Cloud Computing Security Using Blockchain Technology

Santosh Kumar Singh, P.K.Manjhi** and R.K.Tiwari****

ABSTRACT

A blockchain is essentially a disbursed database of records, or public ledger of all transactions or digital events which have been completed and shared among participating parties. Each transaction inside the public ledger is established by way of consensus of a majority of the participants within the gadget. As soon as entered, records can in no way be erased. The blockchain carries a sure and verifiable document of every unmarried transaction ever made. Bitcoin, the decentralized peer-to-peer virtual currency, is the most popular instance that uses blockchain era. The virtual foreign money Bitcoin itself is pretty controversial but the underlying blockchain era has worked flawlessly and observed wide range of programs in both economic and non-economic world.

the principle speculation is that the blockchain establishes a system of creating a allotted consensus in the digital online global. This lets in collaborating entities to know for sure that a virtual event took place by means of developing an irrefutable record in a public ledger. It opens the door for growing a democratic open and scalable virtual economic system from a centralized one. There are exquisite opportunities on this disruptive generation, and the revolution on this space has simply all started.

This white paper describes blockchain era and a few compelling specific packages in each financial and non-monetary quarter. Cloud file storage solutions generally face demanding situations in regions inclusive of security, privateness and data manage. The important problem is that one has to accept as true with a 3rd party with one's exclusive documents. Storj gives a blockchain based peer-to-peer disbursed cloud garage platform.

Keywords: *Blockchain; Safety; Cryptography; Verification; Cloud computing.*

1.0 Introduction

A blockchain is essentially a distributed database of information, or public ledger of all transactions or virtual events which have been executed and shared amongst collaborating events. Every transaction in the public ledger is confirmed through consensus of a majority of the members inside the machine. As soon as entered, information can in no way be erased. The blockchain incorporates a positive and verifiable document of every unmarried transaction ever made. to use a fundamental analogy, it's far less difficult to thieve a cookie from a cookie jar, stored in a secluded region, than stealing the cookie from a cookie jar saved in a market region, being located by using thousands of humans.

Bitcoin is the maximum famous instance that is intrinsically tied to blockchain generation. It's also the most controversial one because it helps to allow a multibillion-greenback international market of anonymous transactions without any governmental manage. Therefore it has to deal with some of regulatory issues related to country wide governments and monetary establishments.

**Corresponding author*; *Research Scholar, Department of Computer Applications, Vinoba Bhave University, Hazaribag, Jharkhand, India. (Email: santosh.trinity17@gmail.com)*

*** Assistant Professor, Department of mathematics, Vinoba Bhave University, Hazaribag, Jharkhand, India. (Email: 19pankaj81@gmail.com)*

**** Professor, Department of IT, R.V.S College of Engg & Tech Jamshedpur, Jharkhand, India. (Email: rajeshkrtiwari@yahoo.com)*

However, Blockchain generation itself is non-controversial and has laboured perfectly over the years and is being correctly carried out to each economic and non-financial global programs. Remaining yr., Marc Andreessen, the doyen of Silicon Valley's capitalists, listed the blockchain dispensed consensus model because the maximum crucial invention for the reason that internet itself. Johann Palychata from BNP Paribas wrote inside the Quintessence magazine that Bit coin's blockchain, the software program that allows the virtual forex to feature must be considered as an invention like the steam or combustion engine that has the ability to convert the sector of finance and past [1].

Modern-day virtual financial system is based totally on the reliance on a certain depended on authority. All on line transactions depend upon trusting a person to inform us the reality— it could be an email provider telling us that our electronic mail has been added; it is able to be a certification authority telling us that a positive digital certificates is sincere; or it can be a social network such as Facebook telling us that our posts regarding our lifestyles activities have been shared simplest with our pals or it may be a financial institution telling us that our cash has been added reliably to our expensive ones in a faraway us of a. The reality is that we live our life precariously in the digital world by using relying on a third entity for the safety and privateness of our virtual property. The reality stays that these third celebration resources may be hacked, manipulated or compromised.

This is where the blockchain era comes available. It has the capacity to revolutionize the digital international via permitting a allotted consensus wherein every and every on-line transaction regarding virtual belongings, past and gift, can be confirmed at any time inside the destiny. It does this without compromising the privateness of the digital property and parties worried. The dispensed consensus and anonymity are two crucial traits of blockchain technology.

