Panel 3 Position Paper: Blockchain can be the Backbone of India's Economy

Manish Nagaraj[1] and Somali Chaterji[2]

***Abstract*—There has been an increase in the interest in blockchain technologies. While the most popular application of this technology is in the cryptocurrency sector in the developed world, recent studies have shown that they hold promise toward deployment in many sectors such as digital contracts and healthcare in the developing world. This article discusses the various use cases of the blockchain technology, particularly from the point of view of developing countries in general and for India in particular.**

I. Introduction

Blockchain, the technology underpinning cryptocurrency, such as, Bitcoin and Ethereum, is a state-of-the-art, cryptographic, distributed *and* decentralized ledger of records or blocks, with the potential to remove the middlemen from all transactions via the use of validators or "miners". It was the brainchild of Satoshi Nakamoto, pseudonym for the person or consortium that resulted in the invention in 2008. While this technology was originally devised for the digital cryptocurrency, Bitcoin, other potential use cases of this technology have long surfaced. The blockchain ledger works by permanently recording, in chronological blocks, the history of all transactions that occur between peers in the network. All validated transactions are recorded in the form of a chain of blocks, hence the name "blockchain". In terms of which chains are the most trusted chains, proof-of-work protocols or functions are what create *distributed, trustless consensus*. The result is that the longest chain has the network's consensus and is the correct one and forks in the chain are discarded.

The *International Data Corporation* (IDC) coined the term 'third platform' for a computing platform model. These platforms provide computing anywhere, whether mobile computing, social networking, cloud computing, or big data analytics, essentially transforming the way people and business relate to technology. Michael Versace, the research director for digital strategies at IDC describes third-platform technologies, such as blockchain, as accelerators for the industry and innovation [1].

Although the popularity of blockchain technologies is higher in developed countries, [2] claims that the greatest impact of these technologies will be in the developing world. The *World Economic Forum* report stated that by 2050, 10% of the global domestic product will be stored using blockchain technology [3]. This incentivizes developing countries toward greater adoption of the blockchain technologies. Such adoption is motivated by the presumed lack of trust in central banking organizations in some developing countries. However, the adoption also meets significant headwinds due to the lack of understanding of the technology and the lack of standardization and well-known commercial ventures providing services in this space.

This project is supported in part by the Lilly Endowment's Grant for the Wabash Heartland Innovation Network (WHIN).

[1]Manish Nagaraj is a PhD student in Purdue University's School of Electrical and Computer Engineering

[2]Somali Chaterji is an Assistant Professor in the Department of Agricultural and Biological Engineering, Purdue University, West Lafayette, IN 47907, USA. schaterji at schaterji.io

II. The Blockchain Technology

Blockchains are distributed immutable ledgers that provide provenance information of all transactions that have been executed and shared by all the participating entities. Each transaction is verified by a mass collaboration of the participating entities. Blockchains eliminate the possibility of equivocation or double spending. Plus, it also affords automation of trust among multiple parties, removing the need for trust-based overheads. This comes from blockchain's focus on *distributed consensus*. Both these properties make blockchains suitable for diverse applications, as summarized in this article.

The basic unit of a blockchain is called a 'block'. These blocks contain some data, which depends on the type of blockchain used and the application. The process of collecting and fitting data into blocks is referred to as *mining*. A cryptographic hash is used to identify each block. A hash function is a *random oracle*. It takes an input of any size and responds with a unique query in the output domain. It responds in the same way each time the input is passed. A cryptographic hash function has three important properties that make it secure. They are:

1) *Pre-image resistance:* A message m cannot be determined given a hash value (or output value) h, such that $hash(m) = h$. Hence, the adversary cannot trace back the input from the output.
2) *Second pre-image resistance:* It is difficult to find a message m_2, given a message m_1 such that $hash(m_1) = hash(m_2)$. Hence, the adversary cannot replace the original data without modifying the output of the hash function.
3) *Collision resistance:* It should not be computationally impossible to find two messages m_1 and m_2 such that $hash(m_1) = hash(m_2)$. This ensures that the adversary cannot use two different messages in creating the blocks.

