Blockchain Computing: Prospects and Challenges for Digital Transformation

Professor Syed Akhter Hossain

Department of Computer Science and Engineering
Daffodil International University, Bangladesh
Honorary Professor, Amity University, India
aktarhossain@{daffodilvarsity.edu.bd, yahoo.com}

Abstract: **A revolutionary trustable sharable computing outcome, the blockchain is essentially a distributed database of records or public ledger of all transactions originated from digital events and shared among participating parties within a computing framework. Each transaction of the chain in the public ledger is verified by consensus of a majority of the participants in the system and its constituents. Once recorded, information can never be erased and neither altered. The blockchain contains a certain and verifiable record of every single transaction ever made during the business operations. In general sense, the blockchain could be described simply as being a way of storing the information of a transaction, between multiple parties in a trustable way. Recording, sharing, storing and redistributing contents in a secure and decentralized way. Being owned, run and monitored by everybody and without anyone controlling it. Besides, avoiding any kind of modifications or abuses from a central authority. Blockchain technology is non-controversial and has worked flawlessly over the last few years and is being successfully applied to both financial and non-financial world applications and listed as as the most important invention since the Internet itself. Besides, digital transformation is taking off as rapid agent for change as part of the global business convergence. In this article, detail of blockchain technologies is presented from the perspectives of digital business transformation along with its future evolutions.**

Keywords: **Blockchain, Bitcoin, Crypto-currency, Business Transformation**

I. INTRODUCTION

A blockchain, the fifth evolution of computing, is essentially a data structure for digital distributed ledger over multiple working system that makes it possible to share data through network of independent parties. It is essentially a distributed database of records of all digital transactions and events which is verified by consensus of a majority of participants in the orchestration of systems [1].

Blockchain is also called chain of trust since the technology of blockchain can support new generation of transactional applications aligned with business processes by establishing the trust, accountability, and transparency. This adds a new domension called “Internet of Value” whereas “Internet of Information” is achieved through different protocols namely TCP/IP for machine communication, HTTP for web content, SMTP for email, and FTP for file transfer along with the new upcoming “Internet of Things (IoT)” for orchestration of devices with Internet [2]. Besides, blockchain facilitates trust and ensures validation of identities without intermediate thrid parties which ensures “Internet of Value” propositions.

In a boarder sense, a blockchain is a peer-to-peer system with no central authority managing data flow. One of the key ways to removing central control while maintaining data integrity is to have a large distributed network of independent users. This means that the computers that make up the network are in more than one location and are often referred to as *full nodes.*

As seen from the literature, there are three different types of blockchains. One is called Public Blockchain, such as Bitcoin [3], which is based on large distributed networks that run through native token. This is open for anyone to participate at any level and have open-source code that maintained by the respective community. The other one is called Permissioned Blockchain, such as Ripple, which control roles that individuals can play within the network. It is also large and distributed system that use a native token.

The third one called Private blockchain which tend to be smaller and do not utilize a token. Their membership is closely controlled. These types of blockchains are favored by consortiums that have trusted members and trade confidential information. All three types of blockchains use cryptography to allow each participant on any given network to manage the ledger in a secure way without the need for a central authority to enforce the rules. The removal of central authority from database structure is one of the most important and powerful aspects of blockchain [3].

An anonymous identity Satoshi Nakamoto is the name used by the unknown person(s) who designed bitcoin and created its original reference implementation. As part of the implementation, the team also devised the first blockchain database. As from the perspective of database administration, blockchain allow different parties that do not trust each other to share information without requiring a central administrator. In each participation, transactions are processed by the network of users acting as a consensus mechanism so that everyone is creating the same shared system of record simultaneously. This creates a database in a distributed manner. Besides, blockchain databases are able to keep

978-1-5090-3012-5/17/$31.00 ©2017 IEEE

information that is relevant now, but also all the information that has come before [4].

As seen from latest trend on the usage of blockchain technology through MIT technology review [5], the potential usages are evolving from health sectors to all business sectors and shaking up the businesses more than the money. Brian Behlendorf, the executive director of the reputed open-source project named "Hyperledger" providing blockchain technologies, commented on using blockchain for carbon emission to health record management in a confernece organzied by MIT Media Lab [5]. As seen from the present practice, the blockchain, on which Bitcoin is built, serves as a distributed, which is cryptographically signed ledger. This makes it possible to track and verify payments without any centralized authority. The encrypted ledger is maintained by computers performing computations that eventually generate more bitcoins. The same distributed cryptographic approach can be used to verify all sorts of transactions.

