JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Study on the Usage and Regulatory Issues of Blockchain Technology in the Government and the Public Sector

Anuj Jain
Law Student, NMIMS Kirit P. Mehta School of Law, Mumbai - 400056

Abstract: With the emergence of cryptocurrencies as the currency of the future, blockchain has also received a lot of attention in the last decade. Though it is unsure whether cryptocurrencies are going to stick around or not, it is clear that the technology that cryptocurrencies are based on, i.e. the blockchain technology is going to become an impactful part of our lives. This is because blockchain technology can be integrated in many fields to increase efficiency, transparency and reliability. Government functions tend to benefit the most from the technology as they have many stakeholders, and an urgent need for the aforementioned qualities. But the main obstacle in its implementation is the lack of awareness. While it is true that almost everyone is aware of the existence of blockchain, most do not understand what it actually is or how it functions. Further, such ignorance leads to unawareness of the possible uses of the technology. Thus, this paper will try to explain the basics of blockchain technology in the simplest way possible and then provide examples of how governments around the world have already implemented the technology in their own systems. The aim is to widen the perspective of the reader around the various applications of the blockchain technology. Further, the paper will also discuss the possible regulatory issues that might be faced during the implemention.

Keywords – Blockchain Technology, Government, Public Sector, Cryptocurreny, Regulatory Issues.

I. INTRODUCTION

Blockchain is a technology that creates a reliable service in an unreliable environment. It utilizes distributed technologies to provide a decentralized service that accomplishes the same objectives as a trustworthy, centralized service. Since 2008, the deployment of the blockchain has expanded, spurred mostly by its capacity to enable any kind of digital transaction. Wall Street investment companies have embraced Blockchains to allow transaction cost reduction, Silicon Valley startups to raise funding via initial coin proposals and a single nation, Venezuela, to promote worldwide investment. The algorithms that drive these dispersed transactions have led to a whole new approach for the safe and often contradictory storage of data in a digital environment. Since blockchain ensures high service availability and data integrity, any sector in which a trusted third-party transactions or processes are used or where a strong security guarantee is needed may consider adopting blockchain solutions, as governments globally should.

II. THE CONCEPT OF BLOCKCHAIN

Three distinct levels may be abstracted from the blockchains. Layer 1 is at the heart of the blockchain: BFT-Consensus, commonly known as the state replication of the machines. There are many types of BFT consensus, ranging from traditional BFT protocols to PoW-based consensus. Although the consensus reaches essential distinctions, every form must resolve the same problem: how to allow nodes to reach an agreement about the entire order (i.e. consistency) of transactions provided by clients as requests. After nodes achieve an agreement on the order, the transaction data/operations are processed in the order of the transactions. As a consequence, dispersed nodes act as if there were a centralized node. This guarantees that there is only one series of customer transactions called the "longest chain." Blockchain's layer 2 is the smart contract, which is basically software code. A smart contract offers blockchain developers with an interface to add new functionalities. smart contracts can then simplify, verify or enforce business transaction performance. A smart contract may be seen as a software connecting layer 3, applications and use cases, with the underlying consensus mechanisms.

The cryptographic principles of hashing and digital signatures make the transactions tamper-resistant and provide validation. One way hash functions produce a unique alphanumeric text output given the transaction list input. Change the list of transactions for one item and the resultant hash is substantially different. The "sign-in" transaction includes digital signatures such as Rivest–Shamir–Adleman or Elliptic Curve Digital Signature Algorithm. The hashes are then connected in a block chain, with each other, except for the first one, which is termed the genesis block. Such a hash chain guarantees that nobody can handle any block's contents or reverse the chain order.

Layer 1: BFT Consesus

All blockchains strive to help decentralized nodes reach agreement by means of encryption and a consensus mechanism on the overall sequence of transactions. Technically speaking, blockchains usually fall into one of two categories:

1. Permissioned Blockchains: Permissioned blockchains offer consensus and security utilizing secure protocols of distributed consensus. Consensus methods do not require costly processes like PoW. Thus, authorized systems have a short latency (the time between the customer's transaction and the response), are also scalable (both in the number of customers and transactions and the number of servers) and use less energy than unauthorized blockchains.

2. Permissionless Blockchain: Most Permissionless blockchains use a "Proof-of-Something" approach. In the case of Bitcoin, This is a PoW, a mathematical challenge that offers all nodes in the system to attempt to overcome (or work through) the so-called mining activity. Once mined, if the request is approved, a node may propose a bloc of transactions and be paid in Bitcoin. The disadvantage of this method is that the performance (the number of transactions per second) is restricted and the energy consumption is significant. In addition, there is cooperation, which is known as cartel-like organisations called mining pools, and mining activities are concentrated under one group's control. The blockchain becomes less decentralised and therefore less safe, and more likely to attack and manipulate using mining pools.