These three properties ensure that the identification of the block can be verified. Cryptographic hash functions are sometimes referred to as the digital fingerprints of the block. Each block also contains the hash of the previous block. This helps in linking the blocks to form blockchains. The first block of the chain does link to the hash of any previous block. This is known as the *Genesis block*. Tampering with one block would

978-1-5386-7902-9/19/$31.00 ©2019 IEEE

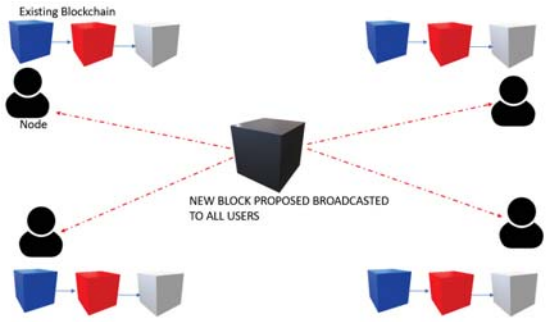

Fig. 1. Proposing a new block

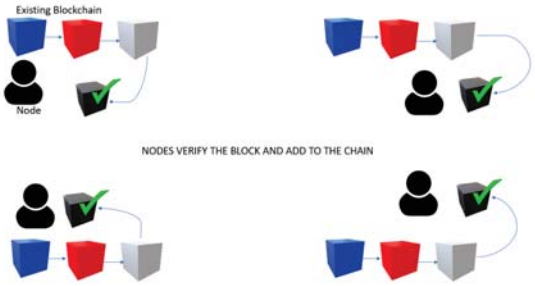

Fig. 2. Adding a new block to the chain

imply that that the hash of that block changes. The blocks that are committed after that will not have a reference block and hence the chain breaks. This provides a safety net and ensures that blocks may not be tampered with. *Forking* is the process in which two blocks build upon an existing chain. This could be due to them being computed within a short time interval or both achieving the necessary conditions to be committed or added onto the chain. Blocks thereafter can be committed to either chain. Both these chains will be valid. As the mining process continues, one of the chains becomes longer and the longer chain would be accepted by the network. In order for a transaction to be added to the blockchain, the proposer prepares the block and sends it to all the nodes in the network (Fig. 1). The nodes verify whether the block is valid and adds it to the blockchain (Fig. 2).

As computer systems advance, it becomes more possible for them to compute hash functions more efficiently and exploit the blockchain algorithm. A malicious entity can use more resources to get a better control of the blockchain. In order to prevent this, blockchain algorithms make use of many *controlled block generation time* techniques. Two popular techniques used are the Proof-of-Work (PoW) and Proof-of-Stake (PoS). These techniques provide an additional difficulty in adding a block to the chain. In order to tamper with one block, all the successive blocks must be recomputed and hence require high computational power. Since systems are limited by their computational power, it is more difficult to tamper with the blockchain. Blocks may also contain simple programs that dictate rules such as exchanging coins based on certain conditions. These simple programs are called *smart contracts*.

Blockchains can be *unpermissioned* or *permissioned*. If all the entities in the network have equal access to the chain in terms of both accessing information and appending blocks, the blockchain is referred to as unpermissioned. In contrast, in certain applications, such as in the healthcare industry, only the patient and the entities granted access to the information, are able to access the blocks. The control of access could be practiced through cryptographic techniques. Such blockchains are called permissioned blockchains.

III. Financial Inclusion and Global Banking

A common problem faced in developing countries around the world is the increasing gap between the rich and the poor. Many of the people in these parts of the world do not have access to banking facilities and are referred to as 'unbanked' people.