The benefits of Blockchain technology outweigh the regulatory troubles and technical demanding situations. One key emerging use case of blockchain era includes "smart contracts". Clever contracts are basically pc applications that can automatically execute the phrases of a settlement. Whilst a preconfigured situation in a clever contract amongst collaborating entities is met then the parties worried in a contractual agreement may be robotically made payments as according to the settlement in a transparent manner [2].

Smart belongings is some other associated concept that's concerning controlling the possession of a belongings or asset thru blockchain using clever Contracts. The property can be physical such as vehicle, house or cell phone, or it is able to be non-physical along with stocks of a organization. It should be mentioned right here that even Bitcoin is not clearly a currency: Bitcoin is all about controlling the ownership of money.

Blockchain era is locating packages in huge range of regions; both monetary and non-economic.

Monetary institutions and banks no longer see blockchain technology as a danger to traditional business models. The sector's largest banks are in truth looking for opportunities in this region by doing studies on progressive blockchain applications. In a recent interview Rain Lohmus of Estonia's LHV financial institution advised that they observed Blockchain to be the most examined and comfortable for some banking and finance associated programs.

Non-economic programs opportunities also are infinite. We will envision putting evidence of existence of all criminal documents, health statistics, and loyalty payments inside the track enterprise, notary, non-public securities and marriage licenses within the blockchain. With the aid of storing the fingerprint of the virtual asset rather than storing the virtual asset itself, the anonymity or privateness objective can be accomplished [3].

In this record, we consciousness at the disruption that every industry in these days' virtual economic system is dealing with due to the emergence of blockchain generation. Blockchain technology has capability to emerge as the new engine of increase in virtual financial system wherein

we're increasingly more the use of net to behaviour digital commerce and proportion our non-public facts and lifestyles activities.

There are notable opportunities in this space and the revolution on this space has simply begun. In this file we cognizance on few key programs of Blockchain era within the location of Notary, coverage, personal securities and few other thrilling non-economic packages. We begin via first describing some records and the era itself.

Section I: BlockChain Technology

1. Short History of Bitcoin

In 2008, a man or woman (or group) writing under the name of Satoshi Nakamoto published a paper entitled "Bitcoin: A Peer-To-Peer digital coins gadget". This paper described a peer-to-peer version of the digital coins that might permit on line bills to be sent at once from one party to any other without going through a economic organization. Bitcoin became the primary awareness of this concept. Now "crypto currencies" is the label that is used to describe all networks and mediums of change that uses cryptography to cozy transactions-as in opposition to those structures wherein the transactions are channelled via a centralized relied on entity [2].

The author of the first paper desired to stay nameless and consequently no person is aware of Satoshi Nakamoto to these days. Some months later, an open source application enforcing the brand new protocol became released, beginning with the Genesis block of 50 coins. Everybody can installation this open supply program and end up part of the Bitcoin peer-to-peer community. It has grown in popularity on the grounds that then.

The popularity of the Bitcoin has by no means ceased to increase seeing that then. Furthermore, the underlying Blockchain era is now locating new range of packages past finance.

2. Blockchain Technology: How does it work?

We give an explanation for the idea of the blockchain by way of explaining how Bitcoin works since it's miles intrinsically connected to the Bitcoin. but, the blockchain era is applicable to any virtual asset transaction exchanged online.

1. Validate Entries
2. Shield Entries
3. Hold historical document

Internet trade is completely tied to the economic institutions serving as the trusted 0.33 party who process and mediate any digital transaction. The role of depended on 0.33 celebration is to validate, guard and maintain transactions as proven in discern 1. A certain percentage of fraud is unavoidable in on-line transactions and that desires mediation via monetary transactions. This results in excessive transaction charges.

Bitcoin makes use of cryptographic evidence in preference to the consider-in-the-1/3-celebration mechanism for two willing parties to execute an internet transaction over the net. each transaction is covered thru a virtual signature, is sent to the "public key" of the receiver, and is digitally signed the use of the "non-public key" of the sender. Which will spend money, the proprietor of the cryptocurrency desires to prove his ownership of the "non-public key".

Figure 1: Traditional Online Financial Transactions using third trusted party (Banks, PayPal, etc.)

The entity receiving the virtual currency then verifies the virtual signature, which implies ownership of the corresponding "private key", by using the "public key" of the sender on the respective transaction.

