© 2018 IJSRST | Volume 4 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Security Issues on Block-chain Technology in Financial Sectors

Dr. Atul Rawal
Assistant Professor, Garware Institute, University of Mumbai, Maharashtra, India

ABSTRACT

In this research paper, the researcher focused on Block chain is a distributed database that provides a secure, yet transparent way to make, record and verify any type of transaction. Transaction does not have to be financial; it is simply any type of transfer between two parties that typically would require a third party to authenticate each party and broker the exchange. Block chain eliminates the need for centralised control – instead all transactions are decentralised, and verified by the block chain database itself in the distributed ledger. Block chain can be used to track and verify any kind of digital asset, as well as code or smart contracts. This paper enables to understand the need of block chain for the moment and also its security.

Keywords : Block-chain, Security, Cybercrime, Bit Coin, Digital Currency

I. INTRODUCTION

Block chain owes its name to how it functions and the way in which it stores information, to be specific that the data is bundled into blocks, which connect to shape a chain with different blocks of comparable data. It is this demonstration of connecting blocks into a chain that makes the data put away on a block chain so dependable. When the information is recorded in a block it can't be adjusted without changing each block that came after it, making it difficult to do as such without it being seen by different members on the system.

Block chain is useful for value-based frameworks. Block chain is a technology to make and keep up a cryptographically secure, shared, and appropriated record (a database) for exchanges. Block chain brings trust, responsibility, and straightforwardness to computerised exchanges.

All exchanges that exist on a block chain are shared and appropriated among a system of distributed PCs. Exchanges are encoded before they are put away and shared.

It helps us to dispose of the requirement for unified control and the extra expenses. It is being dependable in the middle of block chain members. Transactions are carefully marked utilising a benefit proprietor open/private key pair. Once recorded, information in a block can't be adjusted retroactively.

II. BACKGROUND OF STUDY

The block chain idea was first presented by Stuart Haber and W. Scott Stornetta in 1991 as "a cryptographically made sure about chain of blocks," which implies a chain or blocks that are connected and cryptographically made sure about. Each block is a blend of three things; a hash pointer to the past block, a timestamp, and exchange information. By plan, block chains are secure and hard to modify. There are three key reasons why block chain is turning out to be standard today:

1) Increased computerised handling power

2) Rapid development in cybercrime

3) Rise of bit coin and digital currency

Block chain, by configuration, requires higher preparing power than typical information figuring. It is all a direct result of excess of information, conveyed capacity, and cryptography. Information encryption and decoding is an expensive issue commonly. Today, PCs have additionally preparing power because of present day processors created by NVIDIA.

Bit coin and digital money are perhaps the most compelling motivation for the expanding ubiquity of block chain. Bit coin is a cryptographic money made by a mysterious individual named Satoshi Takemoto, who utilised block chain technology to make and disseminate secure advanced cash. Bit coin was made to beat the doubt and non-straightforwardness of monetary organisations.

III. RESEARCH ISSUES

Difficulties

Block chain technology on a very basic level has an issue and it's not for everybody. Sparing repetitive information on a huge number of PCs, getting endorsement from them, scrambling is a great deal of work. Block chain isn't for everybody.

Confounded

Information is excess on a large number of circulated PCs and every one of these PCs must concur and approve. All clients on a block chain are open yet unknown, and can be anyplace on the planet. It's not something where you can get a telephone and make a call. Block chain technology isn't straightforward by non-specialised individuals and requires a specialist level of comprehension of technology.

Open and Straightforward

A block chain based framework requires endorsement from every single taking an interest hub. While the block chain procedure is open and straightforward, it could without much of a stretch lead to some contradiction among taking an interest gatherings and postpone the preparing.

Execution and Time

Execution is a significant worry in a block chain exchange. Every exchange is appropriated and shared and requires every single included gathering to approve and endorse the changes. Not exclusively does the procedure lead to an exchange execution yet the hour of consummation is high.

Exchange cost

Dispersing information and cryptographically tasks are time-and asset devouring and lead to higher exchange costs. Block chain exchanges require a unique sort of equipment and have an appeal for power. Typical PCs aren't adequate to partake as block chain hubs.

