Turkish Journal of Computer and Mathematics Education Vol.12 No.10 (2021), 5770-5776

Research Article

A Survey On Securing Internet Of Medical Things Using Blockchain

Mrs.A.Susi[a], Mrs.E.Poonguzhali[b], R. Kowsalya[c], M. Visali[c], V. Priya[c]

[a]Assistant Professor, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry, India
[b]Associate Professor, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry, India
[c] Student, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry, India

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

ABSTRACT: In this project, we provide a solution to protect and secure the patient records and data against various attacks using the technology of blockchain. We use the fully decentralized blockchain. Also, digital signatures are used for model updates. Therefore, we hold that adversaries are not able to fabricate digital signatures or take control of the majority of the network. Furthermore, an adversary cannot poison the data because it is stored off-chain rather on the public ledger. There are only pointers information encrypted with a hash function inside a public ledger.
In problems of large-grid-level centralized transactions and dispatch centers with information asymmetry and high processing costs, the proposal of a completely decentralized transaction architecture and a weak centralized scheduling strategy based on block-chain is done. Firstly, the defined concepts of transaction decentralization and scheduling decentralization are given, and the reliability of distributed transaction communication is studied. Based on the communication credit consensus mechanism, built a blockchain transaction risk control model. Secondly, security checks are performed under the weakly centralized scheduling architecture based on the autonomous chain of substations, and temporary central nodes are set up to perform scheduling tasks. Finally, an optimal solution is obtained by dynamically updating the credibility by using an improved evolutionary algorithm to solve the above model.

1. INTRODUCTION

1.1 BLOCKCHAIN

A blockchain could be a growing list of records, known as blocks that are connected to mistreatment cryptocurrency. Every block contains a cryptologic hash of the previous block, a timestamp, and dealings data (generally delineate as a Merkle tree). By design, a blockchain is immune to modification of the information. To be used as a distributed ledger, a blockchain is usually managed by a peer-to-peer network together adhering to a protocol for inter- node communication and corroborative new blocks. Once recorded, the information in any given block cannot be altered retroactively while no alteration of all later blocks, which needs an accord of the network majority. Though blockchain records aren't unalterable, blockchain could also be thought of as secure advisedly and exemplify a distributed system with high Byzantine fault tolerance. . Blockchain technology was delineated in 1991 by the analysis somebody Stuart Fritz Haber and W.Scott Stornetta. The invention of the blockchain for bitcoin created it the primary digital currency to unravel the double- spending drawback while not the requirement of a trustworthy authority or central server. The bitcoin style has impressed different applications, and blockchain that is clear by the general public is wide utilized by crypto-currencies. Blockchain is taken into account as a kind of payment rail. Non-public blockchain is projected for business use. Sources like pc world known as the promoting of such blockchains while not a correct security model "snake oil".

In 1992, Merkle Trees were incorporated into the look, which makes blockchain additional economical by permitting many documents to be collected into one block. Merkle Trees are wont to produce a 'secured chain of blocks.' It holds on a series of knowledge records, and every knowledge record is connected to the one before it.

Nakamoto improved the look in a very important means employing a hash cash- like methodology to timestamp blocks while not requiring them to be signed by a trustworthy party and to cut back speed with that blocks ar further to the chain. The look was enforced the subsequent year by Nakamoto as a core part of the cryptocurrency bitcoin, wherever it service because of the public ledger for all transactions on the network.

The words block and chain were used individually in Satoshi Nakamoto's original paper, however were eventually popularized as one word, blockchain, by 2016. Sensible contracts that run on a blockchain, as an example, ones that "create[e] invoices that pay themselves once a cargo arrives or share certificates that mechanically send their homeowners dividends if profits reach a particular level". Need associate degree off-chain oracle to access any "external knowledge or events supported time or market conditions that require to act with the blockchain".

According to Accenture, associate degree application of the diffusion of innovations theory suggests that blockchain earned a thirteen.5% adoption rate inside monetary services in 2016, thus reaching the first adopter's section. Trade teams joined to make the worldwide Blockchain Forum in 2016, associate degree initiative of the Chamber of Digital Commerce.

