsnews.com/blockchain-voting-used-by-danish-political-party/

[27] Follow My Vote, Voting solutions to improve integrity of voting: https://followmyvote.com/contact/

[28] Cognizant Technology Solutions, 2017, https://www.cognizant.com/perspectives/how-blockchain-can-transform-life-insurance-processes

[29] Sun et.al. 2016. Blockchain-based sharing services What blockchain technology can contribute to smart cities, Springer, [Online].Available: http://dx.doi.org/10.1186/s40854-016-0040-y

[30] Gareth W. Peters ,Efstathios Panayi, 2015. Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective, Aug 2015

[31] CNBC News, 2017, https://www.cnbc.com/2017/10/10/bitcoin-price-falls-after-russia-proposes-ban-on-exchanges.html

[32] Australian Taxation Office, https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/

[33] The magic of mining, 8 January 2015, https://www.economist.com/news/business/21638124-minting-digital-currency-has-become-big-ruthlessly-competitive-business-magic

[34] Wei Xin, et.al. 2017. On Scaling and Accelerating Decentralized Private Blockchains, 2017 IEEE 3rd International Conference on Big Data Security on Cloud, https://doi.org/10.1109/BigDataSecurity.2017.25

[35] Peters, G, Vishnia, Guy. 2016. Overview of Emerging Blockchain Architectures and Platforms for Electronic Trading Exchanges, Nov 2016, Elsevier, [Online]. http://dx.doi.org/10.2139/ssrn.2867344

[36] Rimba et.al. , 2017. Comparing Blockchain and Cloud Services for Business Process Execution, https://doi.org/10.1109/ICSA.2017.44

[37] Gencer et.al. Service-Oriented Sharding for Blockchains. [Online]. http://fc17.ifca.ai/preproceedings/paper_73.pdf