The Blockchain: A Comparison of Types and the Use in Industrial Sector

¹Mandara Nagendra, ²C N Chinnaswamy, ³Dr. T H Sreenivas

¹M.Tech. student, ²Assistant Professor, ³Professor
^{1,2}Department of Information Science and Engineering
³Department of Computer Science and Engineering
^{1,2}The National Institute of Engineering, Mysore, Karnataka, India
³VVCE, Mysore, Karnataka, India

Abstract: Internet of Things (IoT) is now in its initial stage but very soon, it is going to influence almost every day-to-day item we use. The more it will be included in our lifestyle, more will be the threat of it being misused. There is an urgent need to make IoT devices secure from getting cracked. Very soon IoT is going to expand the area for the cyber-attacks on homes and businesses by transforming objects that were used to be offline into online systems. This paper presents a comparison of types of blockchain and its use in the industrial sector. We first discuss about the basics of blockchain and how the blockchain came into existence. We next talk about the components of blockchain and types along with a comparison. Finally, we see a real time industrial use to understand the technology better.

Keywords: Internet of Things (IoT), cyber-attacks, blockchain.

I. INTRODUCTION

Blockchain technology is now getting too much of attention from software scientists since it has been created. It has mainly two fields that are going to be influenced by it which are:

- By creating a decentralized system, it removes the indulgence of central servers and provides peer-to-peer interaction.
- It can create a fully transparent and open to all database, which could bring transparency to the governance and elections.

Blockchain technology basically has 4 pillars, first, Consensus, which provides the proof of work (PoW) and verifies the action in the networks, second is ledger, which provides the complete details of transaction within networks. Third, Cryptography, it makes sure that all data in ledger and networks gets encrypted and only authorized user can decrypt the information and fourth is smart contract, it is used to verify and validate the participants of the network.

II. LITERATURE SURVEY

A. "Blockchain: A Game Changer for Securing IoT data"

This paper gives an overview of the blockchain technology and its implementation; and the infrastructure of IoT which is based on Blockchain network.

There is an urgent need to make IoT devices secure from getting cracked. Very soon IoT is going to expand the area for the cyber-attacks on homes and businesses by transforming objects that were used to be offline into online systems. Existing security technologies are just not enough to deal with this problem. Blockchain has emerged as the possible solution for creating more secure IoT systems in the time to come.

B. "Blockchain and the Internet of Things in the Industrial Sector"

Blockchain and the Internet of Things (IoT) are key technologies that will have a huge impact in the next 10 years for companies in the industrial market. This article describes how these two technologies will improve efficiencies, provide new business opportunities, address regulatory requirements, and improve transparency and visibility. The IoT allows for real-time capture of data from sensors. As the price of sensors and actuators keeps falling, companies in the industrial sector will be able to overcome cost obstacles in adopting IoT platforms. Blockchain will enable the sharing of key relevant data captured from the IoT using a distributed, decentralized, shared ledger that is available to participants in the business network.

Supply chain use cases are the most common application of blockchain for solving real business problems due to the lack of visibility of shipment data for product or component information as the shipment moves through the supply chain.

C. "Research on Information Security Technology Based on Blockchain"

Information security is the key to the development of modern Internet technology. The distributed mechanism, decentralized mechanism, password mechanism and scripted mechanism of the Blockchain present a completely new perspective for the

development of Internet information security technology. The Blockchain technology redefines the storage and dissemination methods of the information in the network. Neither participant needs to know each other, and nor does it require third-party certification bodies to participate. It records, transmits and stores transferring activities of the information value by distributed technology, ensures that data is not tampered and forged based on an asymmetric cryptographic algorithm, enables all participants reached a consensus on the status of blockchain data information. It explains the concept of blockchain and data security.

D. "The Blockchain: A Comparison of Platforms and Their Uses Beyond Bitcoin"

. This paper presents a comparison of five general-use blockchain platforms. After capturing worldwide attention through its novel combination of ideas, underpinned by decades of research, Bitcoin has become one of the most successful digital currencies to date. Blockchain technology was key to this success, and although conceived to support the ideas and goals of Bitcoin, researchers and esoteric thinkers alike have since realised the potential of blockchain in applications other than Bitcoin. It gives a technical overview of blockchain, explained in the context of Bitcoin.

E. "From Bitcoin to Cybersecurity: A Comparative Study of Blockchain Application and Security Issues"

With the accelerated iteration of technological innovation, blockchain has rapidly become one of the hottest Internet technologies in recent years. As a decentralized and distributed data management solution, blockchain has restored the definition of trust by the embedded cryptography and consensus mechanism, thus providing security, anonymity and data integrity without the need of any third party. But there still exists some technical challenges and limitations in blockchain. This paper has conducted a systematic research on current blockchain application in cybersecurity. In order to solve the security issues, the paper analyses the advantages that blockchain has brought to cybersecurity and summarizes current research and application of blockchain in cybersecurity related areas.