In could 2018, Gartner found that just one of CIOs indicated any reasonable blockchain adoption inside their organizations, and solely 8 May 1945 of CIOs were within the short-run "planning or [looking at] active experimentation with blockchain.

A blockchain could be a decentralized, distributed, and oft public, digital ledger that's wont to record transactions across several computers so any concerned record cannot be altered retroactively, while not the alteration of all later blocks. This permits the participants to verify and audit transactions severally and comparatively inexpensively. A piece of blockchain information is managed autonomously employing a peer-to-peer network and a distributed time-stamping server. They're genuine by mass collaboration hopped up by collective self-interests. Such a style facilitates sturdy workflow wherever participants' uncertainty relating to knowledge security is marginal. The utilization of a blockchain removes the characteristic of infinite reliableness from a digital plus. It confirms that every unit valuable was transferred just once, determining the long-standing drawback of double defrayment. A blockchain has been delineated as a value-exchange protocol. A blockchain has been delineated as a value- exchange protocol. A blockchain will maintain title rights as a result of once properly found out to detail the exchange agreement, it provides a record that compels supply and acceptance.

1.2 BLOCKS

Blocks hold batches of valid transactions that square measure hashed and encoded into a Merkle tree. Every block includes the crypto logic hash of the previous block within the blockchain, linking the 2. The coupled blocks form a sequence. This unvaried method confirms the integrity of the previous block, all the approach back to the initial genesis block. Generally, separate blocks will be made at the same time, making a brief fork. Additionally, to a secure hash- based history, any blockchain contains such an algorithmic rule for evaluation of completely different versionsof the history so that one with a better score will be elite over others. Blocks not elite For inclusion within the chain square measure known as orphan blocks. Peers supporting the info have completely different versions of the history From time to time. They keep solely the highest - scoring version of the information glorious to them. Whenever a peer, receives a higher– score version (usually the previous version with one new block added)they extend or write their info and transmit the development to their peers. There is a associate will guarantees that any explicit entry can stay within the best version of the history forever. Blockchains square measure generally engineered to feature the score of recent blocks onto the previous blocks and square measure have given the incentives to increase with new blocks instead of write previous blocks. Therefore, the chance of associate entry Changing into outdated decreases exponentially as additional blocks square Measure engineered on high of it, eventually changing into terribly low. For Example, bitcoin uses a proof-of-work system, wherever the chain with the foremost additive proof-of-work is taken into account the valid one by the network. There square measure variety of ways Which will be accustomed demonstrate a comfortable level of computation. At intervals, in a blockchain, the computation is administrated redundantly instead of Within the ancient lily-white and parallel manner.

1.3 BLOCK TIME

The block time is that the average time it takes for the network to come up with one further block within the blockchain. Some blockchain produces a brand-new block as oft as every 5 seconds. By the time of block completion, the enclosed knowledge becomes verifiable. In cryptocurrency, this is often much once the dealings take place, thus a shorter block time suggests that quicker transactions. The block time for Ethereum is ready to between fourteen and fifteen seconds, whereas for bitcoin it's ten minutes.

1.4 HARD FORKS

A hard fork could be a rule modification such as the software package confirming in line with the previous rules can see the blocks created in line with the new rules as invalid. Just in case of a tough fork, all nodes meant to figure under the new rules got to upgrade their software package. If one cluster of nodes continues to use the previous software package, a permanent split will occur. As an example, Ethereum has hard-forked to "make whole" the investors within the DOA, which had been hacked by exploiting a vulnerability in its code. During this case, the fork resulted in a split making Ethereum and Ethereum Classic chains. The arduous fork proposal was rejected, and a few of the funds were recovered once negotiations and ransom payment. As an alternative, to forestall a permanent split, a majority of nodes victimization the new software package could come back to the previous rules, as was the case of bitcoin split on twelve March 2013.

1.5 DECENTRALIZATION

By storing information across its peer-to- peer network, the blockchain eliminates a variety of risks associate with information being control centrally. The redistributed blockchain could use ad-hoc message passing

and distributed networking.