Cryptography:

Cryptography is utilised to trustfully distinguish all system entertainers, and takes into consideration straightforwardness of communications while keeping up the protection of all system on-screen characters. It is a significant device for overseeing tokens through an application called "wallet." Cryptography is moreover a vital piece of the block chain agreement convention.

Open Key Cryptography

The primary reason for utilising open key cryptography for the block chain is to make a safe advanced reference about the character of a client. Secure advanced references about who will be who, and who claims what, are the reason for P2P exchanges. Open key cryptography permits demonstrating one's character with a lot of cryptographic keys: a private key and an open key. The mix of the two keys makes a computerised

signature. This advanced mark demonstrates responsibility for tokens and permits control of the tokens through a bit of so product called the "wallet." Computerised marks demonstrate responsibility for tokens and permit one to control one's assets. Similarly as we sign a bank exchange or a check by hand, or we use confirmation for Web banking, we utilise open key cryptography to sign Bit coin exchanges or other block chain exchanges.

Openly key cryptography, two gatherings disperse their open keys and permit anybody to encode messages utilising their open keys. The open key is scientifically created from the private key. While it is anything but difficult to process the open key from the private key, the switch is just conceivable with sheer beast power; speculating the key is conceivable however restrictively costly. It is, along these lines, not an issue if an open key is known, yet the private key should consistently be stayed quiet about. This implies, despite the fact that one's open key is known to everyone, it's not possible for anyone to get one's private key from it. A message would now be able to go safely to the proprietor of the private key, and just the proprietor of this private key can unscramble the message utilising the private key related with the open key. This strategy additionally works the different way. Any message marked with a private key can be confirmed with the comparing open key. This strategy is likewise alluded to as an advanced mark.

The significant inquiry in broad daylight key cryptography rotates around the subject of how one can broaden the computational sort between getting the private key from the open key, contrasted with getting the open key from the private key. The private key thus is spoken to by a number, which implies that the bigger the number, the harder it is to figure by somebody who doesn't have the foggiest idea about that number. As PCs become quicker and increasingly effective, we should concoct progressively complex calculations, either by utilising greater numbers or by imagining stronger calculations.

In the event that it takes a few decades to figure an arbitrary number, the number is viewed as secure. Each cryptographic calculation is helpless against a supposed savage power assault, which alludes to speculating your private key by attempting every single imaginable mix until an answer test. To ensure that it is difficult to figure the number, a strong private key has least necessities: It should be an (I) arbitrarily created number. It should be an (II) exceptionally huge number. It needs to utilise an (III) secure calculation for the age of the keys. Irregularity is significant, as we don't need some other individual or machine to utilise a similar key, and people are awful at thinking of haphazardness. Huge key sizes take into consideration further circulation of irregularity, and are a lot harder to split with beast power, yet in addition more slow to register.

Because of their multifaceted nature, secure calculations should be logically demonstrated and stress-tried against security breaks. One ought to abstain from imagining one's own calculation. This issue became clear when the group building up the Particle System chose to actualise their own hash work called Twist. Particle is an option appropriated record answer for block chain that professes to determine Bit coin's adaptability issue with an elective agreement instrument and elective cryptography. Their independent Twist work, notwithstanding, was later seen as "non-impact safe."

Since the rise of Bit coin, cryptographic calculations utilised for the Bit coin block chain have withstood all endeavours of information altering. Without cryptography, there could be no dispersed agreement in a system of on-screen characters who don't have the foggiest idea or trust one another. As PCs get all the more remarkable

and can figure numbers quicker, the calculations utilised should withstand time and quickly advancing mechanical benchmarks to keep up the present degree of security. Numerous analysts and designers contend that supercomputers, specifically, quantum PCs, will before long have the option to split most ordinary encryption calculations through animal power. This isn't totally valid and relies upon the cryptographic calculation. While quantum PCs are not essentially better at breaking hashes, they are substantially more impressive with regard to elliptic bends and prime factorisation. The appropriate responses are mind boggling and not completely settled at this point. This speaks to a strategic research territory.