The rest of the sections are organized as follows. Section 2 elaborates on how block chain works. The digital transformation for blockchain computing is discussed in Section 3. Section 4 discuss blockchain computing platform with prospects and challenges are discussed in Section 5 and conclusion in Section 6.

II. HOW BLOCKCHAIN WORKS?

Blockchain is by itself a data structure which defines logical composition of data storage and principles of security, trust and participation as part of the data operations. As a result blockchain is composed of three core parts as follows.

(a) *Block* – is a list of transactions recorded into a ledger over a given time frame based on size, period and triggering event for block which is different for every blockchain. Block in a chain is just like a book which is a chain of pages.

(b) *Chain* – a hash, calculated on the fly, which links one block to another like book pages. This chaining part is difficult to comprehend. It works as the magical glue to keep blockchains together. The hash is known as the fingerprint of the data and locks blocks in order and time. The secure hash algorithm (SHA) Is used to generate hash functions in blockchains. SHA-256 is a common algorithm used to generate almost-unique fixed-size 256-bit (32-byte) hash. Every blockchain will contain hash to ensure the integrity of the chain.

(c) *Network* – composed of full nodes where each node contains a complete record of all the transactions that were recorded in that blockchain. These nodes are located all over the world and can be operated by any one. As it is difficult, expensive, and time consuming to operate a full node, it is done through cryptocurrency provided by the underlying blockchain algorithm as incentives of blockchain operation. The reward is usually a token or cryptocurrency, like Bitcoin.

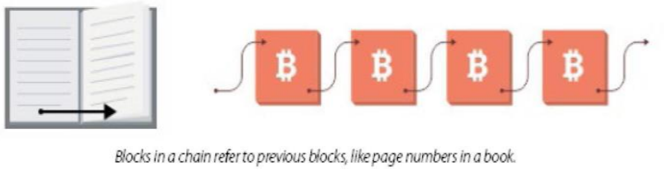

Blocks in a chain refer to previous blocks, like page numbers in a book.

Fig. 1. Blockchain analogy of a Book

The blockchain analogy of a book is shown in the Figure 1 where each page is a block having its content, the Bitcoin, which is chained.

As seen from the present applications, blockchains are powerful tools because of systems that selfcorrect correct data without the need of a third party to enforce the rules. The enforcement of rule is accomplished through their specific required consensus algorithm. In the blockchain computing world, *consensus* is the process of developing an agreement among a group of commonly mistrusting shareholders in order for mutual recognitions. These are the full nodes on the network and are validating transactions that are entered into the network to be recorded as part of the ledger.

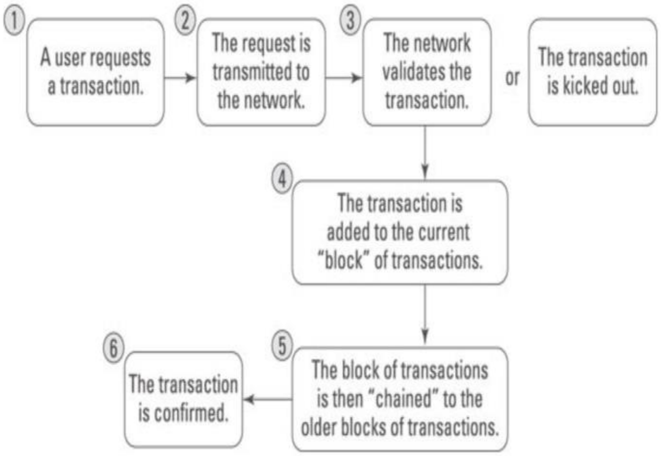

1
A user requests a transaction.
2
The request is transmitted to the network.
3
The network validates the transaction.
or
The transaction is kicked out.
4
The transaction is added to the current "block" of transactions.
5
The block of transactions is then "chained" to the older blocks of transactions.
6
The transaction is confirmed.

Fig. 2. Work process of Blockchain [6]

The work process of blockchain is shown in the Figure 2. Based on the bu iness requirements, each blockchain has its own algorithms for creating agreement within its network on the entries being added. There are many different models for creating consensus because each blockchain is creating different kinds of entries. Some blockchains are trading value, others are storing data, and others are securing systems and contracts etc.

As shown in the Figure 2, the process begins with the request for a transaction from the end user. The requested transaction is broadcasted to P2P network consisting of computers known as nodes shown in step 2. The network of nodes validates the transaction and the user's status using known algorithm or may be kicked out since invalidation. Generally a verified transaction can involve cryptocurrency, contracts, records, or other information. Once verified, the transaction is combined with other transactions to create a new block of data for the ledger. The new block is then added to the exsiting blockchain in a way that is permanent and unalterable. The transaction is then finally confirmed.