Peer-to-peer blockchain networks lack centralized points of vulnerability that pc kookie will exploit; likewise, it's no central purpose of failure. Blockchain security strategies embrace the employment of public-key cryptography. A public key (a long, random-looking string of numbers) is an associate address on the blockchain. Price tokens sent across the network square measure recorded as happiness to its address. A non-public secret's sort of a word that provides its owner access to their digital assets or the means that to otherwise act with the varied capabilities that blockchains currently support. Information keep on the blockchain is mostly thought- about incorrupt. Each node during a redistributed system features a copy of the blockchain. Information quality is maintained by large information replication and procedure trust.

No centralized "official" copy exists and no user is "trusted" over the other. Transactions square measure broadcast to the network exploitation computer code. Messages square measure delivered on a best-effort basis. Mining nodes validate transactions, add them to the block they're building, so broadcast the finished block to different nodes. Blockchains use varied time-stamping schemes, like proof-of- work, to arrange changes. Various agreement strategies embrace proof-of- stake. The growth of a redistributed blockchain is amid the danger of centralization as a result of the pc resources needed to method larger amounts of knowledge become costlier.

1.6 OPENNESS

Open blockchains square measure additional easy than some ancient possession records, which, whereas hospitable to the general public, still need physical access to look at. As a result of all early blockchains were permissionless, the difference has arisen over the blockchain definition. a problem during this current discussion is whether or not a non-public system with verifiers tasked and approved (permissioned) by a central authority ought to be thought about a blockchain.

Proponents of permissioned or non-public chains argue that the term "blockchain" could also be applied to any organization that batches knowledge into time-stamped blocks. These blockchains function as a distributed version of multi-version concurrency management (MVCC) in databases. Even as MVCC prevents 2 transactions from at the same time modifying one object in an exceedingly information, blockchains stop 2 transactions from defraying a similar single output in an exceeding blockchain. Opponents say that permissioned systems correspond to ancient company databases, not supporting localized knowledge verification, which such systems aren't hardened against operator meddling and revision. Nikolai Hampton of Computerworld same that "many in-house blockchain solutions are nothing over cumbersome databases," and "without a transparent security model, proprietary blockchains ought to be blue-eyed with suspicion."

1.7 PERMISSIONLESS

The great advantage to associate open, permissionless, or public, blockchain network is that guarding against unhealthy actors isn't needed and no access management is required. This implies that applications are superimposed to the network while not the approval or trust of others, mistreatment the blockchain as a transport layer.

Bitcoin and alternative crypto-currencies presently secure their blockchain by requiring new entries to incorporate a symbol of labor. Bitcoin uses Hashcash puzzles to prolong the blockchain whereas Hashcash was designed in 1997 by Adam Back, 1st|the initial} plan was first planned by Cynthia Dwork and Moni Naor and Eli Ponyatovski in their 1992 paper "Pricing via process or Combatting Junk Mail". Financial firms haven't prioritized decentralized blockchains.

1.8 PERMISSIONED (PRIVATE) BLOCKCHAIN

Permissioned blockchains use the associate access management layer to manipulate United Nations agency has to access to the network. They are doing not suppose anonymous nodes to validate transactions nor do they get pleasure from the network result. Permissioned blockchains may blow over the name of 'consortium' blockchains.

1.9 DISADVANTAGES OF PRIVATE BLOCKCHAIN

Nikolai jazz musician acknowledged in Computer world that "There is additionally no want for a '51 percent attack on a non- public blockchain because the non-public blockchain already controls 100% of all block creation resources. If you could attack or injury the blockchain creation tools on a non-public company server, you'll effectively management 100% of their network and alter transactions but you needed." This encompasses a

set of significantly profound adverse implications throughout a monetary crisis or debt crisis just like the monetary crisis of 2007–08, wherever politically powerful actors could create choices that favor some teams at the expense of others, and "the bitcoin blockchain is protected by the huge cluster mining effort. at intervals in a non-public blockchain, there's conjointly no 'race'; there isn't any incentive to use additional power or discover blocks quicker than competitors. This suggests that several in- house blockchain solutions are nothing over cumbersome databases.

1.10 BLOCKCHAIN ANALYSIS

The analysis of public blockchains has become more and more vital with the recognition of bitcoin, Ethereum, Litecoin, and alternative cryptocurrencies. A blockchain, if it's public, provides anyone United Nations agency needs access to watch and analyze the chain knowledge, given one has the ability. the method of understanding and accessing the flow of crypto has been a difficulty for several cryptocurrencies, crypto-exchanges, and banks.