Each transaction is broadcasted to every node within the Bitcoin community and is then recorded in a public ledger after verification. Every singled transaction wishes to be proven for validity earlier than its miles recorded within the public ledger. The verifying node needs to make certain two matters earlier than recording any transaction:

1. Spender owns the crypto currency, via the virtual signature verification on the transaction.

2. Spender has enough crypto currency in his account, via checking each transaction against the spender's account, via checking each transaction against the spender's account, or "publics key" that is registered inside the ledger. This guarantees that there's enough balance in his account earlier than finalizing the transaction.

However, there's question of keeping the order of those transactions which are broadcasted to each other node within the Bitcoin peer-to-peer community. The transactions do no longer are available order wherein they're generated, and subsequently there may be a want for a gadget to make certain that double-spending of the crypto currency does now not arise. Thinking about that the transactions are handed node by node via the Bitcoin network, there's no guarantee that orders wherein they are received at a node are the equal order in which these transactions were generated.

The above manner that there may be a need to expand a mechanism in order that the entire Bitcoin community can agree regarding the order of transactions, which is a frightening mission in an allotted machine [3].

The Bitcoin solved this problem by using a mechanism this is now popularly called Blockchain era. The Bitcoin device orders transactions by way of placing them in companies known as blocks and then linking those blocks through what's called Blockchain as proven in discern 2. The transactions in a single block are taken into consideration to have passed off on the identical time. These blocks are related to each-other (like a chain) in a proper linear, chronological order with each block containing the hash of the preceding block.

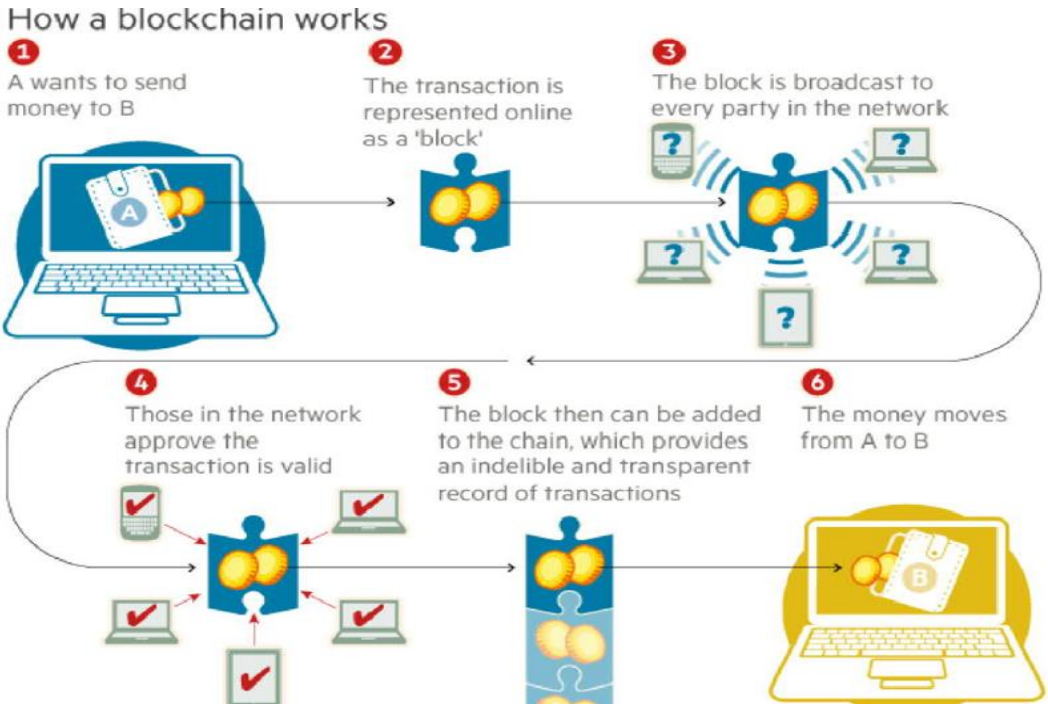

Figure 2: Financial Transactions using the BlockChain Technology [2]

