Advances in Intelligent Systems Research, volume 147

International Conference on Network, Communication, Computer Engineering (NCCE 2018)

Blockchain-based Technology for Industrial Control System CyperSecurity

Mingyang Mao [a)] and Hong Xiao

School of Computer, Guangdong University of Technology, Guangdong 510006, China

[a)] Corresponding author: 1767087147@qq.com

Abstract. With the development of the blockchain technology, and applications of blockchain technologies more and more widely, we can apply the Blockchains to Industrial Control System(ICS) for network security. The key technology of blockchain include: distributed ledge, asymmetric cryptography, consensus algorithm and smart contract. The goal of our works is to realize industrial control system network security and make that is reliable, safety, high efficiency and low cost. We will explain how to apply blockchain technology to industrial control system network for cybersecurity, and also explain how blockchains works and why blockchains technology can realize the cybersecurity of ICS, then describe how blockchains combine with IoT to realize IoT network security and build blockchain-based ICS cybersecurity architecture modal. We also point out a series of problems that should be considered before the deployment of a blockchains network in ICS and Jot Form data transfer to data storage and data management, blockchains technology can solve these problems well include data transfer insecurity, machine malfunction, data storage insecurity and so on. Our solution is that blockchains network replace Industrial Control systems Field network, our conclusion is that blockchains technology can resolve ICS network security and provide a solution for IoT security, Industrial control network security based on blockchain is very meaningful and feasible.

Key words: ICS; IoT; blockchain technology; transfer insecurity; replace Industrial.

INTRODUCTION

This paper applies blockchains technology to realize industrial control system network security, and make it more reliable, safe, high efficiency and low cost. Industrial Control System (ICS) is an automatic control system consisting of computer equipment and industrial process control components. Industrial control process includes real-time data collection, monitoring, deployment to achieve the automation monitoring. Industrial Control System (ICS) is the key infrastructure of the core control system, is widely used in electric energy, petrochemical, municipal facilities, intelligent manufacturing and other industries. However, industrial control network security incidents in recent years showed a steady growth trend, Industrial control system frequently occur network security incidents has aroused the attention of various countries, experts, researchers and engineers are committed to solving industrial control system network security issues. Block chain is a new type of distributed ledge that can securely store data, information cannot be forged and tampered with, smart contracts—scripts that reside on the blockchain that allow for the automation of multi-step processes. The blockchains technology is a distributed database system which is composed of nodes. Each node is an account, records the transaction data, makes up the data block, and uses the cryptography method to form these blocks as block chain, which is based on timestamp and scattered Column values and proof of work and other technologies to ensure data security. The industrial control system network needs to realize the safe and reliable protection mechanism. The essence of the block chain technology is the data storage, transmission and asymmetric encryption data method of distributed structure, and the data block is used to replace the dependence on the central server. To achieve information and industrial automation infrastructure and the environment safe and reliable structures, to provide the underlying technical support. The blockchains technology of distributed data storage to maintain a reliable database, can adapt to the industrial control system network information security, and the

blockchain with cryptography technology to ensure data cannot be tampered with and cannot be forged, For the industrial control system to provide the whole process of safe and reliable support. The distributed storage and decentralization of the block chain technology meet the security requirements of the industrial control system network. The blockchains technology combined with distributed storage technology is used to construct a P2P network in ICS, by which the industrial device transaction data can be stored in Blockchains safely. Through the complex verification mechanism, the blockchains can maintain the integrity and consistency, and can achieve efficient and reliable transmission and exchange data. The Blockchains technology can make industrial device transaction and data exchange process simple and save cost. The blockchains also can automate execute intelligent contract by storing, verifying and analyzing the industrial device transaction data without losing of data confidentiality. Through the blockchain technology improve ICS efficiency, the future intelligent equipment can establish a credit mechanism in a distributed Internet of things, the use of block chain records to monitor and manage intelligent devices, intelligent contracts can regulate the behavior of intelligent devices, which can solve industrial control System network security issues.

BACKGROUND

Industrial control system (ICS) is a general term that encompasses several types of control systems, including data management systems, distributed control systems (DCS) and other control system such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components that act together to achieve an industrial objective execution.ICS control industrial processes are typically used in electrical, water and wastewater, oil and natural gas, chemical, transportation, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing industries.ICS are critical to the operation of the critical infrastructures that are often highly interconnected and mutually dependent systems. It is important to note that approximately 90 percent of the nation's critical infrastructures are privately owned and operated. Federal agencies also operate many of the industrial processes mentioned above as well as air traffic control.ICS are found in many industries such as electric, water, oil and natural gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing. Because there are many different types of ICS with varying levels of potential risk and impact, so we should pay attention to ICS network security. The blockchains technology is a distributed data ledger that is replicated and shared among the members of a network and run consensus algorithms which can ensure the security of device transaction data in ICS if no large fraction of the computing resource. Blockchains technology is a method for network security of ICS which includes a large amount of data processing, real-time requirements of the higher systems and the need to establish a shorter interval update technology system. We take advantage of the greater throughput of the database technology, faster data Communication technology, more efficient consensus mechanism to make sure the security of ICS.

