Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

Integration of blockchain technology for security and privacy in internet of things

B. Krishna, P. Rajkumar, Venkateshwarlu Velde

Vaagdevi College of Engineering, Warangal, India

ARTICLE INFO

Article history:
Received 31 December 2020
Accepted 19 January 2021
Available online xxxx

Keywords:
Blockchain
Secured blockchain
Secured IoT

ABSTRACT

Now days, the Blockchain Technology is in focus because of its enormous features associated with privacy, security and integrity of the transactions in the network environment. A blockchain refers to a chain of records which are interconnected with each other and highly secured because of the dynamic hash and cryptography implemented at every phase of the transaction. The blockchain technology avoids the possibilities of hacking or cracking the transactions by intentional or accidental attempts. Blockchain can be used for the calculation of sensor data and avoid replication of other malicious data. IoT system implementations can be challenging and a distributed ledge is ideal to identify, authenticate and switch IoT devices seamlessly safely. This paper is presenting the usage patterns of Wireless Body Area Networks with the implementation patterns of Blockchain Technology using advanced scripts of Solidity and embedded programming. The presented integration of implementation is giving the effectual results with the blockchain technology as compared to the traditional approach of security using cryptography.

1. Introduction

Several countries are working to incorporate blockchain technology for their citizens' programmes, including e-governance, e-commerce, business apps, agriculture, education, air traffic control, healthcare, telemedicine, among many others, owing to the anonymity among protection of transactions [1].

Following are the key reasons due to which the blockchain technology is getting huge fame and implementation patterns in the security aware applications [2,3] including, Resilience, Time reduction, Reliability, Unchangeable transactions, Fraud prevention, Security, Transparency, Collaboration, Decentralized and many others.

The process flow is encrypted in the blockchain environment. With the application of advanced protocols, each transaction is authenticated and cannot be crushed due to smart contracts built into the network blockchain [4].

2. Blockchains case studies and implementations

According to Statista estimates, global investment in 2019 went up to nearly $3 billion. In the field of agriculture, Blockchain technology is not limited to e-governance or e-commerce. In the agricultural market, blockchain's valuation in 2018 was more than $40 million [5].

United Arab Emirates (UAE) has been working on the construction of a city built on blockchain that is fully implemented. The first town to be entirely operated by Blockchain technologies is proposed as smart Dubai. The studies show that with the implementation of blockchain for different sectors [5] UAE is saving over US$ 3 billion [6].

With digital wallet incorporation, Krisflyer Singapore Airlines supports blockchain technology. Moreover, this technology is also incorporated into the loyalty scheme and payment [6]. In the fields of education, e-government, food business, healthcare and many more, Singapore is extremely involved in the implementation of blockchain technology [7].

Averspace, the first blockchain platform for the purchase and rent of the land, is popular in the real estate market. With automated smart agreements the contracts are deployed in a secure manner (See Fig. 1).

https://doi.org/10.1016/j.matpr.2021.01.606
2214-7853/© 2021 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the Emerging Trends in Materials Science, Technology and Engineering.

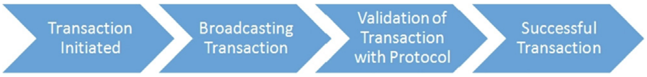

Fig. 1. Process flow with blockchain environment.

2.1. Body area networks (BAN) as key IoT implementation of blockchain

The Body Area networks (BAN), as they provide opportunities for significant changes to the delivery and control of health care, are an active field of research and development. In elderly people or patients with chronic illnesses, this is especially vulnerable but it also monitors athletes' success just to name some applications.

BANs comprise of sensors and actuators all over the human body to detect or transmit impulse or medication to the body or within the body, often know as a pacemaker or a wirelessly transmitted capsule endoscope, with the main points of the illuminated locations – Left Hand (HL), Right Hand (HR), Left Anks (AL), Left Ankle (AL)

A body area (BAN) network is the wireless wearable network of computers [1]. BAN devices may be implanted in the body as implants or placed in a fixed position on the surface of the body or accompanied by device which human beings can wear in various locations. s BAN networking is the body body area network (BSN) or a body sensor network (MBAN). Wireless network for wearable computing devices (See Fig. 2).