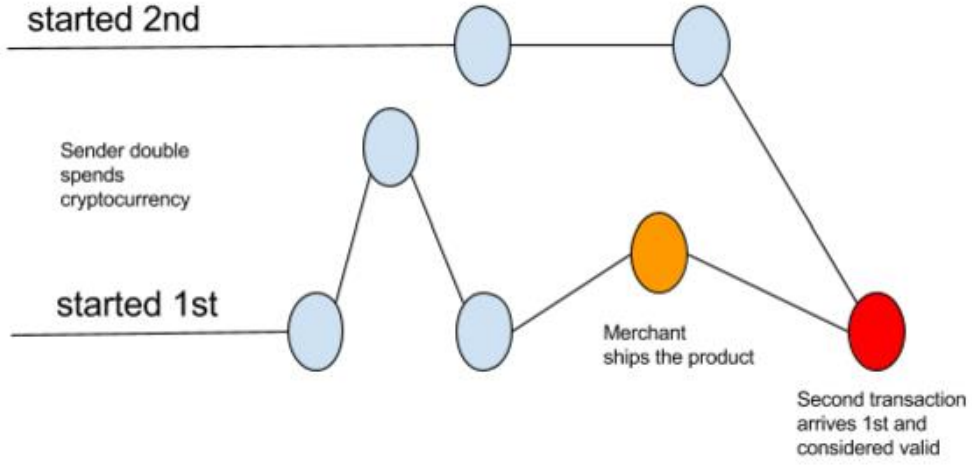

Figure 3: Double spending due to propagation delays in peer-to-peer network.

There still stays one more problem as shown in parent three: Any node within the network can collect unconfirmed transactions and create a block after which broadcast it to the relaxation of the network as a proposal as to which block should be the next one inside the blockchain. How does the community determine which block need to be next inside the blockchain? There may be more than one blocks created by different nodes at the identical time. You'll depend on the order in view that blocks can arrive at one-of-a-kind orders at distinct points inside the community.

Bitcoin solves this hassle with the aid of introducing a mathematical puzzle: each block could be everyday inside the block chain provided it consists of an answer to a very special mathematical hassle as shown in discern four.

This is also referred to as "evidence of labour": a node generating a block wishes to show that it has placed enough computing assets to clear up a mathematical puzzle. As an example, a node may be required to discover a "nonce" which while hashed with both transactions and hashes of previous blocks produces a hash with certain wide variety of leading zeros. The average attempt required is

exponential inside the quantity of 0 bits required but verification process is very simple and may be achieved via executing a single hash [4].

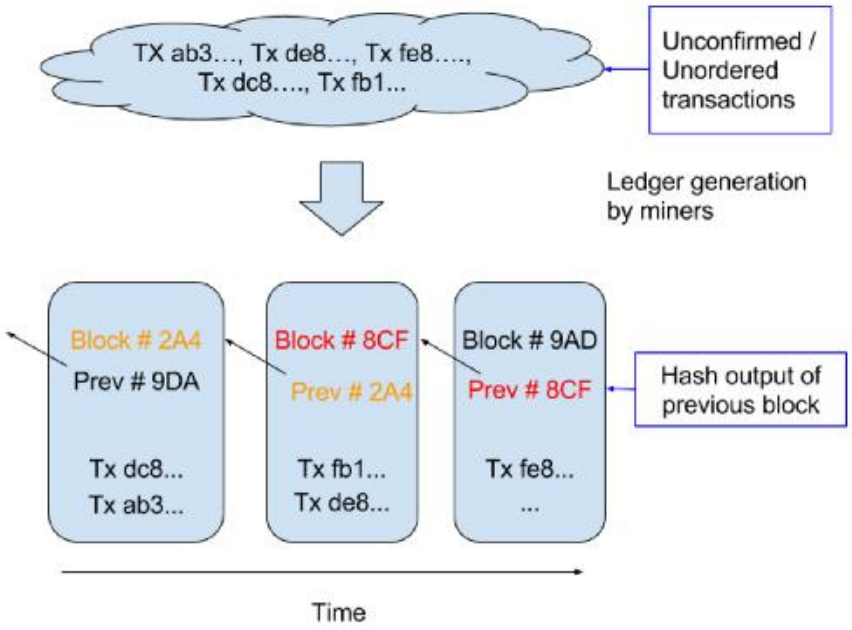

Figure 4: Generation of BlockChain from unordered transactions

This mathematical puzzle isn't trivial to solve and the complexity of the trouble may be adjusted so that on common it takes ten mins for a node in the Bitcoin community to make a proper bet and generate a block. There is very small opportunity that more than one block could be generated within the machine at a given time.

The first node, to clear up the problem, declares the block to the relaxation of the network. Once in a while, however, more than one block can be solved on the identical time, main to numerous viable branches. But, the math needed to be solved is very complex and subsequently the blockchain speedy stabilizes: after this, every node is in settlement approximately the ordering of blocks.

