Developing a Transparent Tax Data Access Control System Based on Blockchain

Hlwam Maint Htet, Khin Than Mya
University of Computer Studies, Yangon
hlwammainthtet@ucsy.edu.mm, khinthanmya@ucsy.edu.mm

Abstract

Access control systems regulate the access to critical resources and they are vitally important for every organization's IT infrastructure. Access controls authenticate and authorize individuals to access or deny the information they requested. Access control systems in today mostly provide the ability for centralized authorities, whether governments, service providers or manufacturers, or to gain unauthorized access to users data. The potential of blockchain, distributed ledger technology (DLT) plays an important role because it provides a decentralized and peer-to-peer network system to certain a transparent and secured information storage and transmission. Current DLT systems are now facing some QoS requirements and virtualization for distributed ledger technology (vDLT) can fulfill such requirements with the benefits of virtualization technology. This paper proposes a testnet of transparent tax administration system by using organization based access control (OrBAC), and multichain, a private blockchain platform with the help of vDLT.

Keywords- *Transparency; Access Control; OrBAC; Blockchain; DLT; Multichain; vDLT*

1. Introduction

With the wide use of Internet and as the technology is developing in momentum, security is a big challenge in every organization's IT infrastructure. Most of the systems in government organizations are computerized and moving to change e-Government in some administrative field. For controlling access to our critical data, access control systems play an important role. Most of the traditional access control systems are centralized and it can face some problems such as single point of failure and trust. Decentralized access control systems are needed in some environments in which transparency is important. Blockchain technology allows building a transparent and decentralized access control system. The first blockchain was used by the bitcoin cryptocurrency protocol which was first proposed by Satoshi Nakamoto in 2008[1]. Although Bitcoin is one of the most famous applications of Blockchain, it can be used in many different fields and applications with its characteristics such as decentralization, anonymity, auditability, transparency, security, and immutability. Generally, blockchain is defined as a distributed ledger that maintains a continually growing list of publicly accessible records cryptographically secured from tampering and revision [2]. It is believed to create a persistent, immutable, and ever-growing public ledger that can be updated.

This paper proposes a vDLT and blockchain-based access control system to transfer the right access of a resource to authorized users.

The rest of the paper is organized as follows. In section 2, an overview of theories mainly used in this work is provided. Section 3 provides the related work to access control and blockchain. And in section 4, we present the proposed approach and end up this paper with a conclusion in section 5.

2. Background Theory

This section shows an overview of the basic concepts which will be used in this proposed system.

2.1. Blockchain Technology

Originally introduced by Satoshi Nakamoto in 2008 [1] to underpin the bitcoin cryptocurrency network, a distributed database of transactions ever executed within its network. Blockchain is a concept rather than a technology. It is bigger and mature enough. All transactions are recorded into a single ledger and it is like a book with page numbers. If one page is lost, the others are meaningless.

When a node connects to a network for the first time, it will download a full copy of the blockchain database onto its computer or server. If two nodes create two different blocks at the same time, the rule in bitcoin, “called the longest chain rule” is used. The longer chain becomes part of the de-facto blockchain. Figure 1 shows how blockchain works.

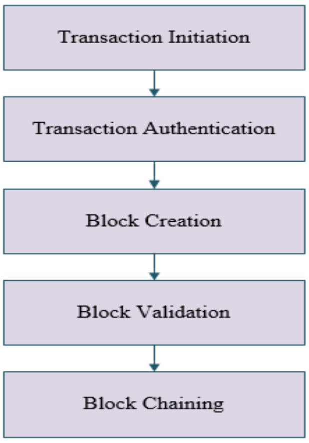

Figure 1. An overview of blockchain processes

Blockchain is the potential use for taxation because of its benefits in data transparency. When the user makes a transaction, it can be traced and it is secured because the digital ledger cannot be altered or tempered once the data has entered. Access to permissioned network is granted to assigned users and real-time information can get because when the data is updated, it will be sent to all participants at the same time [4].

2.1.1 Consensus Algorithms

It will be meaningless if the consensus algorithms are not mentioned in talking about blockchain. Consensus algorithms are the central parts of blockchain. In How to reach consensus among the users to add information to the block is the crucial part of the blockchain. How to reach consensus among the untrustworthy nodes is a transformation of Byzantine Generals (BG) problem, a group of generals who command a portion of Byzantine army circle the city. The attack would fail if some parts of the generals attack the city without knowing all partners. Generals need to communicate simultaneously to reach an agreement whether attack the city or not. Although there might be traitors in the generals, those third parties can send different information to different generals. Therefore, how to reach a consensus is a big challenge in such trustless environment [9]. Proof of Work is a consensus algorithm used in Bitcoin network. It requires a complicated computational process in the authentication. Proof of Stake (PoS) is an alternative of PoW for energy–saving. Practical byzantine fault tolerance (PBFT) is a replication algorithm to tolerate faults and hyper ledger fabric utilizes the PBFT as its consensus algorithm. Delegated proof of stake (DPOS) is different to POS, a direct democratic because it is representative democratic [9].

2.1.2 Multichain

Multichain is an open source platform to create private blockchain within different nodes or between organizations. Although this is mainly designed to handle transactions related to virtual money, it was also used to send the meta data field for each created transactions [8]. It aims to solve a key obstacle to the deployment of blockchain technology in the institutional financial sector, by providing the privacy and control required in an easy to use package. Multichain supports Windows, Linux and Mac servers and provides a simple API and command line interface [3].

2.3 Virtualized Distributed Ledger Technology

Before presenting virtualized distributed ledger technology (vDLT), there has much attention on distributed ledger technology (DLT) and it has been attracted from both academia and industry. DLT can solve a wide range of applications. The first killer application of DLT is cryptocurrency and other services and applications of DLT include supply chain management, identification, healthcare, music, energy, gaming, agriculture, taxation, transportation, publishing, etc. In vDLT, services and applications are classified into different classes according to their QoS requirements such as confirmation latency, cost, security, throughput, security, privacy, etc [5].

Different services and applications built on DLT have widely varying QoS requirements. To address these issues, vDLT- a service-oriented blockchain system with virtualization and decoupled management/control and execution was proposed in [5]. The incoming transactions are classified according to their QoS requirements and queue as in Figure 2.

2.4. Access Control Systems

With the development of technology, every organization uses IT infrastructure and there we face many security threats and losses of our critical data. Without authentication and authorization, there is no data security. Any organization whose employees connect to the Internet needs some level of access control in place. An access control system determines who has access to the environment and what level of access they have. Every IT infrastructure needs a security control with respect to its nature. A security control is a mechanism that is used to protect an asset.

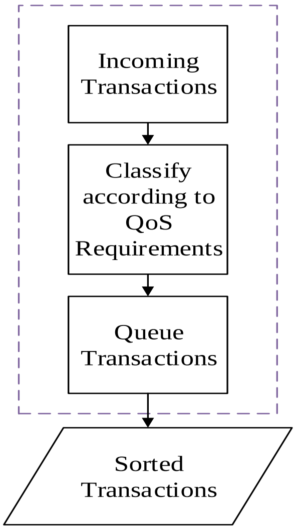

Figure 2. Classification and Queuing transactions in vDLT

Broadly, there are four major types of security controls: (1) Administrative control which is written policy; (2) logical control: technical control such as firewalls, encryption IDs, passwords, etc, ; (3) Physical control as physical facilities and company locations; and (4) operational control which is part of day to day activities such as doing backups.

There are various types of access control models; (i) discretionary access control (DAC) which is a model of who gets access to a resource and a listing of users or groups who are granted access to a resource, (ii) mandatory access control (MAC) where access to resources is controlled and determined by the system administrator through access policies, This approach is centralized and different from discretionary access control (DAC), in which access to an object is determined by the object owner, (iii) role-based access control (RBAC) takes a different approach to controlling access to resources and privileges [11], (iv) attribute-based access control in which accesses are allowed based on the notion of attributes, and (v) organization-based access control (OrBAC) [12] was conceived to handle remaining issues in the extensions of RBAC [13].

3. Related Works

Many access control models have been proposed in the literature to address the security issues in IT infrastructure. In this system, we review some of the related work which leveraged blockchain to enforce access control.

The work of Shorouq Alansari, Fedrica Paci, Vladimiro Sassone in [6] offers a distributed access control system for cloud federations to enforce attribute based access control policies on the data of federated organizations to privacy-preserving fashion. The system uses blockchain to ensure users' identity attributes and access control policies not to alter by malicious users and Intel SGX trusted hardware was used to protect the integrity and confidentiality of the policy enforcement process. A prototype of blockchain-based multi-user system for access control to the datasets which were stored in an untrusted cloud was proposed in [7] using blockchain-based decentralized ledger and ciphertext-policy attribute-based encryption scheme.

4. The Proposed System

The proposed system will be developed using multichain toolkit, a private blockchain platform for immutable log of security events. For identifying roles and policies for making decisions in who can access to what assets of system data, an organization based access control model will be applied. In Figure 3, the system framework of a transparent data access control system is presented. The main difference of this system to other blockchain-based decentralized access control system is that virtualization for distributed ledger technology (vDLT) will be applied. It can solve some issues of QoS requirements in current DLT systems.

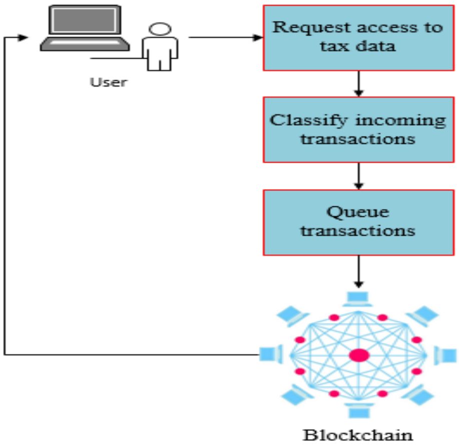

Figure 3. Proposed system framework

When a user creates a transaction to get access to an object, the transaction will be classified based on the nature of the requested transaction's quality of services (QoS) requirements which include confirmation latency, throughput or cost. Then the transaction will be queue in a list before adding to the blockchain. Here, the system will solve some QoS requirements but not all.

Any computers connected to the blockchain networks are called nodes and the simulation of nodes connected in this system will be 5 nodes. These are the tax payer, tax authority, bank, auditor, and government.

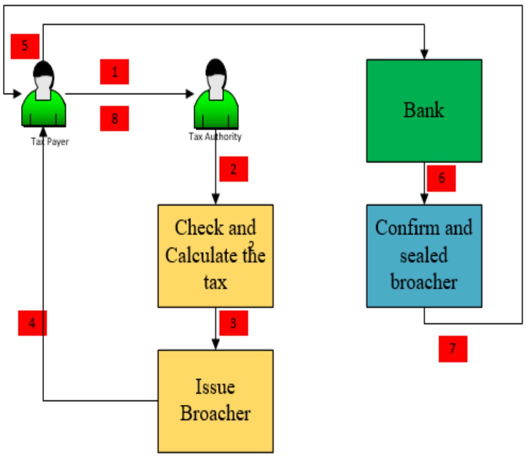

Figure 4. A traditional tax payment process

5. Expected Outcomes

In traditional tax payment process, there are lots of transactions and steps as in Figure 4. Firstly, tax payer need to go to the tax office and meet the tax authority. Tax authority will check the list and calculates the amount of the tax, and then issue broacher to the tax payer. The tax payer goes to the official bank and paid the amount of tax calculated. The bank will make the required transactions and then give a sealed broacher which will identify that the tax has actually been paid. The tax payer needs to return the broacher to the tax authority and the tax administrator need to register and end up the tax process.

In our approach, these steps are reduced. When the user makes a transaction, it will be send to the private blockchain which includes tax payer, tax authority, bank, government authority, and auditor. Because the transaction will be carried out in blockchain, all the participants will get all the information at the same time and no one can alter any transactions. Therefore, it can benefit for reducing financial fraud and the system will enhance security. Moreover, the system will reduce transactions costs and optimize performance with the use of virtualized distributed ledger technology.

6. Conclusions

Tax is the vital role of a nation and there are lots of tax evasion and financial fraud in every sector. The development of a nation depends on how its citizens pay tax correctly. Here, transparency is needed to reduce financial fraud and other illegal affairs. Therefore, researchers and IT technicians should try how to support the tax system with the help of technology. In this paper, we proposed a transparent access control framework based on blockchain and virtualized distributed ledger technology. Here, e-Taxation system is built as a testnet. As the technology is developing in momentum and blockchain technology is growing bigger, no one can deny. Although privacy is a big challenge in public blockchain, the system uses permissioned blockchain where privacy problems can be reduced. This approach will benefit the way traditional tax payment process reducing the administrative burden, saving time and money for the cost of accounting services. Because all of the transactions are real time and transparent, the risks of financial fraud and corruption will be reduced.

Future work will include to implement the tax system in practical use with more nodes and to become a more robust and efficient system satisfying some of the QoS requirements.

Limitations

This system will solve only some QoS requirements and not all of the QoS issues. There may be some political and legal issues in using blockchain technology for practical uses in government organizations according to the nations' rules and regulations.

References

[1] Nakamoto, S.: "Bitcoin: A peer-to-peer electronic cash system", 2008.

[2] HengHou. "The application of Blockchain Technology in E-Government in China", 2017 26th International Conference on Computer Communications and Networks (ICCCN), 2017

[3] Multichain White Paper

[4] Mark Schofield,Global and UK Leader, tax reporting and strategy, PWC, "How blockchain technology could improve the tax system”, 2017 February.

[5] F. Richard Yu, “vDLT: A Service-Oriented Blockchain System with Virtualization and Decoupled Management/Conrtrol and Execution”, IEEE, 2018 September 2.

[6] Shorouq Alansaari, Federica Paci, Vladimiro Sassone, “A Distributed Access Control System for Cloud Federations”, IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017

[7] IlyaSukhodolskiy, Sergey Zapechnikov, “A Blockchain-Based Access Control System for Cloud Storage”, IEEE 2018

[8] Mayssa JEMEL, Ahmed SERHROUCHNI, “Decentralized access Control mechanism with temporal dimension based on blockchain”, The Fourteeth IEEE International Conference on e-Business Engineering, 2017.

[9] Zibin Zheng, Shaoan Xie, Hng-Ning Dai, Xiangping Chen, Huaimin Wang, “Blockchain Challenges and Opportunities: A Survey”, International Journal of Web and Grid Services, December 2017.

[10] Marc Andreessen, “Blockchain technology and its potential in taxes”, Deloitte, December, 2017.

[11] Glen E. Clarke, “CompTIA Security + Certification Study Guide”, McGraw-Hill, 2012.

[12] A. A, E. Kalam et al., “Organization Based Access Control”, in Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks, 2003, pp.120-131.

[13] Aissam OUTCHAKOUCHT, Hamza ES-SAMAALI, Jean Philippe LEROY, “Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things”, International Journal of Advanced Computer Science and Applications, 2017.