III. BLOCKCHAIN TECHNOLOGY

Blockchain is a kind of decentralized database, which keeps record of every transaction made on a network. Rather than having a traditional central database like that of banks or governments, it has a ledger distributed over a network of nodes. This network can be public, like the internet, which is accessible to any person in the world or it can be private, with accessibility given to only members of an organization. Blockchains decentralized cryptographic model allows users to trust each other and make peer-to-peer transactions, eliminating the need of intermediaries.

Bitcoin's blockchain is essentially a distributed ledger system that records transactions conducted in the Bitcoin network. Each transaction is characterised by one or more transaction inputs (previous transactions from which the user has received Bitcoins) and one or more transaction outputs (users to send the Bitcoins to). Bitcoins are transferred by the current owner signing a transaction which transfers value from the inputs to a new owner(s) as identified by the outputs, which are Bitcoin addresses. The new owner then repeats this process to transfer the coins to the next user.

A. Verification

Once the owner of the coin has broadcasted their transaction into the peer-to-peer network, it must undergo a verification process called "mining" before it can become a part of the public ledger. For efficiency, these transactions are grouped into blocks for verification - hence the name blockchain. Verification is then performed by miners who devote computing power to solving a puzzle. This is the "proof of work" mechanism.

IV. COMPONENTS OF A BLOCKCHAIN

Blockchain mainly has 4 components which form its complete infrastructure. Figure 1 shows the component of blockchain.

• Network of Nodes: All the nodes connected through the internet maintain all of the transactions made on a blockchain network collaboratively. The authenticity of the transaction is checked by the protocol, which eliminates the involvement of a trusted third party for validation purpose.

When a transaction is done, its records are added to the ledger of past transaction, this process is known as 'mining'. The proof of work has to be verified by the other nodes present on the network.

- Distributed database system: The database, which is composed of blocks of information, is copied to every node of the system. Each block contains the following data in itself: A list of transactions; a timestamp; Information, which links it to the previous chain of the blocks.
- Shared ledger: The ledger is updated every time a transaction is made. It is publicly available and is incorruptible which introduces transparency to the system.
- Cryptography: It binds the data with the very strong crypto mechanism, which is not easy to track or tampered by unauthorized users.



Fig 1: Components of Blockchain Technology

V. BENEFITS OF BLOCKCHAIN TECHNOLOGY

The key benefits of using blockchain for IoT would be mainly because of three reasons as shown in Fig 2.

- 1. Build trust building trust between parties and devices will reduce the risk of collision and tampering.
- 2. Reduce costs reducing costs by removing overheads associated with middlemen and intermediaries.
- 3. Accelerate transactions reducing settlement time.



Fig 2: Benefits of Blockchain Technology

VI. TYPES OF BLOCKCHAINS

Private blockchains are valuable for solving efficiency, security and fraud problems within traditional financial institutions, but only incrementally. It's not very likely that private blockchains will revolutionize the financial system. Public blockchains, however, hold the potential to replace most functions of traditional financial institutions with software, fundamentally reshaping the way the financial system works.

A. Public Blockchains

State of the art public Blockchain protocols based on Proof of Work (PoW) consensus algorithms are open source and not permissioned. Anyone can participate, without permission.

- Anyone can download the code and start running a public node on their local device, validating transactions in the network, thus participating in the consensus process the process for determining what blocks get added to the chain and what the current state is.
- Anyone in the world can send transactions through the network and expect to see them included in the blockchain if they are valid.
- Anyone can read transaction on the public block explorer. Transactions are transparent, but anonymous/pseudonumous.

Examples: Bitcoin, Ethereum.

Effects: (1) Potential to disrupt current business models through disintermediation. (2) No infrastructure costs: No need to maintain servers or system admins radically reduces the costs of creating and running decentralized applications (dApps).

B. Federated Blockchains or Consortium Blockchains

Federated Blockchains operate under the leadership of a group. As opposed to public Blockchains, they don't allow any person with access to the Internet to participate in the process of verifying transactions. Federated Blockchains are faster (higher scalability)

and provide more transaction privacy. Consortium blockchains are mostly used in the banking sector. The consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public or restricted to the participants.

Example: R3 (Banks), EWF (Energy).

Effects: (1) reduces transaction costs and data redundancies and replaces legacy systems, simplifying document handling and getting rid of semi manual compliance mechanisms. (2) in that sense it can be seen as equivalent to SAP in the 1990's: reduces costs, but not disruptive!