The nodes donating their computing assets to solve the puzzle and generate blocks are referred to as “miner” nodes” and are financially provided for their efforts.

The community most effective accepts the longest blockchain as the legitimate one. consequently, it's miles next to not possible for an attacker to introduce a fraudulent transaction since it has now not best to generate a block by using fixing a mathematical puzzle, however it also has to race mathematically towards the coolest nodes to generate all subsequent blocks in order for it to make the opposite nodes in the network take delivery of its transaction and block because the valid one as shown in figure 5. This task turns into even extra tough due to the fact blocks in the blockchain are linked cryptographically together [5].

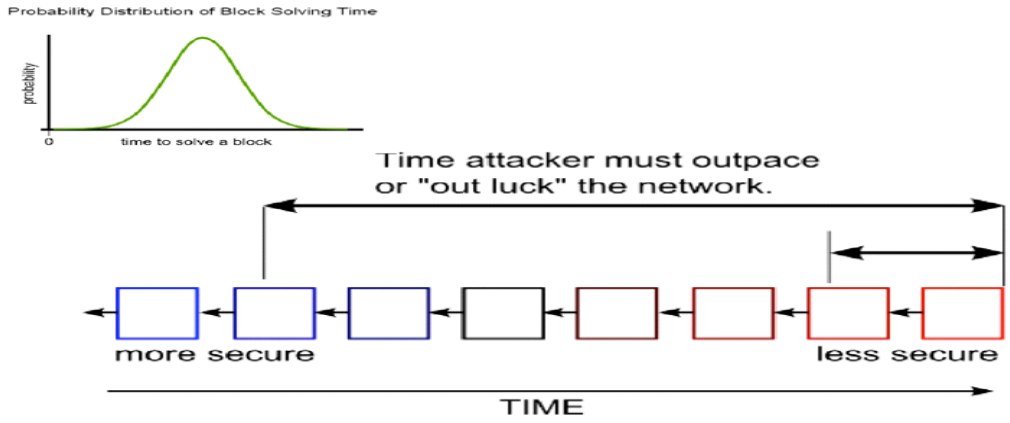

Figure 5: Mathematical race to protect transactions

Section II: Existing Market

Blockchain era is finding applications in each financial and non-monetary regions that traditionally relied on a third trusted on line entity to validate and protect on-line transactions of virtual assets. There has been every other utility "smart Contracts" that was invented in 12 months 1994 via Nick Szabo. It became a brilliant concept to automatically execute contracts among collaborating events. Now the two packages, Blockchain and clever Contracts can work collectively to trigger bills while a pre-programmed situation of a contractual agreement is triggered.

Smart Contracts are contracts that are routinely enforced by means of computer protocols. The usage of blockchain era has made it a great deal less difficult to sign up, verify and execute them. moreover, open source groups like Ethereum and Codius are already enabling clever Con-tracts using blockchain generation and plenty of agencies which operate on Bitcoin and blockchain technologies are beginning to aid smart Contracts.

Particularly, Ethereum has created lot of exhilaration for its programmable platform competencies. The agency allows everybody to create their very own cryptocurrency and use that to execute and pay for clever Contracts, whilst it additionally possesses its personal cryptocurrency (ether) that's used to pay for the offerings. Ethereum is already powering a huge variety of early applications in areas together with Governance, self-sustaining banks, keyless get right of entry to, crowd funding, economic derivatives trading and agreement, all via the usage of smart Contracts.

companies along with IBM, Samsung, Overstock, Amazon, UBS, Citi, eBay, and Verizon Wi-Fi, to name a few, are all exploring alternative and novel makes use of the blockchain for his or her very own packages. 9 of the world's biggest banks which include Barclays and Goldman Sachs5 have recently joined forces with the ny based economic era company R3 in September 2015 in an effort to create a framework for the usage of the blockchain era in the economic marketplace. This is the first time banks have come to paintings together to locate programs of blockchain technology. leading banks like JPMorgan, nation street, UBS, Royal financial institution of Scotland, credit score Suisse, BBVA and Commonwealth financial institution of Australia have joined this initiative [5].

Now we flip to provide a quick description of the kinds of interesting programs and tasks that modern and visionary corporations are doing on this space.