III. BLOCKCHAIN COMPUTING FOR DIGITAL TRANSFORMATION

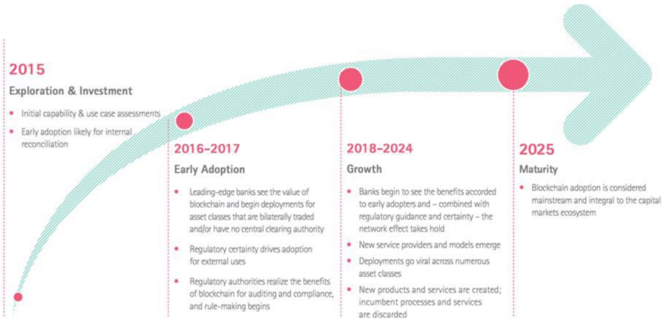
Digital transformation today is an integral part of the business development worldwide. World Information Technology and Services Alliance (WITSA) proposed on “Digital Transformation: Enabling Principle Recommendations for Digital Transformation” on January 2017. As per the recommendations by WITSA, digital transformation is not well formalized and understood yet form the point of view of value creation. Since digital technology is triggering the changes in our society in an appreciable way on continuous basis. As a result, digital transformation affects neatly every aspect of business and government operations encompassing the digital life. Even software development is being digitally transformed and taking seamless integrations. This digital transformation intends to develop or enhance trust, security and privacy challenges.

Digital business process management is an outcome of the digital transformation of business. Blockchain technology is connected to digital business process management. The emergence of distributed and decentralized ledger technologies with smat contracts and Internet of Things (IoT) plan vital role in business development. Blockchain holistically manage business processes interactivity for participatory data sharing and financial relationships.

Most obviously, digital transformation is one of the challenges an enterprise can undertake, but the integration of IoT with blockchain makes it much easier due to the nature of digital emergence. Based on number of partners may it be internal, external, or both, involved in any given business process, a system in which a multitude of electronic parties can securely communicate, collaborate, and transact without human intervention is highly agile and efficient. This digital business cohesion brings productivity and efficiency in the business.

Despite obvious benefits and productivity, blockchain technology has been slow to catch on in the enterprise due to knowledge gap along with the skills. One major reason is a general lack of standards. For example, should an organization use an open network or a privte one? Who should regulate the technology to make sure blockchains are effectively regulating themselves, and what cybersecurity threats might arise that threaten a blockchain’s integrity?

As seen despite Bitcoin surge of August 2017, and with blockchain still in its infancy, these are all questions that financial institutions are beginning to answer as they experiment with different implementations.


2015
Exploration & Investment
Initial capability & use case assessments
Early adoption likely for internal reconciliation
2016–2017
Early Adoption
Leading-edge banks see the value of blockchain and begin deployments for asset classes that are bilaterally traded and/or have no central clearing authority
Regulatory certainty drives adoption for external uses
Regulatory authorities realize the benefits of blockchain for auditing and compliance, and rule-making begins
2018–2024
Growth
Banks begin to see the benefits accorded to early adopters and – combined with regulatory guidance and certainty – the network effect takes hold
New service providers and models emerge
Deployments go viral across numerous asset classes
New products and services are created; incumbent processes and services are discarded
2025
Maturity
Blockchain adoption is considered mainstream and integral to the capital markets ecosystem

Source: Accenture Research

Fig. 3. Blockchain adoption – Accenture Research

As seen from the Figure 3, based on the research work published by Accenture, one thing that may be of surprise is that while maturity of blockchain will likely take 5+ years.

Business process transformation faces reality is that most businesses operate under some form of existing regulation, are either themselves an intermediary, or are working within an eco-system of value chain partners that are intermediaries. In order to transform for blockchain, dis-intermediating the central authority or the middleman as its main goal, it raises some concerns as well as presenting new opportunities. For business transformations, every organizations need to design business drives based on blockchain to explore blockchain technology via a proof-of-concept. Before starting with a particular solution or selecting a vendor, it is critical to assess the many considerations that come into play when selecting the best approach to exploring blockchain.

Business transformation to deploy blockchain requires deep analytics of business based on the following perspectives:

a. Impact of implementing blockchain in business

b. Impact on customer experiences

c. Impact on partner’s eco-system

d. Ensuring privacy, security and integrity

e. Use cases appropriateness for blockchain

f. Platform selection and implementation design

g. Handling regulatory requirements

h. Transformation project planning

IV. BLOCKCHAIN COMPUTING PLATFORMS

There are different blockchain platforms for rapid prototyping of solution based on specific goals. Blockchain implementation platform is purely based on subjective assessment and business requirements. The different platforms are: Ethereum, Multichain, Hyperledger, HydraChain, OpenChain, and IBM Bluemix Blockchain.