WBAN technology began to evolve around 1995 with the aim of using WLAN technology to enforce interactions on the human body, near and around it. Around six year back, the word 'BAN' originated from networks where contact is fully inside, on and around a human body [8,9]. WPAN wireless technology can be utilised by a WBAN device as gateways to expand the reach of a human body. With passage systems, portable devices may be attached to the internet on the human body. Medical practitioners are thus free to use the internet online, regardless of patient venue, to view patient data [10].

A modern generation of wireless sensor networks, now used for traffic control, crops, utilities and healthcare, has been able to evolve rapidly in physiological sensors, embedded low-power circuits, and wireless networking. The network region of the body region is an interdisciplinary sector that facilitates cost-effective and continuous surveillance of health with online real-time alerts (See Fig. 3).

Using a variety of intelligent physiological sensors in a wireless wearable network may be used to rehabilitate the device or to diagnose medical problems easily and quickly. This field depends on the viability to incorporate very lightweight, comfortable biosensors inside the human body that do not impede normal operations. In order to monitor the health state of the patient, the implants in the human body will collect different physiological modifications. The data were wirelessly transferred to an external server centre. All of the details will be sent to physicians around the world simultaneously in real time. When an emergency is identified, the doctors automatically alert the patient by sending related notifications or alerts through the computer system (See Table 1).

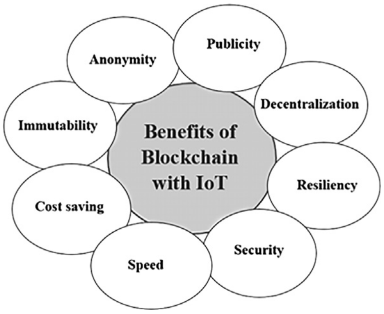

Fig. 2. Blockchain with assorted dimensions.

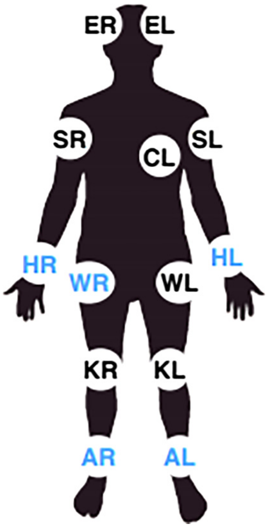

Fig. 3. Body area network.

The knowledge and energy services given and able to power the sensors are currently being limited. The system is still being studied and if implemented at its primitive stage but it is supposed to be an innovation that cuts through healthcare and makes telemedicine and mHealth real [11]. The latter is still in its primitive stage (See Fig. 4).

Recent advancements in integrated circuit technologies have led to devices with capabilities to track, incorporate or even substitute biomedical functions with special ultra-low-power circuitry designs. This biomedical instruments were usually pacemakers. These pacemakers, which take years to work on a single battery, are extremely energy limited since they are inserted under the skin of the human body.

2.2. Implanted body area network (IBAN)

2.2.1. IBANs contain various main parameters that differentiate them from other networks

Less reading of biological signals in a given time, compared with an industrial application, is expected comparatively slowly. Important is energy use. A primary cell in the pacemaker typically functions without battery substitution for 7–10 years. A rechargeable

Table 1
High performance technologies for blockchain programming.

URL	Technology/Platform
https://www.corda.net/	Corda
https://www.hyperledger.org/	Hyperledger
https://www.bigchaindb.com/	BigChainDB
https://github.com/HydraChain/hydrachain	HydraChain
https://www.openchain.org/	OpenChain
https://erisindustries.com/	Eris
http://www.multichain.com/	MultiChain
http://iotatoken.com/	IOTA
https://chain.com/	Chain
https://www.ethereum.org/	Ethereum
https://console.ng.bluemix.net	IBM Bluemix Blockchain

Fig. 4. Body area network in human body.

cell must be charged enough to allow a patient to operate and not to require routine daily recharge. For patient convenience, embedded devices must be lightweight, which contribute to functional problems with components such as antennas. In comparison to a trade WiFi network with a stationary device, when the patient shifts and sleeps, the IBAN will have to operate. The duration of transmission from an implant into a body-wearing controller or less than 3 m for an implant to the top controller of a clinician is comparatively short. It is difficult to communicate to and from the body. The body uses the signal that holds the data to dissipate and consume its energy. With frequency, this effect varies dramatically.