C. Private Blockchains

Write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent. Example applications include database management, auditing, etc. which are internal to a single company, and so public readability may in many cases not be necessary at all. In other cases, public audit ability is desired. Private blockchains are a way of taking advantage of blockchain technology by setting up groups and participants who can verify transactions internally. This puts you at the risk of security breaches just like in a centralized system, as opposed to public blockchain secured by game theoretic incentive mechanisms. However, private blockchains have their use case, especially when it comes to scalability and state compliance of data privacy rules and other regulatory issues.

Examples: MONAX, Multichain.

Effects: (1) reduces transaction costs and data redundancies and replaces legacy systems, simplifying document handling and getting rid of semi manual compliance mechanisms. (2) in that sense it can be seen as equivalent to SAP in the 1990's: reduces costs, but not disruptive!

Table 1 gives the comparison between public and private blockchains on the basis of access, speed, security, identity and asset.

Table 1	Comparison	of types	of bl	lockchains
---------	------------	----------	-------	------------

	Public	Private	
Access	• Open read/write	Permissioned read and/or write	
Speed	• Slower	• Faster	
Security	 Proof of work Proof of stake Other consensus mechanism	Pre-approved participants	
Identity	AnonymousPseudonymous	Known identities	
Asset	Native Asset	Any Asset	

VII. CASE STUDY

Supply Chain Solutions

Supply chain use cases are the most common application of blockchain for solving real business problems due to the lack of visibility of shipment data for product or component information as the shipment moves through the supply chain. Shipment delays are often due to intermediaries within the supply chain whose role is approval of paperwork associated with the shipments. Paperwork has a tendency to get misplaced or lost or is awaiting processing as the piles of paperwork grow. What if this paperwork could be digitized on the blockchain? The need for these types of intermediaries could be removed from the supply chain.

The blockchain would capture key shipment data emitted from IoT devices attached to products or components as the shipment moves from source to destination. The IoT platform would invoke a transaction for the blockchain that contains the shipment container location and timestamp. The transactions captured in the blockchain would serve as proof of shipment and proof of delivery for container shipments. Shipment delays would be minimized and lead times for materials flowing to manufacturing facilities could be more accurately predicted. Inventory levels at the facilities could be better aligned with just-in-time practices.

In Fig 3, location data is captured by IoT sensors that forward the data to an IoT platform. The IoT platform captures location data in the blockchain. Participants in the supply chain include original equipment manufacturers (OEMs), suppliers, third-party logistics providers, shippers, and warehouses. Each participant has visibility to pertinent shipment data in the blockchain based on the participant's role. Logistics management systems are used by manufacturers to query the blockchain for shipment data and provide additional shipment information to the blockchain.



Fig 3: Blockchain and Internet of Things (IoT) supply chain solution.

VIII. CONCLUSION

Blockchain technology explains a new way of trading based on key technologies such as password security, decentralized coherence, shared public accounts and visibility of its proper controls and permissions. It can completely change the way our society produces and lives by registering and exchanging assets which are physical and virtual, tangible and intangible. Blockchain technology is not just an application technology for new-generation transactions. It creates trust, responsibility and transparency while simplifying business processes.

Blockchain and IoT solutions in the industrial sector will need to address regulatory, legal, and insurance requirements for goods transferred on the supply chain, autonomous vehicles, and manufacturing plant equipment. Safety records and test results will need to be closely monitored by regulators, insurance adjusters, and legal institutions. Regulators will need access to compliance and safety records in the blockchain.

REFERENCES

- Madhusudan Singh, Abhiraj Singh. Shiho Kim: "Blockchain: A Game Changer for Securing IoT data", Internet of Things, 2018.
- [2] Phillip A. Laplante: "Blockchain and the Internet of Things in the Industrial Sector", Internet of Things, 2018.
- [3] Liang Liu, Budong Xu: "Research on Information Security Technology Based on Blockchain", 2018 the 3rd IEEE International Conference on Cloud Computing and Big Data Analysis.
- [4] M. Macdonald, L. Liu-Thorrold, R. Julien: "The Blockchain: A Comparison of Platforms and Their Uses Beyond Bitcoin", 2017.
- [5] Fangfang Dai, Yue Shi, Nan Meng, Liang Wei, Zhiguo Ye: "From Bitcoin to Cybersecurity: A Comparative Study of Blockchain Application and Security Issues", The 2017 4th International Conference on Systems and Informatics.
- [6] Singh, Dhananjay, Gaurav Tripathi, and Antonio J. Jara. "A survey of Internet-of-Things: Future vision, architecture, challenges and services." Internet of Things (WF-IoT), 2014 IEEE World Forum.