IV. RBLOCK CHIAN TECHNOLOGY AND DISCUSSION

The Three Pillars of Block chain Technology the three main properties of Block chain Technology which have helped it gain widespread acclaim are as follows:

- Decentralization
- Transparency
- Immutability

Pillar #1: Decentralisation

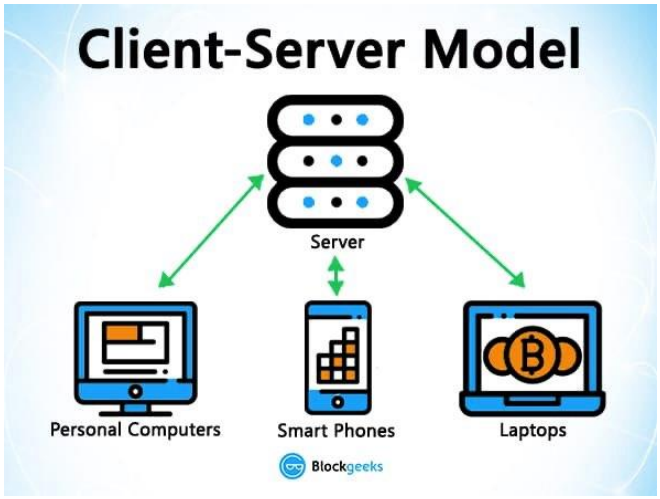

Fig.1.1: Decentralization System

Pillar #2: Transparency

If the person's real identity is secure, you will still see all the transactions that were done by their public address. This level of transparency has never existed before within a financial system. It adds that extra, and much needed, level of accountability which is required by some of these biggest institutions.

V. METHOD

The BT is, besides the financial area, also emerging in many other sectors and gets continuously more popular. It is difficult to overview the market of existing and planned projects since there is no holistic public database or repository for it. Further, the range of visions, concepts, and prototypes is constantly increasing, which means that this review can only provide a snapshot and does not claim to be complete or exhaustive.

We conducted a systematic review of the research topic by first searching for relevant literature. It has turned out that this topic is quite novel, and there are just a few publications about how BT can be used to foster open science or science in general. In a literature review about the usage of BT in different domains (Casino et al., 2018), the application field of science did not even get mentioned as an application domain. Besides literature, we also focused our analysis on various blockchain projects that can foster open science in different ways. We want to provide a transparent and reproducible review, thus in the following, we describe our research questions and methodology.

1. What are the current requirements for a technical open science infrastructure, and how do they compare with BT features?

2. What is the current status and perspectives for the use of BT in science and academia?

3. What are the biggest challenges and obstacles that are preventing successful implementation and

adoption of BT as supporting infrastructure for open scIence?

To answer the second research question, we discussed relevant literature, gray literature, and projects that we found, collected, and screened from different search engines and reference lists until April 2019. Primarily, we used Google Scholar3, PLOS4, CiteSeerX5, Microsoft Academic Search6, and GitHub as file hoster of software development projects. Secondarily, we examined research publications, whitepapers, and blogs. We found the most relevant literature and projects by using the search terms “blockchain” with “science,” “publishing,” “peer review,” and “reproducibility.” The relevance of literature was made sure by reading their abstracts and, partially, the whole work if the abstract was not clear enough to rate the specific content. If a paper had no meaningful content for our research, we excluded it from our review. From there on, we screened the reference lists of the remaining literature to find further suitable sources, known as snowballing.

Besides the literature, we also collected exciting and promising blockchain-based projects consisting of concepts, prototypes, and already deployed applications. We found in numbers many more projects than relevant scientific publications. The majority of the projects got identified in the reviewed literature and the rest through search engines. These projects are either designed specifically for open science, or some of their functionalities are usable in that area. We also found some very early concepts and ideas that only exist in forums or social media networks. However, their potential is not ratable yet due to low progress and information scarcity, so we did not include them into detailed analysis. Altogether, we collected and analyzed 83 projects but removed 23 of them early due to cancelation, irrelevancy, or inactivity (no actions or news for more than 1 year), leaving 60 projects left. We summarized and mapped these into different categories according to their use and created an overview of our approach.

Speaking purely from the point of view of crypto currency, if you know the public address of one of these big companies, you can simply pop it in an explorer and look at all the transactions that they have engaged in. This forces them to be honest, something that they have never had to deal with before.