The body's normal conductivity affects the strength of an antenna. A frequency X antenna built and calibrated in the air now operates best with a different frequency Y when it is interaction with the body.

The BAN sector is one field which may allow medical data to be tracked cheaply and continuously over the Internet. A No. of Smart PH Sensor can be combined into a portable WBAN, which is used for the monitoring of medical problems. The feasibility of the very tiny biosensors being inserted within the human body in this region depends. The stationary sensors in the human body collect different physiological patterns to verify the patient's health status.

2.3. Medical applications of IoT, BAN and blockchain

Original BAN implementations are required mainly in the health sector to track and record critical criteria of patients with chronic diseases such as diabetes, asthma and heart attack.

- BANs on the patient will alert the hospital of changes in their vital signs right before they have a heart attack.
- A BAN will auto-inject insulin from a pump into a diabetic patient until their amount of insulin reduces.
- The fundamental changes to wellness and the dynamics of an infection should be used for a BAN [5]

Sports, military or defence are other uses of this technology. Extending technologies to new places can also promote contact between individuals or between people and machines by smooth knowledge exchanges.

2.4. Non-medical applications

Sports – Sensors can be used to measure navigation, timer, distance, pulse rate and body temperature.

Military – Can be used for communication between soldiers and sending information about attacking, retreating or running to their base commander.

Lifestyle and entertainment – Wireless music player and making video calls.

3. Key technologies and frameworks for blockchain implementations

For blockchain programming there are a range of frameworks and technologies available. The main factors in deciding the relevant programming platform include the network type, programming language, consensus protocol, prominence and operation. These considerations must be evaluated in order to create a compliant and high-performance blockchain framework [12].

The following are quotes from the main functions of blockchain programming and smart contracts implemented in leading networks.

3.1. Eris

It is the efficient and multi-functional programming framework [9]. The intelligent contracts can be easily written and carried out on Eris. The private blockchain networks with multiple applications can be configured with greater anonymity and reliability. The software is commonly used to simplify smart contracts by blockchain programmers. In order to evaluate and verify transactions in stable environments, the configured smart agreements are used.

3.2. HydraChain

For the permitted distributed loads, HydraChain is used. HydraChain's main feature is completely Ethereum protocol compliant. HydraChain's core sector covers the private or consortium-based configuration. Furthermore, HydraChain allows native contracts to be configured with improved flexibility for customisation and fast deployment.

3.3. OpenChain

OpenChain refers to an open source and free sharing ledger network. It is used by enterprises and business implementations of high performance scalable applications. Compared to other platforms, execution speed is much higher.Openchain supports multiple signing and validation keys [10]. In Openchain multiple signature keys are available.

The most critical characteristics of OpenChain are

- No fee for mining
- Digital signatures protection
- Various control levels
- Transactions immediately checked
- Unchanged.
- Review of operations
- Management of transparency and validation

3.4. Ethereum

Ethereum is a forum for blockchain programming under open source distribution. Ethereum can be used for all forms of decentralised applications. It is the open source community that has a wide degree of security and flexibility on various platforms. The intelligent contracts can be configured and enforced using Ethereum and is commonly used for public blockchains. Ethereum supports languages such as Go, Python and C++.

3.5. Hyperledger

It is now an open source framework for innovative blockchain software. It is commonly used to work with business apps and private blockchain networks. For Hyperledger, the Python programming language is used. Hyperledger combines a variety of projects with distributed ledgers for blockchian programming. These ventures include BESU, BURROW Hyperledger, Cloth Hyperledger, ING, IROHA Hyperledger, SAWTOOTH Hyperledger. There is a vast collection of resources in Hyperledger, which can track or plan the blockchain network in a wide variety of dimensions, including AVALON, CALIPER, CELLO and EXPLORER.

In the foundation, the device that we want to control and track, IoT uses sensors or embedded chips. Classic devices for IoT deployment based on RFID (Radio Frequency Identification). The topics included in the IoT are various instruments such as cardiovascular implants, biomass transponders for remote monitoring and prescribing patients, livestock, coastal electric clams, vehicles with built-in sensors, or on-site operating systems that support firemen in search and rescue operations. Examples on the market include smart heat systems and washing machines or dryers with remote monitoring wireless internet connectivity.

There are several languages used to programme real life software using blockchain technologies, including Python, JavaScript, Java, PHP, Go, etc.