According to the World Bank, about one million of these unbanked people have access to phones and around half of those have access to the internet [4]. Although mobile banking exists in these countries, it is infeasible for a bank to perform transactions below a certain threshold. Yet, with cryptocurrency, the poorer citizens can perform these microtransactions. These people can then create an online cryptocurrency wallet and perform transactions online. Another advantage of using blockchains in microtransactions is that one does not need a collateral as there is a higher level of trust embedded right within the technology. However, the devices available to most people in developing countries have poor connectivity and the connection is not continuous. Existing blockchain techniques need to be modified before they can be used to provide financial inclusion to the unbanked masses. A good example of the success of such systems is *BitPesa*, which was launched in 2014. This enabled the citizens of Kenya to convert their virtual money into the local currency.

Many citizens of developing countries often work abroad and need to transfer their earnings overseas back to their families. Online bank transfers often have high fees and remittance fees. With the introduction of blockchains, one can circumvent the need for middlemen and hence the remittance fees can drop significantly. The *Noah Project* aims in helping achieve just that [5]. It helps overseas workers from the Philippines to transfer money. The statistics from the Philippine Statistics Authority state that this makes up to 10% of their GDP. The remittance fee is projected to drop as low as 2% to 3%.

Blockchain technologies and financial inclusion also eliminate the need for middlemen when it comes to selling crops. This creates a peer-to-peer platform for trade, where farmers can transact directly. This could possibly help in reducing price dictation by monopolies.

IV. Transparency in Governance

One of the main features of a blockchain technology is the high level of trust embedded within the system. Corruption appears to be a problem in many developing countries. [6] states that corruption is centralized and a small group of people have access to most of the power and resources. Blockchains provide a publicly accessible ledger, which cannot be modified

by corrupt entities. Hence, this provides transparency and has the potential to reduce corruption. Property records, birth and death records, and other official records can also use blockchain technologies.

Converting existing ledger methods to blockchain technologies also simplifies the process of registration of records. Smart contracts ensure that payments are irreversible and cannot be tampered with. This could prevent illegal seizures of lands based on false land deeds. One implementation of this is in the Republic of Georgia. There, *BitFury* [7] is working along with the National Public Registry to use a secure ledger for maintaining the land records. It is projected that this could reduce property registration fees by up to 95%.

As many of these documents can be counterfeited, the verification of the originality of the document can be a tedious process. Blockchain technologies, which provide an inbuilt layer of trust, eliminate the need for a tedious verification process. *Factom* is a startup that utilizes blockchain technology on securing data [8]. One of the projects that Factom is working on is the Honduran Land Registry Project where public ledgers are being created. This helps in creating permanent records to prevent illegal land seizures through violence. The *Dubai Blockchain Strategy* is another example of utilizing blockchains for maintaining records of government-issued documents. The project aims to move all the documents to blockchains by the year 2020 [9].

V. Health Care

Although traditionally blockchains are not meant to be used in the healthcare sector, recent studies have demonstrated the myriad use cases of such systems in the healthcare industry. These vary from public health record management to counterfeit drug handling [10]. The *World Health Organization* estimates that around 10% of the drugs available in the developed world are counterfeit while up to 30% of them are counterfeit in developing countries [11]. This is a crucial issue and must be addressed. Counterfeit Medicines Project launched by *Hyperledger* tries to address this issue [12].

Another issue that can be addressed is making medical health records more trustworthy and publicly accessible. The people and organizations that will benefit from using blockchains include hospitals, practitioners, and insurance agencies. This also reduces the time taken to receive and process such information. *Guardtime*, a healthcare platform is collaborating with the government of Estonia to provide medical information using the blockchain technology [13]. Health Insurance companies have been able to access the medical and medical related data from the trusted source.