Layer 2: Smart Contracts

Smart contracts are self-executing programmes that activate when nodes reach a consensus without the need for human interaction. Smart contracts are not the same as the contracts that most people are familiar with. Instead, the nodes of a blockchain are set up to check a set of conditions to see if the triggering criteria have been met. If the conditions are met, the nodes will run a contract, which is a software that performs business-defined functions. Smart contracts allow users to add new features and functions to their blockchains without having to shut down their services. Developers could, for example, create a new smart contract with a set of functionalities. Authorized users might call the contract after it was implemented on the blockchain to use those functions. To enable these new tasks, other blockchain-based services do not need to be disrupted in any way. The Ethereum Virtual Machine (written in the Solidity programming language) and Hyperledger Fabric's Chaincode are the two most popular smart contract platforms (written using a combination of the languages Go, node.js, and Java).Because all blockchain transactions are included in the hash chain and thus immutable, a fault in the contract or a weakness that may be exploited puts the system at danger. It's also worth mentioning that, according to numerous research studies, using smart contracts will most certainly decrease the system's performance.

Layer 3: Applications and Use Cases

There are numerous applications and uses of the blockchain technology like Secure sharing of medical data, NFT marketplaces, Music royalties tracking, Cross-border payments, Real-time IoT operating systems, Personal identity security, Anti-money laundering tracking system, Supply chain and logistics monitoring, Voting mechanism, Advertising insights, Original content creation, Cryptocurrency exchange and Real estate processing platform. In this paper, the researcher will be focusing on the applications and uses of blockchain technology in the government and the public sector.

III. GOVERNMENT ADOPTION OF BLOCKCHAIN TECHNOLOGY

The researcher examined the known initiatives and used examples sponsored by governments worldwide. The objective of this article is to offer a thorough but not complete, representative list. The aim is to describe some representative and relevant applications. In fact, applications in possibly all sectors may be found with growing interest in blockchains. However, many of them are far from practical or helpful. The researcher thus chose just the representative instances of usage and categorized them by country and area. This will make it simpler to observe the trend in instances of government usage. Blockchain government acceptance may be seen from regulatory, consumer and developer viewpoints. As a regulatory authority, a state may want, as with cryptocurrencies, to oversee how blockchains are utilized. Governments may utilize blockchains as an application user to enhance procedures. And a government may sometimes build its own blockchain-based application to meet an internal need.

1. U.S. Government

The U.S. Department for Health and Human Services (HHS) has created a contract management tool called 'Accelerate' which uses blockchain, AI, ML, and process automation. Accelerate is intended to better manage the HHS portfolio of approximately $25B worth of 100,000 contracts across around 50 systems. The Accelerate blockchain captures an indication of unstructured data (for example, documents) instead of storing the data itself. Accelerate was able to obtain contractual information throughout the entire administrative process through data replication and became the first federal blockchain application to be certified by a designated approving authority, an internal senior management officer, for authorization to operate, indicating that the system is of an acceptable level of risk and that it can be used for use in the government. Acceleration has been extended into procurement management, providing researchers with contract information easier to locate appropriate material for their study. At the time of acquisition HHS has anticipated savings of up to $720M over time and may extend Accelerate into clinical data – HHS leadership has been discussing utilizing blockchain in septic tracking.

The U.S. Centers for Disease Control and Prevention (CDC) are carrying out research to utilise blockchain to monitor epidemics in public health such as hepatitis A[96]. In 2017, the Center for Surveillance Epidemiology and Laboratory Services' leading software architect started developing proof of the idea of better surveillance across state borders. Since then, the CDC and IBM have been working together to find a blockchain-based solution to track the ongoing crisis of opioid disease. The researcher presumes that blockchain is a factor to monitor COVID-19. Despite many years of no published research, the interest in blockchain in medicinal applications is increasing fast. Most of these articles are for theoretical study, with few addressing blockchain implementation. Many highlight the tamper resistant characteristic of blockchain as well as its distributed nature, attributes important to interoperability with health data. These blockchains are often privately permitted; Ethereum is being investigated because of its smart contract capabilities and Hyperledger Fabric since it is open source supported by major businesses such as IBM.

2. Asian Governments

In 2019, the Philippine government approved the use of an Ethereum-based system to provide financial services to about 80 rural banks. The fact that just 42% of Filipinos aged 15 and above have a bank account, owing to a variety of circumstances, motivates the endeavour.