Ethereum is an open blockchain platform that provide resources and use cedntralized applications that utilizes blockchain technology. It is an open-source project. It is adaptable and flexible unlike the Bitcoin protocol. Ethereum facilitates Python, Go and C++ language interface to work with. Multichain is a platform for the creation and deployment of private blockchain either within or between organizations. It facilitates deployment of blockchain technology in financial sector. It provides the Bitcoin level private financial transactions. Multichain supports Python, C#, JavaScript, PHP and Ruby language interfaces. The Hyperledger is an open-source collaborative platform to advance cross-industry Blockchain technologies. It is a global collaboration encompassing field of finance, banking, Internet of Things (IoT), supply chains, manufacturing and technology. Hyperledger is based on Python. HydraChain is a join development effort of brainbot technologies and the Ehtereum project. HydraChain is also based on Python. OpenChain is based on partition consensus system for validating transactions depending on the assets being exchanged. OpenChain is based on JavaScript. IBM has also released Blockchain platform as part of the Bluemix service catalog. It is built on the top of HyperLedger.

V. PROSPECTS AND CHALLENGES

With the collaborative development of technologies, blockchain adds more capabilities and as an outcome its underlying ledger system becomes more dynamic and self-governing and self-organizing. Despite the challenges of adoption, several industries are exploring how blockchain technologies can be used to transform their business model and change their operating assumptions. Major banks and financial companies such as Bank of America, Santander, Barclays, Goldman Sachs and NASDAQ are piloting the technology's capabilities in data registry and smart contracts for cross-border payments, remittances, micropayments, trade finance, loans, securities and derivatives trading. Organizations across different industries worldwide are experimenting with blockchain to determine how it can be leveraged to disrupt current business models, increase profitable growth, and enable more efficient operations.

Blockchain as an emerging technology goes through a hype stage over the passage of the year 2016. It is natural that takes a while to get the kinks out and for pilots and proofs of concepts to prove use cases and shift the curve to broad adoption of blockchain in business processes. The power and disruption of blockchain is evident in the news almost daily, and people are beginning to understand how blockchain distributed ledger technology works at recent times.

There are potential issues to adoption of blockchain in business domain. Regulations play a vital role in the adoption of blockchain. It is often observed that regulatory entities often lag technology innovation, and this is certainly the case with blockchain. As new products and services are evolving based on blockchain transactions, but there are currently no regulations on how the transactions should be written. The second very important issue is Standard. Along with the regulations, there is currently lack one common set of standards for writing transactions on a blockchain. In fact, there are three open source consortium organizations, each with its own standards and code which creates anomalies in attaining boarder sense of unified approaches.

Another very important issue to adoption is Validation issues. The general fear of the technology which has not been tested enough in pilots and POCs. Ultimately, what are blockchain's limitations? Early POCs validate its scalability, but what are its limitations for handling a large volume of enterprise transactions and data? Different applications will face different scalability issues as adoption increases. And how much time and computing power will be necessary to process a huge number of transactions? This is vital for the long term sustainable blockchain technology.

VI. CONCLUSION

In this article, blockchain technology is discussed from the perspectives of business process and operational viewpoints. It is evident that blockchain technology has the potential to upend if not transform industries. However, before it can become mainstream, there are numerous challenges to overcome. A key challenge associated with blockchain is a lack of awareness of the technology and how it works. The skills required to implement blockchains are often beyond the traditional IT skill sets.

Thus, it is imperative for carriers to understand how others – competitors and peers – have implemented blockchain, and gaining equivalent knowledge of blockchain applications.

REFERENCES

[1] Bitcoin transactions per blocks. https://blockchain.info/charts/n-transactions-per-block

[2] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". www.bitcoin.org, 1 November 2008. www.bitcoin.org/bitcoin.pdf, accessed 20 June 2017.

[3] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timon, andP.
Wuille. Enabling Blockchain Innovations with Pegged Sidechains. White paper, Blockstream, 2014.
https://blockstream.com/sidechains.pdf.

[4] Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In 2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17-21, 2015, pages 104–121, 2015

[5] Narayanan, James Grimmelmann & Arvind. Slate: Bitcoin's blockchain technology won't change everything. Slate. [Online] February 16, 2016. http://www.s late.com/articles

/technology/future_tense/2016/02/bitcoin_s_blockchain_technology_won_t_change_everything.html

[6] J. A. Kroll, I. C. Davey, and E. W. Felten. The economics of bitcoin mining, or bitcoin in the presence of adversaries. In WEIS 2013.