Blockchain programming is based on cryptographic hash functions needed for blocks and transactions to be encrypted. Furthermore, intelligent contract programming incorporates cryptographic libraries to ensure the complete communication and data processing in blockchain [11].

The following scripts form the basis for network or smartphone device blockchain programming for multiple domains where transfers are to be carried out in protected scenarios.

4. Creating and triggering blocks with WBAN and blockchain technology

Below is the code snippet for the site and smartphone framework in which several transactions or processes are required to join the block in a blockchain environment.

```
const SHA256=require(“crypto-js/sha256″);
class PrivateBlock
{
constructor(BlockIndex, CurrentTime, DataBlock, PreviousHashValue = ”)
{
this.BlockIndex=BlockIndex;
this.PreviousHashValue=PreviousHashValue;
this.CurrentTime=CurrentTime;
this.DataBlock=DataBlock;
this.hash=this.calculateHash();
}
calculateHash()
return SHA256(this.BlockIndex + this.PreviousHashValue + this.CurrentTime + JSON.stringify(this.DataBlock)).toString();
}
}
```

The library of cryptography hash functions is invoked so that the dynamic hash can be generated for the blocks in the blockchain application. crypto-js can be used for the implementation of hash functions. The constructor declared in the class is used to initialize the values and these can be further called in the program. The hash of the block and transaction is processed with JSON to have the retrieved hash in the string.

5. Dynamic blockchain creation

The creation of blockchain is required so that the blocks can be participating in the secured environment and to have the validation of transactions after successful authentication

```
class PrivateBlockchain
{
// GenesisF Block (The First Block of Blockchain)
constructor()
{
this.chain=[this.createGenesisFPrivateBlock()];
}
createGenesisFPrivateBlock()
{
return new PrivateBlock(0, “01/01/2020″, ”GenesisF PrivateBlock“, ”0″);
}
// Inserting Blocks
getLatestPrivateBlock()
{
return this.chain[this.chain.length – 1];
}
addPrivateBlock(newPrivateBlock) {
newPrivateBlock.PreviousHashValue=this.getLatestPrivateBlock().hash;
newPrivateBlock.hash=newPrivateBlock.calculateHash();
this.chain.push(newPrivateBlock);
}
// Validation and Authentication Process
isChainValid()
{
for (let i=1; i < this.chain.length; i++)
{
const currentPrivateBlock=this.chain[i];
const previousPrivateBlock=this.chain[i – 1];
if (currentPrivateBlock.hash !== currentPrivateBlock.calculateHash()) {
return false;
}
if (currentPrivateBlock.PreviousHashValue !== previousPrivateBlock.hash)
{
return false;
}
}
return true;
}
}
```

The genesis block refers to the very first block that is created in any blockchain network. There is no previous hash value of this block as it is the initial block in the blockchain. After this genesis block, all other blocks are generated and inserted after validations using protocols and smart contracts. Once the blocks get activated in the blockchain, the validation of blocks is done for further transactions and transmission of data [12].

A global wireless body area network has been studied extensively, including providers of medical technology, hospitals, insurance companies and industries which cooperate strategically. WBANs have been a common subject for research and are used in various applications. In different future implementations on the Internet of Things (IoT) [13] they provide extensive programming resources and techniques. But WBAN is still at its earliest stage and is faced with the challenges of energy usage, interoperability, device equipment, security, sensor validation, accuracy of data and so on. In 2012 the task force IEEE802.15 ended with IEEE

802.15.6 the world's first WBAN standard. In 1998, the working group IEEE 8002.15 was set up to specialise in the standardisation of WLAN. Its role was to build the Wireless Network (WPAN) standard in short distance, as it is widely referred to. When accepted, technology is a big advance in health care [14].

Although there are wonderful conveniences for the wireless body network, it is still a few hidden risks. The WBAN stores and processes sensitive information on personal health (for example, medical problems, history, signs of life, etc.) posing many questions about privacy and protection [15]. The unauthorised assailants hack the WBAN and snatch user details. These attacks breach the privacy of consumers, for instance, whether an intruder sells insurance provider data to a customer. The attacker modifies the signals in the WBAN to receive bogus user information from the data collector. That can affect users' wellbeing, if the user is a psychiatrist, for instance, and the patient details the doctor gets are misleading and lead to the doctor being treated inappropriately [16].