The notion of a blockchain city has been implemented at Melaka Straits City in Malaysia, a tourism destination financed by the Chinese government. The initiative seeks to track tourist permits, passengers, luggage, and booking services using blockchain. The city will also administer its own token, the DMI coin, which will let visitors to convert their cash into digital currencies and pay for goods and services in the city using their mobile phones.

The government of South Korea has announced a 4 billion won ($3.5 million) grant to build a blockchain-enabled virtual power plant in Busan, the country's second-largest city. To maximise power generation, the power plant should be cloud-based and integrate different energy resources.

3. European Governments

The European Horizon program promotes European Union-wide blockchain projects. In 2017, Luxembourg started a Luxembourg digital project focusing on creating a governance blockchain infrastructure. The aim is to create a blockchain community of skills and to develop blockchain governance standards.

E-Estonia offers a range of functions, including e-identity, e-healthcare and e-governance. Many are now operational, with 98% of Estonians submitting tax filings online and 99% of their health information being

digitized and kept on blockchain. Although problems and concerns persist, the manner in which the government keeps and processes data has truly transformed the blockchains.

Nations like Georgia and Sweden (and non-EU countries like Switzerland) utilize asset management blockchains. Georgia (at the crossroads of Asia and Europe) developed a land title registry blockchain and associated property transactions that helped improve efficiency of the process. Sweden has also developed a blockchain-based registration and immobilization application.

Blockchain was also used in teaching. The Maltese administration has just completed the first national blockchain pilot to administer academic credentials such as diplomas, school certificates and transcripts. This has shown to enhance the security of personal data, to reduce bureaucracy and to make it easier for students to access their credentials..

IV. REGULATORY CHALLENGES

1. Legal framework regarding the legal nature of blockchains and shared distributed ledgers.

This covers territoriality (jurisdictional and legal concerns) as well as responsibility in the event of a mishap. Shared distributed ledgers (or DLT) have no physical location by definition. Territoriality is an issue in terms of jurisdiction and applicable legislation, because each network node may be subject to various legal requirements, and there is no "central administration" in charge of each distributed ledger, whose nationality might serve as a "anchor" in terms of regulation. Liability is also a problem, as there may be no person ultimately liable for the running of distributed ledgers and the information stored within, based on the same logic.

2. Legal framework for recognition of blockchains as immutable and tamper-proof nodes, ensuring the veracity of information contained therein.

To use blockchains as unique and reliable sources of identification, a legal framework is necessary. Before this to happen, consistent regulations on data protection and the authentication of legal persons' identities are required. While the cryptographic and IT communities agree on the practical immutability of blocks in a well-defined blockchain, either because it is technically impossible to modify blocks in "work test" systems or other types of controls linked to consensus mechanisms, there is currently no legal recognition of this aspect of blockchains, and thus it cannot be used as a security measure.

3. Regulation regarding interpretation of the "right to be forgotten"

The "tamper-proof" feature of blockchains contrasts with the European regulation's right to be forgotten, which protects personal data. The immutability of a blockchain might be an issue, since it could clash with other rights recognised by politicians, governments, and/or regulators. The "right to be forgotten" is a European legislation that gives every European citizen the right to have information held in external databases, whether on paper or in electronic form, destroyed if they so want. Replacement of the right to have information "erased" with a right to "prohibit the use" of personal information by third parties may be the only way to reconcile such rights with the nature of blockchains. This might be accomplished by a mix of automated data encryption when specific criteria are met and other ways to prohibit access to that information when an individual chooses to exercise their right.

4. Legal framework regarding the legal validity of documents stored in blockchains as evidence of possession or existence.

Like the acknowledgment of blockchains as unique, unchanging sources of truthfulness, a second degree of recognition is needed before blockchains may be utilised in specific companies. This applies not only to acknowledgment that the information cannot be changed but also to the acknowledgement that the inclusion

in a blockchain of an act declaring possession or of the existence of an asset is legitimate evidence of ownership or the actual existence of such an asset.

However, if the verification of the property/existence process is sufficiently sound before the document is included in a blockchain, and if we trust that blockchain technology is effective in cryptographic mechanisms, recognition of blockchains as immutable sources of trust implies that documents located in blockchains can be truly applied as evidence of their existence However, it is also an issue whether the courts of a certain nation can accept that. Again, we have no jurisprudence on which to revert.

5. Legal framework regarding the legal validity of financial instruments issued in blockchains.

When blockchains are used to define "native" financial products like bonds or derivatives, regulators and supervisors must acknowledge the legal legitimacy of those financial instruments. Money is, of course, a crucial financial item that might be issued on blockchains. Native money created on blockchains might have significant consequences for monetary policy and macroeconomics, necessitating a more in-depth investigation outside the scope of this report.