VI. Blockchain, privacy, and decentralized federation

Blockchain technology is potentially helpful for identity and access management (IAM) in federated infrastructures, as envisioned in [14]. By combining cryptographic hashing with blockchain technology, one can bring one's own identity, i.e., the BYOI paradigm, to the federated platform (such as MG-RAST [15], the largest metagenomics repository that would benefit from such decentralization) and can receive the proper authentication. For example, the cryptographic SHA256 hash computational algorithm would return a 64 digit, fixed length set of numbers called a hexadecimal signature for an input transaction (say, for personal genomic records of an individual or metagenomic signature of one's gut flora). Thus, changing even a single attribute in the input would create a distinct and random hash value, however, the same set of records would transform into the exact same hash value. By altering the hash of the input transaction, the access credentials of this input will change, allowing for different access credentials, for example. On the algorithmic side, Hash values are in turn combined into Merkle trees—the simplest one being the binary Merkle tree, with more complex Merkle trees being possible such as the "Merkle Patricia tree" being used in Ethereum. The block's header now contains all of these hashing results, along with a hash of the previous block's header. This time-stamped header then becomes a part of a cryptographic puzzle solved by manipulating a number called the nonce. Once this puzzle is solved by miners (who then get a small reward), this new validated block is added to the blockchain. Thus, for every human, a hash of all the personal information can be created and the personal information need not be stored. Then, when the time comes to check the identity of an individual, the identity can be checked against the archived hash without the validator ("miner") needing a copy of the original digital information deck. This is going to come in handy as more and more genomics, epigenomics [16], and metagenomics datasets pertaining to an individual are generated, including being amassed by the patient herself and the associated digital liability. There is increasing trend toward the use of cloud infrastructure for genomic analyses and a slowly emerging trend of protecting such computation with the use of privacy-preserving transforms such as cryptography and obfuscation. Now, with the maturation of the blockchain technology, it may well serve as the new organizing paradigm for healthcare-related data.

One challenge to its adoption in IAM for federated infrastructures is that with the current bitcoin-based blockchain design, large amounts of raw data cannot be stored in a single block *yet*, so one full genome in one block is not possible. One solution would be to hash the genomic data file and store this hash file and information about the file's location in a blockchain transaction. However, the file will still need to be stored securely, which can be solved by the approach used by Proofofexistence.com to securely store the distributed proof of the existence of any document. Alternately, the genomic data can be divided into multiple blocks and a peer-to-peer storage network can be used. File metadata can also be stored on a blockchain. One risk, of course, is to see if the blockchain technology actually scales if used truly widely, much beyond its current use to store volumes of genomic and metagenomic data in a truly distributed, multi-organization federation.

In the arena of identity and access management (IAM), again, the blockchain technology can allow the enterprise to decouple the identity from existing applications. This can enable focus on access control at a fine granularity in concert with a blockchain-based identity, as encrypted using a hash

function, as described above.

VII. Incentives for Renewable Energy

It is very important for us to explore and invest in renewable sources of energy. However, developing countries often lack the motivation and desire to do so, due to the absence of infrastructure and the high initial costs. Blockchain technologies can reduce transaction costs and help in incentivizing the generation and distribution of renewable energy [17]. Developing countries can utilize distributed low-cost renewable energy sources to help meet their growing energy demands. The increasing popularity of cryptocurrency can also help instigate the private markets to come into play.

One example scenario for the use case of blockchains in this sector is explained in [17]. A villager can set up a small-scale, solar power-generation unit. This may then be sold to other members of the community as a *pay-as-you-go* service, using cryptocurrency. If more members of the community wish to set up more generators, then smart contracts allow the members to buy and sell energy from one other at low transaction rates. The trustworthy feature of blockchains allows the process to be more automated and hence prevents corruption by entities.

VIII. Conclusion

The senior operations officer at the world bank, Mariana Dahan who was in charge of the 2030 development agenda explained that the blockchain will play a key role for the 2030 Development Goals adopted by UN members due to their trust element. It was further added that these technologies will be designed to eradicate poverty and to ensure prosperity.

Although there are significant problems in utilizing blockchain technologies in the developing world, such as lack of infrastructure, there are many ongoing works that aim to address these issues. Case scenarios like that of Uganda and Senegal's birth registration using Orange's Mobile Platform where village representatives and hospitals are equipped with mobile devices and are responsible for sending data of births provide hope and motivation to explore the idea of blockchains in developing countries further.