6. Conclusion

A blockchain is a decentralised digital digital database decentralising, distributed and mostly public documents called blocks which are used to document transactions on several machines and make it difficult to retroactively undo any inferred block without changing any subsequent blocks. This enables participants to freely and reasonably inexpensively check and inspect transactions. The independent use of a peer to peer network and distributed time stamp server is the maintenance of a blockchain database [17]. They're authenticated through mutual self-interest-led partnership. This architecture makes for solid workflows where the confusion among participants over data privacy is negligible. The implementation of a blockchain extracts from a digital commodity the trait of constant reproductivity. It confirms that any value unit has only been moved once to address the long-standing dual spending issue. A blockchain has been defined as a protocol for value-exchange [20]. A blockchain may hold title rights, because it offers a record of the bid and approval when set up to detail the agreement. The Wall Street Journal announced in reaction to the 2020 COVID-19 pandemic that Ernst & Young is working on a blockchain to help businesses, governments, airlines and others monitor people who have undergone anticorpore testing and who may be immune from the virus. A blockchain was also used by hospitals and retailers for required medical supplies. Blockchain technology was used in China to speed up the time taken to pay health-care providers and patients for medical benefits.

CRediT authorship contribution statement

B. Krishna: Conceptualization, Methodology, Software, Data curation, Supervision. **P. Rajkumar:** Writing - review & editing, Software, Validation. **Venkateshwarlu Velde:** Visualization, Investigation, Writing - original draft.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] K. K. Venkatasubramanian and S. K. S. Gupta, "Security Solutions for Pervasive Healthcare," in Security in Distributed, Grid, Mobile, and Pervasive Computing, Y. Xiao, Ed., Auerbach, 2007, pp. 443–64.
[2] O.G. Morchon and H. Baldus, "Efficient Distributed Security for Wireless Medical Sensor Networks," Int'l. Conf. Intelligent Sensors, Sensor Net., Info. Processing, Dec. 2008, pp. 249–54.
[3] Q. Wang et al., "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance," Proc. IEEE INFOCOM '09, Apr. 2009.
[4] R. Di Pietro et al., Catch me (If You Can): data survival in unattended sensor networks, Proc. IEEE PerCom, Mar. (2008) 185–194.
[5] Abadi, J., & Brunnermeier, M. (2018). Blockchain economics (No. w25407). National Bureau of Economic Research.
[6] Ana Alexandre, "UAE Can Save Over $3B by Deploying Blockchain, New Research Reveals", URL: https://cointelegraph.com/news/uae-can-save-over-3b-by-deploying-blockchain-new-research-reveals.
[7] Kiran, Siripuri, U. Vijay Kumar, and T. Mahesh Kumar. "A Review of Machine Learning Algorithms on IoT Applications." In 2020 International Conference on Smart Electronics and Communication (ICOSEC), pp. 330-334. IEEE, 2020.
[8] S. Kiran, S.B. Sriramoju, A study on the applications of IOT, Ind. J. Public Health Res. Dev. 9 (11) (2018) 1173–1175.
[9] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman, Blockchain technology: beyond bitcoin, Appl. Innovat. 2 (6–10) (2016) 71.
[10] S.S. Gupta, Blockchain, John Wiley & Sons Inc, 2017.
[11] M. Nofer, P. Gomber, O. Hinz, D. Schiereck, Blockchain, Bus. Inform. Syst. Eng. 59 (3) (2017) 183–187.
[12] M. Risius, K. Spohrer, A blockchain research framework, Bus. Inform. Syst. Eng. 59 (6) (2017) 385–409.
[13] S. Chessa and P. Maestrini, "Dependable and Secure Data Storage and Retrieval in Mobile, Wireless Networks," Int'l. Conf. Dependable Sys. Net., June 2003, pp. 207–16.
[14] Smart Dubai, URL: https://www.smartdubai.ae/initiatives/blockchain.
[15] Statista Business Data Platform, "Blockchain Statistics & Facts", URL: https://www.statista.com/topics/5122/blockchain/.
[16] The Asean Post, "Blockchain to innovate Southeast Asia's airline industry", URL: https://theaseanpost.com/article/blockchain-innovate-southeast-asias-airline-industry-0.
[17] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. arXiv preprint arXiv:1906.11078.