The reason for this can be accusations of blockchain-enabled cryptocurrencies facultative illicit dark market trade of medication, weapons, concealment, etc.a standard belief has been that cryptocurrency is personal and untraceable, so leading several actors to use it for ineligible functions. This can be ever- changing and currently, specialized tech companies give blockchain following services, creating crypto exchanges, law enforcement, and banks a lot of awake to what's happening with crypto funds and rescript crypto exchanges.
The development, some argue, has light- emitting diode criminals to rate the use of the latest crypto-like Monero. The question is regarding public accessibility of blockchain knowledge and therefore the personal privacy of the same knowledge. It's a key discussion in cryptocurrency and ultimately in blockchain.

1.11 USES

Blockchain technology can be integrated into multiple areas. The basic use of blockchains is as a distributed ledger for cryptocurrencies, most notably bitcoin. .For Placing blockchain at the core of business structure, businesses are far reluctant.

1.12 SMART CONTRACTS

Blockchain-based sensible contracts are planned contracts that will be partly or dead or enforced while not human interaction. One among the most objectives of a wise contract is machine-driven written agreement. A United Nations agency employee's discussion reportable that sensible contracts supported blockchain technology would possibly scale back ethical hazards and optimize the employment of contracts generally.

However "no viable sensible contract systems have nonetheless emerged." because of the shortage of widespread use, their position is unclear.

1.13 FINANCIAL SERVICES

Major parts of the monetary trade square measure implementing distributed ledgers to be used in banking and per a September 2016 IBM study, this is often occurring quicker than expected. Banks have an interest in this technology as a result of its potential to hurry up back workplace settlement systems. Banks like UBS square measure gap new analysis labs dedicated to blockchain technology to explore however blockchain may be employed in monetary services to extend the potency and scale back prices. Berenberg, a German bank, believes that blockchain is an associate degree "overhyped technology" that has had an oversized range of "proofs of concept", however still has major challenges and really few success stories. The blockchain has additionally given rise to Initial Coin Offerings (ICOs) moreover as a brand new class of digital plus referred to as Security Token Offerings (STOs), additionally generally spoken as Digital Security Offerings (DSOs).

STO/DSOs are also conducted in private or on public, regulated stock market and square measure won't to tokenize ancient assets like company shares moreover as a lot of innovative ones like holding, property, art, or individual merchandise. Variety of firm's square measure active during this space providing services for complaint tokenization, personal STOs and public STOs.

1.14 SUPPLY CHAIN

There are a variety of efforts and business organizations operating to use blockchains in provide chain supplying and provide chain management. The Blockchain in Transport Alliance (BiTA) works to develop open standards for provide chains. Everledger is one of all the inaugural shoppers of IBM's blockchain-based pursuit

service. Walmart and IBM are running a shot to use a blockchain-backed system field-grade officer some efforts and business organizations are operating to use blockchains to provide chain supplying and provide chain management. The Blockchain in Transport Alliance (BiTA) works to develop open standards for provide chains.

Everledger is one of all the inaugural shoppers of IBM's blockchain- based pursuit service. Walmart and IBM are running a shot to use a blockchain- backed system for r provide chain observation — all nodes of the blockchain Are administered by Walmart and are set on the IBM cloud. Hyperledger Grid develops open elements for blockchain provide chain solutions.

1.15 RECENT TRENDS IN HEALTH CARE

Blockchain technology contains the potential to remodel health care, putting the patient in the middle of the health care scheme and increasing the protection privacy and ability of health knowledge. This technology may give a replacement model for health data exchanges (HIE) by creating electronic medical records.