Blockchains can play a crucial role in the case of India, which works in an informal economy. Nearly three-fourths of the transactions rely on interpersonal trust. Hence, trust is a very important factor in India. It was estimated in 2017, that nearly $2 billion USD is lost via fraudulent loans. Blockchains provide an opportunity to facilitate a trustworthy transaction environment. A good example of proactive work in the blockchain arena in India can be seen in the state of Andhra Pradesh. It launched the '*Fintech Valley in Vizag*' program. It aims to build a financial technology ecosystem. Although the state has invested in blockchain projects, such as maintaining land records and vehicle registrations, it still lacks a full-fledged system for widespread adoption. With programs such as the twelve-week course to learn blockchain architectures being launched by the collaboration between IBM and Indian e-learning Platform National Program, there is hope for innovation by the burgeoning and educated youth in India.

India faces many hurdles before blockchain technology can become mainstream here, if at all it does. The recent Supreme Court decision to uphold RBI's decision to keep financial institutes from working with cryptocurrencies is one example. India can only make progress and fully utilize all the use cases of blockchains through collaboration of the government, the industry, and technical researchers. If successful, it holds the promise of increasing transparency, reducing the burden on the public toward generating and obtaining official records, and performing micropayments in a safe and secure manner for a repertoire of goods and services.

References

[1] S. Underwood, "Blockchain beyond bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[2] A. Castor, "Blockchain's greatest impact will be in developing countries, says upenn lecturer," Feb 2018.

[3] D. Shift, "Technology tipping points and societal impact," in *World Economic Forum*, 2015.

[4] "How blockchain can eradicate poverty in third-world countries," Apr 2018.

[5] "Blockchain forces a breakthrough in developing countries," Oct 2018.

[6] B. A. Olken, "Corruption and the costs of redistribution: Micro evidence from indonesia," *Journal of public economics*, vol. 90, no. 4-5, pp. 853–870, 2006.

[7] L. Shin, "Republic of georgia to pilot land titling on blockchain with economist hernando de soto, bitfury," *Forbes. April*, vol. 21, 2016.

[8] P. Snow, B. Deery, J. Lu, D. Johnston, and P. Kirby, "Factom business processes secured by immutable audit trails on the blockchain," *Whitepaper, Factom, November*, 2014.

[9] S. Dubai, "Dubai blockchain strategy," *Smart Dubai, Dubai Government, Dec*, 2016.

[10] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–3, Sep. 2016.

[11] J. Morris and P. Stevens, "Counterfeit medicines in less developed countries," *International Policy Network, London*, 2006.

[12] P. Taylor, "Applying blockchain technology to medicine traceability," 2016.

[13] O. Williams-Grut, "Estonia is using the technology behind bitcoin to secure 1 million health records," *Bus Insid*, 2016.

[14] S. Chaterji, J. Koo, N. Li, F. Meyer, A. Grama, and S. Bagchi, "Federation in genomics pipelines: techniques and challenges," *Briefings in bioinformatics*, 2017.

[15] F. Meyer, S. Bagchi, S. Chaterji, W. Gerlach, A. Grama, T. Harrison, T. Paczian, W. L. Trimble, and A. Wilke, "MG-RAST version 4–lessons learned from a decade of low-budget ultra-high-throughput metagenome analysis," *Briefings in bioinformatics*, 2017.

[16] S. G. Kim, M. Harwani, A. Grama, and S. Chaterji, "EP-DNN: a deep neural network-based global enhancer prediction algorithm," *Scientific reports*, vol. 6, p. 38433, 2016.

[17] J. Thomason, M. Ahmad, P. Bronder, E. Hoyt, S. Pocock, J. Bouteloupe, K. Donaghy, D. Huysman, T. Willenberg, B. Joakim, L. Joseph, D. Martin, and D. Shrier, "Chapter 10 - blockchainpowering and empowering the poor in developing countries," in *Transforming Climate Finance and Green Investment with Blockchains* (A. Marke, ed.), pp. 137 – 152, Academic Press, 2018.