Pillar #3: Immutability

Immutability, in the context of the block chain, means that once something has been entered into the block chain, it cannot be tampered with.

The reason why the block chain gets this property is that of the cryptographic hash function. In simple terms, hashing means taking an input string of any length and giving out an output of a fixed length. In the context of crypto currencies like bit coin, the transactions are taken as input and run through a hashing algorithm (Bit coin uses SHA-256) which gives an output of a fixed length.

INPUT	HASH
Hi	3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome to blockgeeks. Glad to have you here.	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

Fig. 1.2: Hashing Controlling

As you can see, in the case of SHA-256, no Matter how big or small your input is, the output will always have a fixed 256-bits length. This becomes critical when you are dealing with a huge amount of data and transactions. So basically, instead of remembering the input data which could be huge, you can just remember the hash and keep track.

Matter how big or small your input is, the output will always have a fixed 256-bits length. This becomes critical when you are dealing with a huge amount of data and transactions. So basically, instead of remembering the input data which could

be huge, you can just remember the hash and keep track.

A cryptographic hash function is a special class of hash functions that has various properties making it ideal for cryptography. There are certain properties that a cryptographic hash function needs to have in order to be considered secure. You can read about those in detail in our guide on hashing.

Even if you make a small change in your input, the changes that will be reflected in the hash will be huge. Let's test it out using SHA-256:

INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C

Fig. 1.3: Hashing ControllingThe block chain is a linked list that contains data and a hash pointer that points to its previous block, hence creating the chain. What is a hash pointer? A hash pointer is similar to a pointer, but instead of just containing the address of the previous block it also contains the hash of the data inside the previous block.

The block chain is a linked list that contains data and a hash pointer that points to its previous block, hence creating the chain. What is a hash pointer? A hash pointer is similar to a pointer, but instead of just containing the address of the previous block it also contains the hash of the data inside the previous block.

This one small tweak is what makes block chains so amazingly reliable and trailblazing.

Imagine this for a second, a hacker attacks block 3 and tries to change the data. Because of the properties of hash functions, a slight change in data will change the hash drastically. This means that any slight changes made in block 3, will change the hash which is stored in block 2, now that in turn will change the data and the hash of block 2 which will result in changes in block 1 and so on and so forth. This will completely change the chain, which is impossible. This is exactly how block chains attain immutability.

- *The Blockchain users*

As a web infrastructure, you don't need to know about the block chain for it to be useful in your life. Transactions online are closely connected to the processes of identity verification. It is easy to imagine that wallet apps will transform in the coming years to include other types of identity management.

VI. ISSUES WITH BLOCKCHAIN TECHNOLOGY

Awareness and understanding. The principal challenge associated with blockchain is a lack of awareness of the technology, especially in sectors other than banking, and a widespread lack of understanding of how it works. ...

1. Organisation. ...
2. Culture. ...
3. Cost and efficiency. ...
4. Regulation and governance. ...
5. Security and privacy.

VII. CONCLUSION

Currently, finance offers the strongest use cases for the technology. International remittances, for instance. The World Bank estimates that over $430 billion US in money transfers were sent in 2015. And at the moment there is a high demand for block chain developers. The block chain potentially cuts out the middleman for these types of transactions. Personal computing became accessible to the general public with the invention of the Graphical User Interface (GUI), which took the form of a "desktop". Similarly, the most common GUI devised for the block chain are the so-called "wallet" applications, which people use to buy things with Bit coin, and store it along with other crypto currencies.

VIII. REFERENCES

[1]. https://safenet.gemalto.com/blockchain/
[2]. https://www.c-sharpcorner.com/article/do-you-need-a-blockchain2/
[3]. https://blockchainhub.net/blog/blog/cryptography-blockchain-bitcoin/
[4]. https://safenet.gemalto.com/blockchain/

Cite this Article

Dr. Atul Rawal, "Security Issues on Block-chain Technology in Financial Sectors", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 4 Issue 7, pp. 1004-1010, March-April 2018.

Journal URL : http://ijsrst.com/IJSRST18455155