Section III: Applications of Technology in both Financial and Non-Financial Areas

1. Financial Applications:

- Non-public Securities

Its miles very costly to take a agency public. A syndicate of banks should work to underwrite the deal and appeal to buyers. The inventory exchanges list organization stocks for secondary market to characteristic securely with trades settling and clearing in a well-timed manner. it is now theoretically feasible for agencies to immediately difficulty the stocks through the blockchain. These shares can then be purchased and bought in a secondary marketplace that sits on top of the blockchain. Here are some examples:

NASDAQ non-public equity: NASDAQ launched its personal fairness change in 2014 [6]. This is supposed to offer the key functionalities like Cap desk and investor relationship control for the pre-IPO or private companies. The current system of trading shares in this trade is inefficient and gradual because of involvement of a couple of third parties. NASDAQ has joined fingers with a San Francisco based totally begin-up referred to as chain.com [7] to implement personal equity change on top of Blockchain. Chain.com is imposing Blockchain primarily based clever contracts to put into effect trade capability. This product is anticipated to be speedy, traceable and efficient. Medici is being evolved as a securities change that uses the Counterparty implementations of Bitcoin 2.zero. This gets rid of the want for an intermediary, together with a broker, alternate or financial institution. Block movement is an open source project with consciousness on facet chains to keep away from fragmentation safety and different troubles associated with opportunity crypto currencies. Coin setter is a big apple based Bitcoin exchange. it's miles operating on a venture Highline, a technique of the usage of the blockchain to settle and clear economic transactions in T+ 10 mins in preference to the standard Three or T+2 days. Augur is a decentralized prediction marketplace with a purpose to allow customers to buy and promote stocks in anticipation of an occasion with the possibility that a particular outcome happens. This could also be used to make monetary and financial forecasts based totally at the "expertise of crowds". Bit stocks are virtual tokens that live within the blockchain and reference precise assets which include currencies or commodities. The Token holders might also have the precise function of incomes interest on commodities, which includes gold, and oil, as well as bucks, Euros and forex units.

- Coverage

Belongings which may be uniquely identified by one or greater identifiers which are hard to wreck or replicate can be registered in blockchain. This can be used to confirm possession of an asset and additionally hint the transaction records. Any property (physical or digital together with real estate, automobiles, bodily belongings, laptops, different valuables) can probably be registered in blockchain and the possession transaction history may be demonstrated by everyone, in particular insurers. Ever ledger is a business enterprise which creates everlasting ledger of diamond certification and the transaction history of the diamond the use of blockchain. The traits which uniquely discover the diamond inclusive of top, width, weight, depth, coloration and many others. Are hashed and registered within the ledger. The verification of diamonds may be accomplished via coverage agencies, regulation enforcement businesses, owners and claimants.

2. Non-economic applications:

- Notary Public

Verifying authenticity of the record may be achieved using blockchain and removes the need for centralized authority. The file certification provider allows in evidence of possession (who authored it), proof of existence (at a positive time) and proof of Integrity (not tampered) of the documents. Stampery is a corporation which could stamp e-mail or any documents the use of block-chain. It simplifies certifying of emails through simply emailing them to an e-mail mainly created for each consumer. Regulation companies are the use of Stampery technology for a very cost effective manner to certify files. Through coin is one of the corporations which

use clearinghouse protocol for notary carrier. Block Notary is an iOS app which helps you create evidence of lifestyles of any content (photograph, documents, any media) the use of TestNet3 or a Bitcoin community. Crypto Public Notary makes use of Blockchain of Bitcoin to notarize files by using the usage of trivial quantity of Bitcoin to file the report's checksum in a public blockchain. Proof of lifestyles is some other service which uses blockchain to SHA256 digest of the file in Bitcoin blockchain. Ascribe is some other employer which does authorship certification the usage of blockchain. It also offers transfer of possession provider with attribution to the authentic writer.

Applications of Blockchain in the Music Industry

The track industry has long gone a big trade in ultimate decade because of the growth of internet and availability of a number of streaming offerings over the internet. this modification is impacting every person inside the track enterprise: artists, labels, publishers, songwriters and streaming service providers.

- Decentralized proof of life of documents

Validating the lifestyles or the possession of signed files is very crucial in any felony answer. The traditional document validation models rely on primary government for storing and validating the documents, which presents a few obvious safety demanding situations. Those models turn out to be even greater hard because the files become older.

The blockchain era offers an alternative version to proof-of-lifestyles and possession of legal documents. Proof of existence is a easy carrier that permits one to anonymously and securely save online evidence of existence of any document.