2. RESEARCH DIRECTION

S.NO	TITLE	TOOLS AND TECHNIQUE	ADVANTAGE	DISADVANTAGE
1	A survey on homomorphic encryption schemes:Theory and implementation	RSA algorithm Key Gen Algorithm Encryption algorithm Decryption algorithm	RSA has overcome the weakness of regular of regularrule i.e., believability and confidentiality.	RSA algorithm when larger data is encrypted by the samecomputer becomes very slower.
2	Block chain technology Applications in health care.	Cybersecurity	Managing electronic medical record (EMR). Protection of Healthcare data. Personal Health record data management.	It is evident that the impacts of blockchain on the healthcare system are boundless.
3	Blockchain: Securing aNew Health Interoperability Experience. Accessed	Raft Consensus Algorithm	Raft protocol has the most targeted use case segment, so it is very easy to implement thanother alternatives. Even if a minority of the servers fail to work, the distributed system which follows the Raft consensus protocol will be actively operational.	Maintaining of identical replicated state machines by raft may cause the performance of global application. It requires data from several fragments located at different sites may be slower.

4	BIoMT: Blockchain forthe Internet of Medical Things	Attribute Number Selection (ATS). Security generator (SecGen) Identity issue (ID)	Improved accuracy, Training is reduced and reduces overfitting are the key benefitsof ATS.	When the number of observations is insufficient, there is a increasing overfittingrisks. When the number of variables is large, thereis a significant computation time inATS.
5	A secure system forpervasive social network-based healthcare	CMAC algorithm Hash algorithm Secure Hash Algorithm (SHA) Elliptic Curve Digital Signature Algorithm (ECDSA) Signature algorithm	CMAC algorithm is used for providing the authentication service. In Hash algorithm, Synchronization and also Hashtables is more efficient than search trees.	An issue of CMAC is its computational inefficiency, and security concerns. Practically, Hash collisions are unavoidable while hashing random subset.
6	Healthcare Blockchain System Using SmartContracts for Secure Automated Remote Patient Monitoring	Practical Byzantine Fault Tolerance (pBFT) algorithm. Consensus algorithm Proof-of-work	PBFT is a consensus algorithm where partially members aretrusted. Allowing the blockchain for validating and confirming transactions and operations are done by consensus algorithm.	Only when the number of nodes in distributed network is small,pBFT works in an efficientway. Consensus requires plenty of computingpower.

3. CONCLUSION

The fusion of the IoMT, Cloud Storage with Block Chain technologies not only offers benefits like reduced cost, speed, automation, immutability, near impossible loss of data, permanence, removal of intermediaries, decentralization of consensus, but also overcomes most of the issues especially the security issues of through the use of latest encryptions. The effective deployment Internet of Medical Things (IoMT), demands for more individualized, patient-centric care IoMT that augments affordability (cost effective care, reduced operational costs),simplicity and easy to use, improved life quality, life more comfortable, convenient, healthier and longer lives, provide proactive approach to preserving good health, cater to remote medical support care, continuous monitoring, allow patients to direct health information data to doctors, augments precise disease identifications, management of diseases is real time, decrease in errors, improve and accelerate clinician workflows,improvisation in care for patient, easymanagement of patients records by doctors, keep personal health records, energy efficiency, manage drugs, outcome of patient, user end experience, empowers extreme connectivity due to betterautomation and perceptions in the DNA of IoMT functions.

REFERENCES

1) Acar, H. Aksu, A. S. Uluagac, and M. Conti, (2018) *''A survey on homomorphic encryption schemes: Theory and implementation,'' ACM Comput. Surv., 51(4), Art. no. 79.*

2) S. Angraal, H. M. Krumholz, and W. L. Schulz, (2017) *''Block chain technology: Applications in health care,'' Circulat., Cardiovascular Qual. Outcomes, 10(9), Art. no. e003800.*

3) C. Broderson, B. Kalis, C.Leong,E. Mitchell,E.Pupo,and A. Truscott. (2016). *Blockchain: Securing a New Health Interoperability Experience. Accessed: Sep. 30, 2020. [Online].*

4) M. Seliem and K. Elgazzar, (2019) *''BIoMT: Blockchain for the Internet of medical things,'' in Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom), pp. 1–4.*

5) J. Zhang, N. Xue, and X. Huang, (2016) *''A secure system for pervasive social network-based healthcare,'' IEEE Access, 4, pp. 9239– 9250.*

6) K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, (2018) *''Healthcare blockchain system using smart contracts for secure automated remote patient monitoring,'' J. Med. Syst., 42(7), p. 130.*