BLOCKCHAIN WORKS IN ICS

Blockchains is a distributed data ledger comprising a chain of blocks which includes device transaction data and acts as a distributed database or a global ledger which maintains records of all device transactions data on a ICS Blockchain network. These transactions data are time stamped and bundled into blocks where each block is identified by its cryptographic hash, through these device transaction data in blockchains, we can check whether the sender's data and the receiver's is validated and tampered. These data is stored in blocks and these blocks form a linear sequence where each block references the hash of the previous block, forming a chain of blocks called the Blockchain. A Blockchain is applied to a ICS network of device nodes and every devices node executes smart contracts and records the transactions data. The Blockchain is replicated among the device nodes in the ICS network. Any device node in the ICS network can record all transactions data. As a result, the device nodes on the ICS network append validated, mutually agreed upon transactions. The blockchain transaction modal in ICS as showed by Fig 1: Each block in the chain carries a list of a transactions data and a hash to the previous block. The transactions is the one node with another node in ICS network, when Blockchain technology applied to ICS network, the transaction is made by one device node and another machine node in ICS. The exception to this is the first block of the chain, called genesis, which is common to all clients in a blockchain network and has no parent. Blockchain whose records are batched into timestamped blocks, each block is indented by its cryptographic hash. Each block references the hash of the block that came before it. This establishes a link between the blocks, thus creating blockchain. Any device node with access to

this ordered, back-linked list of blocks can read it and gure out what is the world state of the data that is being exchanged on the network, by this way we can find the ICS network error and avoid network attacks.

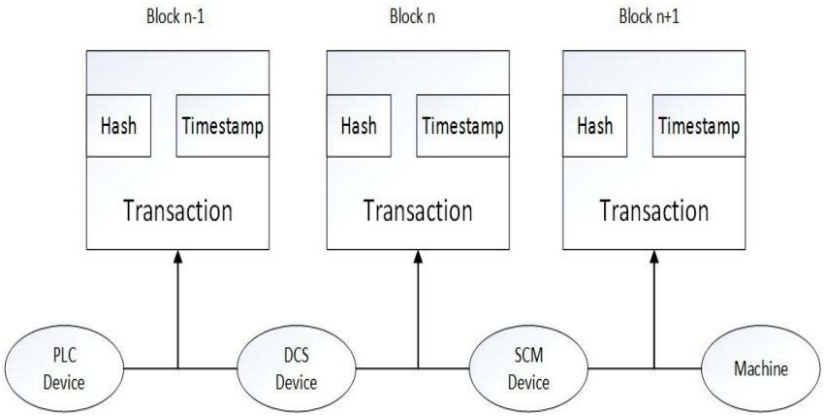

FIGURE 1. Blockchain transaction modal in ICS

The Architecture of Blockchain

A block is a collection of data transmitted by each device node, and the relevant information and records are included, which is the basic unit for forming the block chain. In order to ensure the traceability of the block chain, each block will have a timestamp as a unique tag. The block consists of two parts: Block headers, link to the front blocks, and provide integrity for the block chain; The block body records the updated data information in each terminal. The organization of the block chain as showed by Fig 2:

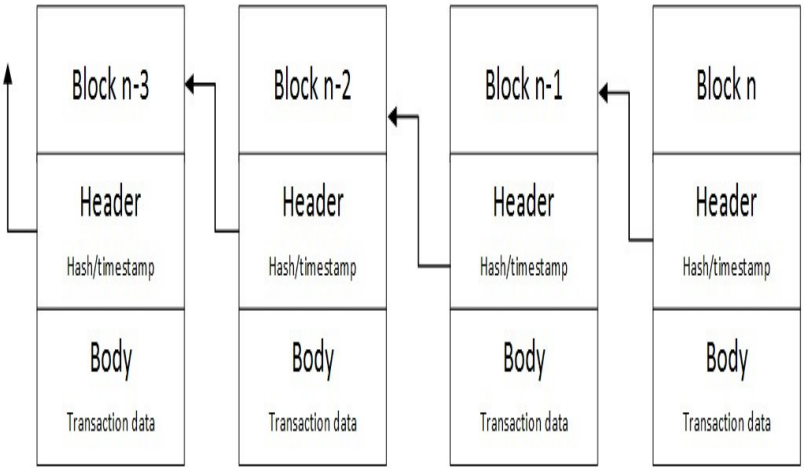

FIGURE 2. The Organization of the Blockchain

Blockchains Security Principle

The purpose of a consensus mechanism algorithm is to allow for the secure updating of a state. according to state transition rules, where the right to perform the state transitions is distributed among the ICS data set. The ICS data set can be users which are given the right to collectively perform transitions through an algorithm. The ICS data set in question should be securely decentralized. This refers to no single actor or a set of actors can take up majority of the set and no one can change entire ICS network software system without the majority of the entire network of users accepting the change. While the majority of the nodes are honest, attackers cannot harm the system, only the attacker who have astronomical computer power can corrupt the blockchains and ICS network system.

Blockchains Security Mechanism in ICS Network

In order to understand of how a blockchain works, and how a blockchain network runs. there is a set of client's nodes that operate on the same blockchain via holds transaction data copy. We assume that a device node in ICS can be regard as blockchains network node, every device node transacts on the blockchains network, so we can take advantage of the trait of blockchains technology: distributed ledger, consensus mechanism, smart contact, asymmetric encryption, all of these features can apply to industrial control system to solve the cybersecurity problem.

EXPERIMENTAL RESULTS

In this ICS blockchain network attack and defense experiment, we build ICS blockchain network modal, let device node transaction mutually and transfer data to each other, and let blockchains to store. Blockchain and decentralized ledger is a foundational and disruptive technology, with the potential to revolutionize industrial control system network security, we have presented the ICS application of blockchain technology. The fundamental blockchain question is ultimately that of trust. In spite of these important reservations, we believe that more blockchain applications will emerge in the near future in areas as diverse as art, tourism and sports. While still in their infancy, one should not underestimate the promising socio-economic benefits of these extraordinary technological changes.

CONCLUSION

The machine devices nodes form a peer-to-peer network where one machine device node interact with another machine device node on blockchain, and communication between nodes via a pair of private or public keys. They use their private key to sign their own transactions, and they are addressable on the network via their public key. The use of asymmetric cryptography brings authentication, integrity, and nonrepudiation into the network. Every signed transaction is broadcasted by a user's node to its neighboring peers. The neighboring peers make sure this transaction is valid before transferring it any further, invalid and false transactions are discarded and refused, eventually this transaction is spread across the entire ICS devices blockchains network. The machine device transactions data that have been collected and validated by the blockchains network using cryptographic algorithms and blockchains node hash value, and blockchains node transaction are ordered by timestamped, which can record machine device usage time and examine block valid transactions, then link the correct previous block on their chain. If there is a new transaction between device, they add the block to their chain, and apply the new transactions it contains to update their ledger, this is a repeating process. A blockchain network essentially is a set of non-trusting node interact with the other no trusted node with shared database, each device node contains entire database transaction information which is called one block and one ledger, all device node in ICS formed blockchains and distributed ledger. In order to prevent attacker from erupting in this distributed environment, and in order to help the network reach consensus, each blockchain network needs to establish certain rules that each device node transaction should follow. These rules are programmed into each blockchain client node, which then uses them to decide whether an incoming transaction is valid, and consequently whether it should be relayed to the network or not. In the implied shared database model, we present here, let us assume that each row of the database is mapped to a public key or address that corresponds to the device node. Valid transaction then is one that attempts to modify a row for which the corresponding signature is present. When each node in the network follows the steps listed above, the shared blockchain it operates becomes an authenticated and timestamped record of the network's activity. The nodes do not have to trust any other entity, giving rise to the term trustless environment, trust is achieved as an emergent property from the interactions of different participants in the system. Things get more interesting when we examine how blockchains can be used for the transfer and tracking of assets.

ACKNOWLEDGMENTS

This work is supported by the national natural science foundation of China under grant (No. 61572144), natural science foundation of Guangdong province under grant (No.2016A030313713).

REFERENCES

1. Bahga A, Madisetti V K. Blockchain Platform for Industrial Internet of Things[J]. Journal of Software Engineering & Applications, 2016, 09(10):533-546.
2. Raymaekers W. Cryptocurrency Bitcoin: Disruption, challenges and opportunities[J]. Journal of Payments Strategy & Systems, 2015:30-46(17).
3. Christidis K, Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things[J]. IEEE Access, 2016, 4:2292-2303.
4. Lou X, Ding J. Biomass Energy Development Present Situation and Application Prospect[J]. Agricultural Science & Engineering in China, 2017.
5. Bonneau J, Miller A, Clark J, et al. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies[J]. 2015, to appear:104-121.
6. Pilkington M. Blockchain Technology: Principles and Applications[J]. Social Science Electronic Publishing, 2015.