The fundamental benefits of safety and privateness that allow a person to give decentralized evidence of the file that couldn't be modified by way of a 3rd party. The life of the file is established the usage of blockchain that does not rely upon a unmarried centralized entity. Evidence of existence net service is available at https://proofofexistence.com/.

- Decentralized storage

Cloud report storage solutions including Drop field, Google power or one force are developing in popularity to save documents, photos, and video and track files. No matter their reputation, cloud report garage answers typically face challenges in areas along with protection, privacy and information manage. The predominant issue is that one has to trust a third party with one's private documents.

Storj presents a blockchain based totally peer-to-peer dispensed cloud storage platform that lets in users to switch and percentage statistics without relying on a 3rd party Statistics Company. This allows human beings to percentage unused internet bandwidth and spare disk area of their personal computing devices to those trying to keep large files in return for Bitcoin based micropayments.

Absence of a important control gets rid of most conventional information screw ups and outages, as well as drastically increasing security, privateness and records manipulate. Storj's platform depends upon a project set of rules to offer incentivization for customers to properly participate on this community. On this way, Storj can periodically test the integrity and availability of a document cryptographically, and offer direct rewards to those keeping the document.

In this situation, Bitcoin-based totally micropayments serve as each an incentive and method of payment even as a separate blockchain is used as a statistics keep for report metadata.

- Decentralized IoT

IBM, in partnership with Samsung, has advanced a platform ADEPT (self-sufficient Decentralized Peer to peer Telemetry) that uses factors of the bit coin's underlying layout to construct a dispensed network of gadgets, or decentralized internet of factors (IOT). ADEPT makes use of 3

protocols within the platform: Bit Torrent (document sharing), Ethereum (smart Contracts) and TeleHash (Peer-To-Peer Messaging). Filament is a start-up that offers a decentralized IoT software stack that uses the Bitcoin blockchain to permit gadgets to hold precise identities on a public ledger.

- Net applications

call coin is an alternative blockchain technology (with small versions) this is used to put into effect a decentralized version of domain name Server (DNS) that is resilient to censorship. Public Key Infrastructure (PKI) era is broadly used for centralized distribution and control of virtual certificate. Each device needs to have root certificate of the Certification Authority (CA) to confirm virtual signature. While PKI has been broadly deployed and highly a success, dependence on a CA makes scalability a problem [10].

Conclusion

Blockchain is Bit coin's backbone technology. The distributed ledger functionality coupled with the security of Blockchain makes it a very appealing technology to solve the modern monetary as well as non-economic industry troubles.

There's sizable interest in Blockchain-based business applications and as a result several begin-united states running on them. Massive financial establishments together with Visa, MasterCard, Banks, and NASDAQ, are making an investment in exploring packages of modern-day commercial enterprise fashions' on Blockchain. In fact, a number of them are trying to find new enterprise fashions inside the global of Blockchain.

Storj presents a blockchain based totally peer-to-peer distributed cloud storage platform that allows users to switch and share statistics without relying on a 3rd party information issuer. Having stated this, we must be seeing extensive adoption in a decade.

References

Borenstein, J. (2015). A Risk-Based View of Why Banks Are Experimenting with Bitcoin and the Blockchain. *Spotlight on Risk Technology. Np*, *18*.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.

Wild, J., Arnold, M., & Stafford, P. (2015). Technology: Banks Seek the Key to Blockchain-FT. com. *Financial Times. Np*, *1*.

Driscoll, S. (2013). How bitcoin works under the hood. *ImponderableThings. Blogger. http://www. imponderablethings. com/2013/07/how-bitcoin-works-under-hood. html*.

Kelly, J. (2015). Nine of world's biggest banks join to form blockchain partnership. *Reuters. Thomson Reuters*, *15*.

Niforos, M., Ramachandran, V., & Rehermann, T. (2017). Block Chain.

Kalinin, K. P., & Berloff, N. G. (2018). Blockchain platform with proof-of-work based on analog Hamiltonian optimisers. *arXiv preprint arXiv:1802.10091*.

Infante, Andre. "Quantum Computers: The End of Cryptography?
http://www.makeuseof.com/tag/quantum-computers-end-cryptography/
Lee, Timothy B. "Bitcoin's Value Is Surging. Here Are 5 Charts on the Growing Bitcoin Economy."
https://www.vox.com/technology/2015/10/31/9651168/bitcoin-growing
[10] Gartner, G. S. (2015). Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor, 2014