6. Legal framework for smart contracts

As far as jurisdictional problems are concerned, there is not just the question of whether the distributed ledger itself has a particular location, but also the issue of signatories to the contract being subject to various laws under their separate countries. Regarding liabilities, many parties are engaged in smart contracts: not only the parties to the contract, but also the author of the same and the custodian of the contract. As well as the obvious potential of one of the contractual parties breaking the contract, there is a danger that the contract itself may be defective, either owing to code flaws or design problems. Thus, when a smart contract fails to function as anticipated, which side would be liable?

7. Regulation on the use of blockchains as a valid regulatory registry for the Internet of Things.

Blockchains have been suggested to be especially helpful for the Internet of Things. All linked gadgets have an identity on the Internet of Things. It is thus necessary to create a common register containing each linked item's "identification" and information, and enabling it to carry out transactions, including M2M (machine-to-machine) payment.

The concept of one or more "shared ledgers" for the Internet of Things appears to have gained momentum and would need a legal framework which would recognise distributed ledgers as legitimate regulatory registers. All of the difficulties mentioned above with respect to territoriality, responsibility and the application of smart agreements are of course equally relevant to any blockchain linked to the Internet of Things' operation.

V. CONCLUSION

Since 2008, the deployment of the blockchain has expanded, spurred mostly by its capacity to enable any kind of digital transaction. Blockchain is now considered to provide reliable service even in unreliable environments. Therefore, there have been attempts to integrate this technology in day to day government functions as well. But there are many challenges in the way of implementation of blockchain technology in the Government and the public sector. Through this paper, the researcher found that the regulatory challenges related to blockchain implementation include lack of legal framework regarding the legal nature of blockchains and shared distributed ledgers, lack of legal framework for recognition of blockchains as immutable and tamper-proof nodes, legal validity of documents stored in blockchains, legal validity of financial instruments issued in blockchains, legal validity of smart contracts, and so on. Further, Blockchain technology may infringe upon some rights like the "right to be forgotten".

But this does to mean that these challenges cannot be tackled, as demonstrated by the many countries which have successfully integrated blockchain technology in their governmental activities. The U.S. Department for Health and Human Services (HHS) has successfully created a contract management tool called 'Accelerate' which uses blockchain, AI, ML, and process automation. Accelerate is intended to better manage the HHS portfolio of approximately $25B worth of 100,000 contracts across 50 systems. The CDC and IBM are working together to find a solution to track the ongoing crisis of opioid disease. The idea of a 'blockchain city' has been implemented at Melaka Straits City in Malaysia. South Korea has announced a grant to build a 4 billion won ($3.5 million) project. Malta has just completed the first national blockchain pilot to administer academic credentials such as diplomas, school certificates and transcripts. In 2019, the Philippine government approved the use of an Ethereum-based system to provide financial services to about 80 rural banks in the Philippines. These case studies are proof of the potential of blockchain technology implementation in the government. Previously criticized technologies have now been successfully implemented by tackling the various challenges in the way. Therefore, Null Hypothesis (H0): Blockchain Technology can be implemented in the Government and the public sector is proved.

REFERENCES

[1] Giudici, G. 2018. Legal Problems of the Blockchain: A Capital Markets Perspective from SSRN Electronic Journal. Published. https://doi.org/10.2139/ssrn.3240273

[2] Clavin, J., Duan, S., Zhang, H., Janeja, V. P., Joshi, K. P., Yesha, Y., Erickson, L. C., and Li, J. D. 2020. Blockchains for Government. Digital Government: Research and Practice, 1(3), 1–21. https://doi.org/10.1145/3427097

[3] Salmon, John; Myers, Gordon. 2019. Blockchain and Associated Legal Issues for Emerging Markets. EMCompass;Note 63. International Finance Corporation, Washington, DC. © International Finance Corporation. https://openknowledge.worldbank.org/handle/10986/31202 License: CC BY-NC-ND 3.0 IGO.

[4] Yaga, D. , Mell, P. , Roby, N. and Scarfone, K. 2018. Blockchain Technology Overview from NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.8202

[5] Tena, M. (2017). 7 regulatory challenges facing blockchain. NEWS BBVA. https://www.bbva.com/en/7-regulatory-challenges-facing-blockchain/

[6] Lubin, J. (2020). Blockchain in Government and the Public Sector from ConsenSys. https://consensys.net/blockchain-use-cases/government-and-the-public-sector/

[7] Deloitte. (2017). Blockchain – speeding up and simplifying cross-border payments from Deloitte Nigeria Blog. https://blog.deloitte.com.ng/blockchain-speeding-up-and-simplifying-cross-border-payments/

[8] Cheng, S., Daub, M., Domeyer, A., & Lundqvist, M. (2020). Using blockchain to improve data management in the public sector. McKinsey & Company. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector#