Supply Chain Management, Certificate Management at the Transportation Layer Security in Charge of Security

Tsara Ayuninggati[1], Eka Purnama Harahap[2], Mulyati[3], Raihan[4]
University of Raharja, Indonesia[1,2,3,4]

Jl. Jenderal Sudirman No.40 Cikokol, Kec.Tangerang, Kota Tangerang[1,2,3,4]
e-mail: tsara@raharja.info[1], ekapurnamaharahap@raharja.info[2], mulyati@raharja.info[3], raihan.raihan@raharja.info[4]

Author Notification
22 January 2021
Final Revised
22 June 2021
Published
07 July 2021

Ayuninggati, T. ., Purnamaharahap, E. ., Mulyati, & junior, raihan. (2021). Supply Chain Management, Certificate Management At The Transportation Layer Security In Charge Of Security. *Blockchain Frontier Technology*, *1*(01), 1–12. Retrieved from

https://journal.pandawan.id/b-front/article/view/3

Abstract

In the public key infrastructure, the certification authority is fully trusted, and the security of the public key infrastructure depends on the trust of the certification authority; however, recent attacks and corruption on the certification authority indicate that the certificate is forged when the certification authority fails . New solutions, blockchain-based public key infrastructure products and registry can repair vulnerabilities in public key infrastructure, especially weaker security systems. Proposals for infrastructure-based public key infrastructure. Public keys are still the target of global attacks. According to the registration of the target victim, it is signed as a temporary public key infrastructure based on the blockchain. High growth rates require permission to use the wallet. To solve this problem, this document introduces an integrated and responsible system for managing security certificates at the transport layer that represents the next generation of public key infrastructure.I merged two new architectures, introduced a new process, and created a registration and CA server. The domain owner has been notified. In supply chain management, the domain certificate signed by the CA is stored on the registration server, and the certificate server and the CA registration server are forwarded to the group that owns the domain. Compared with existing supply chain public key infrastructure products. The above-mentioned blockchain-based public key infrastructure scheme and registry are used for security and governance analysis.

Keywords: *Transparency, blockchain, public key infrastructure, supply chain management.*

1. Introduction

Millions of online users rely on the security of the transport layer to protect their financial and non-financial transactions from medium-sized attackers. The security of the transport layer depends to a large extent on the public key infrastructure. It is a central unit with similar functions. Browser. The X.509 certificate signed by the CA is used for communication on the transport layer to verify the proxy and prevent attacks. Since the security of millions of online transactions depends on the security of the public transport layer of critical infrastructure, the security of the transport layer can be expected: the security of critical public infrastructure will coincide with its adoption and popularization [1].

Unfortunately, examples of common public key infrastructure are very fragile. In this example, the security of the public key infrastructure depends on the trust and security of the certification authority, but the certificate under test cannot protect the client from tampering with the certification authority itself. The main drawback comes from the following message:

Browsers/operating systems store hundreds of certificates of certificate authorities that they believe can authenticate [2]. Currently, the security of public key infrastructure clients relies on a single certification authority key, which can be easily stolen or lost. If the certificate authority is corrupted, it can issue transport layer security certificates for other fail-safe certificate authority domains, thereby highlighting the idea of a single point of failure and weaker channel security. 4 Attackers can use invalid but valid certificates issued by sinners to websites to spoof a client's connection with the website.

Since certificate authorities are commercial organizations and sell transport layer security certificates to domain/web server operators, they must have appropriate security procedures in place to protect your private keys. Recent certificate authority errors have helped uncover the processes used to manage weak keys and issue certificates [3]. The certificate authority ecosystem has issued a certificate. All over the world, Comodo confirmed that a third-party registry vulnerability had been hacked. Hackers use fake certificates to access well-known domain names like Google and Yahoo. Another attack was announced in August 2011. This time DigiNotar was also hacked. He received nearly 500 fake certificates. Even for the certificate authority Symantec which has about a quarter of the transport layer security certificates on the market, Google has issued fake certificates for distribution based on testing.

This data shows that certificate authority corruption can lead to a real virtual global attack. In addition to certificate authority vulnerabilities, transport layer security other drawbacks. For example, an attacker can use a self-signed certificate to launch a phishing-protected attack. If the target victim ignores the security warning, then the attacker will succeed, and security warnings are common practice in this field. In Syria, the government launched such aggression against Facebook [4].

2. Job Relationship

Customer centered approach. In a certificate- centric authority scheme. Certificate authorities issue CRLs to prevent clients from connecting to domain servers whose certificates have been revoked. Unfortunately, customers should be able to get the latest CRLs online. Otherwise, even if the certificate is revoked, the permanent vent will remain open. Due to its size, the CLR is also expensive in terms of connectivity. To reduce the burden on clients and network resources, clients with OCSP can use the OCSP online request server to verify and verify the public key of the domain server in real time. Buchmann and Bayer suggest using OCSP to investigate the revocation status of travel documents that machine certificate authorities can carry in public key infrastructure. However, OCSP has privacy, security and performance issues. Another option is a short-term certificate, which allows data exchange without having to check the revocation status online.

Recommendations based on coverage limits reduce the reputation of the certificate authority by limiting the number of domain servers that the certification authority can guarantee. In PIN-based schemes, such as Langley and Marlinspike, the domain declares a valid public key so that the browser can display the key [5]. Unfortunately, this technology cannot protect the customer during the visit. First in the domain. DANE is a proposed DNS Security Extension, which domains can use to verify security settings and certificates in DNSSEC records. In addition, CAA makes the domain a trusted certification authority for issuing certificates. It uses a blockchain based system for domain server authentication.

The registry-based method allows the public to verify certificates verified by a certification authority by forcing the domain owner to issue his certificate in a public CB. For example, Eckersley introduced a new public key scheme called Sovereign Key, which provides more robust transport layer security certificate authentication than the certification authority model. In SK, the domain generates SK pairs to sign the certificate and register the public key.

CT is a project initiated by Google, which extends the existing transport layer security ecosystem by making certificate management transparent and identifying invalid certificate authorities [5]. At CT, all certificates are written in the form of a Merkle tree into a special register of attachments maintained by the CB. In chronological order. The domain can receive confirmation of the existence of a certificate certificate in the CI registry. During a transport layer security connection, this registration confirmation information will be provided to the client along with a transport layer security certificate. Unfortunately, when the adversary controls the CA, CT can't prevent its customers from getting fake certificates.

Policert extends AKI so that domains can define detailed SCP policies ("subject certificates") and clearly define a list of trusted certificate authorities, server logs, connection attributes, and overall security in SCP. Multiple certificates are signed by different certification authorities and linked to SCP via signature. During the transport layer security handshake , a special SCP key and a multi-signature certificate called MSC are registered in the server logs and presented to the client along with a PoP (Proof of Status). However, there is no defined method for the spread and disclosure of drug-related crimes. ATCM detects and prevents attacks against Policy by introducing checks and balances and increasing certificate revocation. ATCM is highly secure and can protect clients from powerful attackers who control trusted entities. Security features of Tamarin Prover. However, because all entities participate in each process, ARPKI , TriPK , and ATCM introduce additional delays [6].

A blockchain solution is a decentralized framework for managing public keys. Bitcoin is one of the public key infrastructures for decentralized authentication and key management. It is based on Namecoin being mixed into Bitcoin to ensure identity preservation. However, Knecht, Loibl and Naab do not have IDs. Second, each identity user can only use one public key. With PB- Certcoin -based public key infrastructure , customers can communicate with each other without revealing their real identities. Unfortunately, the proposed scheme is not suitable for transparent certificate lifecycle and domain server identity management [7].

3. Planning

3.1 Multi Signature Scheme

In supply chain management, we need a signature algorithm that allows multiple keys to authorize operators. Schnorr's signature algorithm can be extended so that multiple independent signers can create accurate and concise signatures [8]. CoSi is one of the protocols leaders can use to call this statement, which has been publicly verified and confirmed by all witness groups [9]. Each logging process creates a collective signature that is comparable to a single signature in terms of size and verification costs. The company concludes that the administration and the signatories have reviewed the statement and agree to endorse it [10].

3.2 Smart Contracts From Blockchain

Blockchain provides a distributed ledger that can only be publicly recorded and maintained as an attachment. The entries in the public ledger called transactions are organized into new blocks, each block containing multiple transactions. Usually, new transaction records are added randomly to the global ledger, which is called mining. Each transaction requires payment in the form of a transaction fee [11] [12]. A smart contract is an executable code that is used to store contracts and execute the rules specified in the contract without the involvement of a third party. Smart contracts can manipulate states and charges stored on the blockchain. Learn more about blockchain [13].

4. System Problem Model And Definition

4.1 Definition of problem

The main problem that we want to accomplish is to develop a management infrastructure security certificates layer transport new hybrid that will prevent spoofing attacks, reduce the amount of trust that is hosted on the infrastructure component of any (such as a certificate authority and log server), and makes the control center reliable transparent, but the attack surface on the system is reduced, and there is a single point of failure [13].

4.2 System Modeling

You want to establish a secure connection with a supply chain management domain server. Using the services provided by the supply chain management domain, this can be a complete site or an efficient site. Since the supply chain management registry memory is very small (less than 100MB per year), anyone using or providing the service can act as a full node (if using a dedicated blockchain platform) [14].

The supply chain management blockchain platform requires a blockchain platform that customers can use to check final authorization status and maintain smart contracts. CMMs can run on custom blockchains or on existing blockchain platforms (such as Bitcoin24** and Ethereum.25). According to the decision of Wüst and Gervais 70, when is a public review necessary? Yes, it is recommended to use blockchain platforms without permission (such as Bitcoin and Ethereum) or without public permission (such as Sovrin.io). In supply chain management, anyone can review each claim to ensure transparency and accountability. Therefore, supply chain management can be used through the blockchain platform without public approval or approval [15].

4.3 Competitor Model

We are looking for a strong adversary whose main goal is to use HTTPS to impersonate the victim's domain. To this end, the adversary can control certificate authority and server logs for counterfeit attacks by creating multiple versions of the server log database (Single World Attack) for the target victim. Signature) We assume that the electorate is not controlled by the enemy [15].

4.4 Threat Impersonation

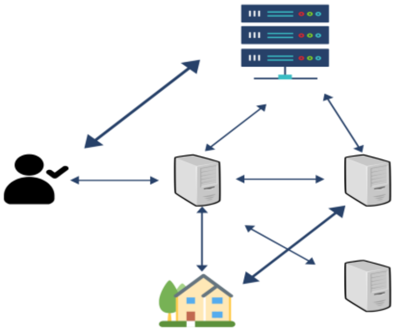

Figure 1. Threat Impersonation

This is an attack. The attacker managed to obtain an invalid but valid certificate for a valid domain server, and used a valid server ID for the fake certificate in the communication protocol. Any enemy different from A.com, you will receive a fake but valid certificate . The certificate, communicating with client C and playing the role of A, can persuade client C to contact and accept the forged certificate [16].

Tree based registration, where the registry is corrupted and given to the target victim (i.e. sharing your customer base) via two modified versions of the tree. The pseudo version violates very detailed server log operations by entering, omitting [11] [17], or changing registry keys. Powerful adversaries who control certificate authorities and CBs can forge forged but valid certificates contained in infected CBs (showing two different versions and signing for different customer groups) Alabama [18].

5. Secure Accountable Certificate Management

5.1 Supply Chain Management Digest

Supply chain management is a hybrid public key infrastructure solution that provides strong consistency and prevents misleading CIs. Although a strong enemy controls most parties, it can also protect customers and increase a sense of responsibility to all parties. Our

EC based supply chain management is publicly verifiable and observable on the blockchain platform [18].

Alice will now download the server log embed certificate, attach it with CertCAA , and send it to the client during the transport layer security handshake connecting to A.com over HTTPS [13]. The client browser uses the certificate authority's standard public key to verify CertCAA , just like the standard. Practice using predefined public keys for trusted server logs, and compare the root hashes of the server logs with the extracted tree root hashes to ensure that the server logs are included [19].

5.2 Platform

We outlined our blockchain model and extracted details that are not relevant to our research. Before using supply chain management services, let us prepare some basic knowledge of using blockchain as a service. CM needs a blockchain platform that customers can use to check the status of closed eligibility, and a suitable support contract to check status changes. You can use any consensus algorithm that does not enforce time forks to run on custom blockchains or blockchain media. keep going. CM stores valuable information in the form of state objects. , Which is a digital record controlled by a tamper-proof smart contract, such as Kublai et al. It is found that every transaction in supply chain management will lead to a change in the state tracked by the relevant organization.

5.3 Creation

In order to achieve connectivity in the hybrid supply chain management architecture, the TA key ID, if it is a TA certificate, contains the smart contract address space certificate of the statust, and the issuer ID supports the address certificate of the TA smart contract issued, only for the certificate field Valid, the TA certificate is empty.

5.4 Authorization

Travel agencies that wish to become part of the supply chain management infrastructure and sign or register certificates require voters to initiate the authorization process. After the TA confirms that it is correct, it generates a certificate with the extension of supply chain management, and contacts the group to register. On the blockchain, a group of voters (with CoSi) begins to sign a transaction to add TA. Meet the requirements of the supply chain management standardization agency for the global general ledger. The registered corporate client confirms the approved transaction and performs all necessary checks on the TA certificate. If the verification process is successful, the TA certificate will be added to the TA certificate list.

5.5 Domain Blockchain

After A.com CB receives the registration request of the domain name certificate, it will first check whether the database certificate already exists. If A.com does not exist, the server registration will generate a confirmation notification indicating that the certificate will be added from the server during registration [20]. In step 3, the registration server sends a CoSi-signed receipt to the client and instructs another registration center on the trusted server to add the certificate to its data record. The voters of this group have started the CoSi signing process. In step 5.

5.6 Server log updates

CB regularly updates its database with new certificates or updates existing certificates that need to be updated at known intervals. After the tree is updated, a new root will be calculated for the latest version of the server log tree. The fresh root is called the signature tree. The server's private registry keys are managed by root. The server registration sends the STR to one of the selectors to co-sign the relay with CoSi. Voters require voters to sign the collective signature root is the collective signature. It was published. The team then approves it as a transaction sent to the blockchain platform. The server log update cycle can be any time from one hour to one day. Frequent updates can ensure that the information is new, but will increase communication costs, because the domain needs to update the CB information regularly as a comprehensive test.

5.7 STR recorder

Miners implement a global supply chain management ledger and accept transactions. In addition, after updating the server log, voters can initiate a new transaction composed of the collectively signed root hash and resend the transaction through the P2P network. The miner will check this and insert the STR into the new block. Miners are motivated by the incentive mechanism used in Bitcoin or Ethereum. Voters will continue to monitor certification agencies for false certificates and violations. If a voter finds that an agency (such as a certification body or CB) has committed a crime by issuing or registering a forged certificate, the voter can revoke the certificate by signing the authorization to lift the blockade. Voters create a new transaction consisting of a forged authorization certificate and a revocation request. The transaction is distributed through the P2P network. The smart contract status regulator reviews the signed transaction and performs all checks. The process is successful, and the TA certificate is added to the list.The CA certificate has been revoked.

5.8 Membership contract

After the server logs update their database tree, the domain should receive new evidence that its CertCAA is actually registered in the server logs. The domain owner requests server logs to reaffirm CB membership. Upon receiving a PoP request for CertCA , the log server will perform appropriate tests on CertCA.

```
Algorithm 1 Certificate validation
Input : $Cert^{CA}_{A,}$,STR, PoP
Output : success, fail
function ISVALID($Cert^{CA}_{A}$,STR, POP)
        If ((pre-Validate($Cert^{CA}_{A}$,A.com) = 0)) then
            return fail
        end if
        if ((PoP.TR ≠ Miner.TR) ^ (CheckPoP($Cert^{CA}_{A}$,PoP,$pk_{LS}$)) = 0 ) then
            return fail
        else if ((verify($Cert^{CA}_{A}$,$pk_{CA}$))^(CA.status=”invalid”)=0) then
            return fail
        else
            return success
        end if
end function
```

Figure 2. Algorithm Certificate Validation

5.9 Log Server algorithm

Anyone can ask the central bank. The owner of the domain name submits questions as proof of acceptance to the central bank and protects it with its certificate. server logs answer questions after receiving test requests [21]. The following are tests that any log server can possibly perform. Our server logs can be described as tuples by the following algorithm, and the algorithm in Figure 3 has been formally defined.

5.10 Enter Server Log

Anyone can follow and review the EC. However, voters have the right to question server logs and find fake entries. Certification authorities can also look for faulty certificates in CI. the server log responds to the request after receiving the proof request [15]

5.12 Domain Renewal In Certificate

In supply chain management, certificate renewal can be used to renew a certificate or restore a certificate after the private key is leaked or lost. The revocation process (renewal process) of the supply chain management certificate is different from the standard X.509 PKI certificate. Chain management revokes a certificate by replacing the certificate with a new certificate [22]. Before the certificate expires or the key is lost, the domain owner creates a new key pair and sends a request to a trusted certificate authority to accept the new password. The domain owner also uses the previously registered private key to find the new key [23] [24]. The domain owner forwards the key update request to the server. Register and send a certificate update confirmation to the selector to generate a key update confirmation. Display new entries and updates and force the European Commission to update certificate entries. It will be added to the server log tree in the next update.

6. Safety Analysis Results

We assume that the password structure used for sending, tagging, and signing is secure. Sentence 1. If the anti-collision PoP (Authentication Path) and the certificate are not registered in the server log, the certificate authority will only cause damage, and the adversary cannot use a valid but forged certificate to simulate the domain.

Certificate. Because supply chain management is initialized on an existing blockchain (like Bitcoin) or a dedicated blockchain platform. In the first case, when an existing blockchain (such as Bitcoin) is used as a platform, the expenditure on global attacks will be double that of Bitcoin. It is clearly demonstrated that supply chain management can eliminate the attacks of a divided world.

We assume that a dedicated blockchain platform that uses supply chain management uses PBFT71 as the consensus algorithm . To attack a single world, the enemy must destroy at least n + 1 participants (consensus node) to collude. Create shared virtual blocks and create blockchain. We assume that A is assigned to n + 1 nodes. Enemies can trick target customers and use blocks with fake STR. However, this assumption contradicts the BFPT consensus algorithm (for example, no more than n nodes remain in the BFPT).

7. Supply Chain Management Performance

There are currently 3.3 × 108 domain registrations, and there are 27, so we are studying certificates for each subject, and CB is expected to have certificates for 3.3 × 108 domains registered with CB. We also assume that on average 20% of them are canceled each year. This equates to 904,109 registrations per day and 180,821 cancellation requests per day, for a total of 1,048,930 transactions per day. Guaranteed by the ECDSA algorithm , the approximate size of an X.509 certificate using a 256-bit public key is 29 bytes.

7.1 Server Log Performance

We consider the worst case, where each CB keeps every domain certificate, and one certificate has been registered with the CB for all domains. Therefore, for each CB, all 3.3 × 108 certificates must be stored, which equates to approximately 3.3 × 108 × 29 bytes≈ 168 GB [19]. This is constant and will not increase with the number of domains over time. 1GB disk space costs around US$0.053, while the server log maintenance costs are US$9.23, which is a negligible investment. Similarly, the size of the test depends on the number of certificates and the hash function used when computing the Merkle tree. In supply chain management, SHA256 is used as a hash function, and the number of certificates is 3.3 × 108. This test consists of about 32 hashes and STRs 1KB of data.

7.2 Blockchain Performance

Compared to the previous proposal, CM greatly reduces the size of the blockchain. Blockchain-based public key infrastructure solutions typically require the same amount of storage space as the number of domain certificates stored in the registry. The blockchain size of a 1.65 x 108 CertLedger domain certificate is approximately 512 GB. Now, let's estimate the cost of blockchain supply chain management, which is calculated using the following formula: STRsize × nlog × ndays × updaterate, where STRsize is approximately 136 bytes. We assume that nyt requires 8 bytes of memory. Figure shows that if the log server updates the database once a day, the size of the blockchain is 100 server logs, which is less than 10 MB a year. The size of the blockchain increases linearly with the update speed, and becomes maximum when the log server updates its data records every hour. Figure 7B shows that when the update speed is 1 per day, even for 1000 server logs, the blockchain size will barely reach 50MB. Figure 7C shows the 1 month data required to extract the blockchain on the platform, and the amount increases linearly with increasing numbers.

7.3 Experimental Installation

An example blockchain that stores root credentials and hash information. The server is implemented using the Nginx server extension, and the client is implemented in Chromium. The server registry is created by modifying existing and existing Merkle structures. The local blockchain is modified through OpenSSL through Python and CA. We use ECDSA with elliptic secp256k1 as the signature algorithm. The experiment was carried out on five physical machines. The machine configuration is shown in Table 3. Voters uses CoSi ## to simulate a small network consisting of three machines, with Leader as the public unit of blockchain transactions. The platform and Internet configuration connection via 10 Mbit/s Wi-Fi, CM cost and overhead will not cause any significant delay in establishing a secure connection for the transport layer. However, due to the PoP cluster, supply chain management requires about 1KB of bandwidth to establish a transport layer secure connection, and the browser trusts the CA registered on the blockchain.The verification of the domain certificate includes performing the pre-verification function, checking the root hash, checking the PoP in the server log, checking the certificate and verifying whether your CA is Credible. It takes approximately 80 milliseconds to register the certificate, and approximately 10 milliseconds to verify the application. Verification in CertLedger18 requires approximately 20 milliseconds to generate a CoSi signature, while verification requires 0.08 and 0.07 per second. The time to create the Merkle hash tree is 12 seconds, and the time is p. The average test creation time is 45 seconds, and the average test time is 140 seconds. With the support of a dedicated blockchain, any node can easily become a mature node. We are also investigating the addition of root hashes to existing blockchain platforms such as Bitcoin. The research team must pay bitcoin transaction fees to add the root hash value to the ledger. This is explained in Section 7. First, the client must synchronize with the Bitcoin network, which costs about 40.6 MB. After that, the client chain management software will periodically connect to the blockchain and the platform registration server to obtain the new block header and root hash value for monitoring. The client needs less than 15MB of space for root hash transactions and header blocks (if the database is updated once a day, every 100 server records).In addition, the Bitcoin architecture generates approximately 160 blocks per day, so customers must download approximately 12.8 KB of data per day.

7.4 Ratio

Which is conducted. We are also exploring the implementation of various blockchain and ledger based proposals. First, we examine whether the certification authority or domain needs to change its business model (process and configuration) to implement a particular infrastructure. If the certificate authority changes, CT instructs the certificate authority to embed the certificate's timestamp [25]. On the other hand, AR public key infrastructure forces certificate authorities to control server logs, whereas in BlockPKI, certificate authorities participate in multi-signature protocols. To use a layer of security certificates transport and signature key anti signature AKI and ARPKI , you should contact several certificate authorities' trusted list and bind their certificates. In CertLedger , the domain must monitor for fake certificate registrations.

8. Discussion Results

In terms of implementation, CT is supported by all major CAs (such as Lets Encrypt), and all major servers and browsers are currently using CT. Google recently started implementing CT registration for all its recently issued transport layer security certificates. Extend to CT registration server with minimal changes. Google Transparent Log is optimized for deployment, while supply chain management is optimized for deployment and security. To this end, a supply chain management infrastructure has been developed, and a general CT model can be used. For security and transparency reasons, domain name owners are also interested in implementing supply chain management. Therefore, we believe that as people become more interested in secure networks, domain owners and the Internet community can apply supply chain management to CT while making minor changes to the environment. Today's transport layer security public key infrastructure.Supply chain management in supply chain management includes preventive measures, which can prevent the spread of global attacks by reducing the credibility of CI. The client receives the CI-generated confirmation only after it obtains the root hash and is verified by a group of voters to ensure that the client sees the original version of the server log seen by other voters and the client [8]. Transport layer security standardizes transport layer security, data protection and performance, and makes authorization management transparent. Remove security from weak channels and prevent spoofing attacks. Since the supply chain management domain server sends a server commitment regarding transportation safety guarantee in the transportation safety extension, the supply chain management directly provides the advantage of adding the transportation safety extension to the transportation safety extension.3 Supports sending test certificates through the best transport layer security extension [26] [15]. Browser warnings Most Internet users trust the public key infrastructure and are unaware of certificate warnings. Usually they ignore this warning and click on it, which may cause a man-in-the-middle attack. 14 Supply chain management does not have to impose solutions on customers, but it can detect attacks and prevent them from being unable to click on the appropriate options.

9. Conclusions

In this article, we will introduce supply chain management, a new type of hybrid public key infrastructure that takes advantage of the advantages of the two new architectures. Supply chain management counteracts the absolute authority of TA (certification body and server registration) by allowing domains (voters) to respond to authority and revoke certificates immediately. Supply chain management also eliminates the need for supply chain management customers to manage or store trusted keys or certificates, and reduces the reliance on browser vendors to manage trusted keys. Security analysis shows that supply chain management provides strong protection against spoofing attacks and powerful attackers. The ability to control most details. In addition, compared with previous blockchain-based work, supply chain management reduced the data storage on the blockchain from 512 GB to 120 MB, and significantly reduced the number of transactions. Inventory, cost and performance analysis shows that supply chain management can be used in practice. In the future, we plan to implement supply chain management in existing blockchain structures for comprehensive performance. We also plan to set detailed requirements and instructions for adding/removing CA and server logs.

Acknowledgments

With high enthusiasm and motivation to work on a journal entitled "Blockchain Technology as a Media for Sharing Information that Generates User Access Rights and

Incentives" Thank you to University of Raharja and also Alphabet Incubator who have fully supported this research. So that participation in this research is able to expand knowledge for myself and for other communities, especially for the world of digitization.

References

[1] K. M. Moriarty, *Transforming Information Security: Optimizing Five Concurrent Trends to Reduce Resource Drain*. Emerald Group Publishing, 2020.

[2] U. Rahardja, Q. Aini, H. D. Ariessanti, and A. Khoirunisa, “Pengaruh Gamifikasi pada iDu (iLearning Education) dalam Meningkatkan Motivasi Belajar Mahasiswa,” *NJCA (Nusantara J. Comput. Its Appl.*, vol. 3, no. 2, pp. 120–124, 2018.

[3] U. Rahardja, I. Handayani, and A. A. Ningrum, “Pemanfaatan Sistem iMe Berbasis WordPress sebagai Official Site RCEP pada Perguruan Tinggi,” *Creat. Inf. Technol. J.*, vol. 4, no. 3, pp. 207–219, 2018.

[4] S. Ayvaz and S. C. Cetin, “Witness of Things: Blockchain-based distributed decision record-keeping system for autonomous vehicles,” *Int. J. Intell. Unmanned Syst.*, 2019.

[5] D. Ahmad, N. Lutfiani, A. D. A. R. Ahmad, and U. Rahardja, “Blockchain Technology Immutability Framework Design in E-Government,” *J. Adm. Publik Public Adm. J.*, vol. 11, no. 1, pp. 32–41, 2021.

[6] Q. Aini, N. Lutfiani, and M. S. Zahran, “Analisis Gamifikasi iLearning Berbasis Teknologi Blockchain,” *ADI Bisnis Digit. Interdisiplin J.*, vol. 2, no. 1, pp. 79–85, 2021.

[7] P. Edastama, N. Lutfiani, Q. Aini, S. Purnama, and I. Y. Annisa, “Blockchain Encryption on Student Academic Transcripts using a Smart Contract,” *J. Educ. Sci. Technol.*, 2021.

[8] J. Lin, Z. Shen, C. Miao, and S. Liu, “Using blockchain to build trusted LoRaWAN sharing server,” *Int. J. Crowd Sci.*, 2017.

[9] D. Sinha and S. R. Chowdhury, “Blockchain-based smart contract for international business–a framework,” *J. Glob. Oper. Strateg. Sourc.*, 2021.

[10] I. Amsyar, E. Christopher, A. Dithi, A. N. Khan, and S. Maulana, “The Challenge of Cryptocurrency in the Era of the Digital Revolution: A Review of Systematic Literature,” *Aptisi Trans. Technopreneursh.*, vol. 2, no. 2, pp. 153–159, 2020.

[11] P. R. Sousa, J. S. Resende, R. Martins, and L. Antunes, “The case for blockchain in IoT identity management,” *J. Enterp. Inf. Manag.*, 2020.

[12] U. Rahardja, A. N. Hidayanto, N. Lutfiani, D. A. Febiani, and Q. Aini, “Immutability of Distributed Hash Model on Blockchain Node Storage,” *Sci. J. Informatics*, vol. 8, no. 1, pp. 137–143, 2021.

[13] A. S. Bein, Y. I. Graha, and A. P. Pangestu, “Pandawan Website Design Based Content Management System As Media E-commerce Transaction,” *Aptisi Trans. Technopreneursh.*, vol. 2, no. 1, pp. 87–97, 2020.

[14] I. Noburu, A. Himki, A. Dithi, K. Kano, and M. Anggraeni, “Covid-19: Portrait of Preservation of the Batik Industry as a Regional Autonomy,” *Aptisi Trans. Technopreneursh.*, vol. 2, no. 2, pp. 143–152, 2020.

[15] U. Rahardja, Q. Aini, and D. Sartika, “Build A Business To Customer Online Store Using Airzone Content Management System,” *CCIT J.*, vol. 8, no. 2, pp. 112–122, 2015.

[16] J. Hom, B. Anong, K. B. Rii, L. K. Choi, and K. Zelina, “The Octave Allegro Method in Risk Management Assessment of Educational Institutions,” *Aptisi Trans. Technopreneursh.*, vol. 2, no. 2, pp. 167–179, 2020.

[17] R. Untung, I. Handayani, and B. A. Pahad, “Pemanfaatan Rinfoform Sebagai Media Update Artikel Pada iRan,” *J. CSRID*, vol. 8, no. 3.

[18] X. Xue, J. Dou, and Y. Shang, “Blockchain-driven supply chain decentralized operations–information sharing perspective,” *Bus. Process Manag. J.*, 2020.

[19] E. Guustaaf, U. Rahardja, Q. Aini, H. W. Maharani, and N. A. Santoso, “Blockchain-based Education Project,” *Aptisi Trans. Manag.*, vol. 5, no. 1, pp. 46–61, 2021.

[20] P. Xie, Q. Chen, P. Qu, J. Fan, and Z. Tang, “Research on financial platform of railway freight supply chain based on blockchain,” *Smart Resilient Transp.*, 2020.

[21] U. Rahardja, Q. Aini, and A. Khoirunisa, “The Effect of Rinfogroups as a Discussion

Media in Student Learning Motivation," *Aptisi Trans. Manag.*, vol. 2, no. 1, pp. 79–88, 2018.

[22] N. Kant, "Blockchain: a strategic resource to attain and sustain competitive advantage," *Int. J. Innov. Sci.*, 2021.

[23] S.-C. Oh, M.-S. Kim, Y. Park, G.-T. Roh, and C.-W. Lee, "Implementation of blockchain-based energy trading system," *Asia Pacific J. Innov. Entrep.*, 2017.

[24] A. B. Turner, S. McCombie, and A. J. Uhlmann, "A target-centric intelligence approach to WannaCry 2.0," *J. Money Laund. Control*, 2019.

[25] Q. Aini, Y. I. Graha, and S. R. Zuliana, "Penerapan Absensi QRCode Mahasiswa Bimbingan Belajar pada Website berbasis YII Framework," *Sisfotenika*, vol. 7, no. 2, pp. 207–218, 2017.

[26] R. P. George, B. L. Peterson, O. Yaros, D. L. Beam, J. M. Dibbell, and R. C. Moore, "Blockchain for business," *J. Invest. Compliance*, 2019.