Design Printed Signature Protocol based on a Blockchain Concept

Aslan Alwi
Universitas Muhammadiyah Ponorogo

Julan Hernadi
Universitas Ahmad Dahlan Yogyakarta

Munirah
Universitas Muhammadiyah Ponorogo

ABSTRACT
For a certain reason, usually an agency validates certain document sheets using a printed signature, for example the Dukcapil Office in signing a family card. The printed signature here uses a Qr-Code or barcode instead of a wet signature. Verification of the printed signature is done by scanning a Qr-Code or barcode which triggers the appearance of a website page stating the validity of the printed signature. One of the disadvantages of printed signatures is that they are vulnerable to tampering, such as transferring signatures for unauthorized documents. This is because the signature authenticity validation authority is single. This article introduces a blockchain-based signature protocol that is believed to be able to guarantee the security of printed signatures and the document itself. The security guarantee here is because the validation authority holder is not single but is distributed among the various parties involved.

General Terms
Blockchain, Print Signature Protocol, Protocol for generating of the printed signatures (PTC), Metadata storage protocol on blockchain (PMB), Printed signature verification protocol (VTC).

Keywords
Printed Signature, Protocol, Blockchain, Validation, Verification, Authority.

1. INTRODUCTION
Each country, including ASEAN countries, issues its own regulations regarding digital signatures that might be used to understand the position of printed signatures in general [1]. The legal basis for this printed signature is issued by the government. In Indonesia, the legal umbrella for printed signatures is Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE) and was revealed in Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions [2], [3], [4].

Printed signatures are part of the electronic signature. This type of signature is very useful for bulk signing of many documents without having to involve the presence of the signer at the place of the signature. People may also apply similar ideas to sticky stamps [5]. Printed signatures in the form of using Qr-Code to sign documents in office administration activities have become a part that we commonly encounter in various institutions, be it government or private institutions. Such as affixing a Qr-Code on a family card stating the signature of the Head of the Population and Civil Registration Service, or on the issuance of a certificate that affixes a Qr-Code as the signature of the certifying authority.

Print signatures such as Qr-Code are usually used for signing documents that do not involve transactions or transactions of large value, because their legal force is weaker than wet signatures[6], [7].Verification of the printed Qr-Code signature rests on a site that provides information on the validity of the printed Qr-Code signature. Because of this, usually a Qr-Code represents a URL link that leads to an official site that certifies its validity. However, it is also possible that Qr-Code can represent other codes or certain images that can be seen as sufficient power to validate the signature. This is one of the drawbacks of these Qr-Code-based signatures and documents.

From the network aspect, if the official website is hacked, then people can easily manipulate the printed signature as if the entity listed in the document is a legitimate entity listed in the document and recognized by the authorities. Documents with printed signatures can be used to commit fraud. Another drawback is that other unauthorized persons can manipulate the Qr-Code by creating a new Qr-Code and printing it in a similar document and redirecting it to another ostensibly official site. The person can also use the document to commit malicious acts. There is yet another drawback, printed Qr-Code signatures might be used as a troyan that redirects to malicious sites causing someone's device to be attacked by malware or other malicious code.

This article offers a printed signature protocol which is expected to overcome the above weaknesses, and is expected to increase the legal power of a printed signature although it may not be as strong as a wet signature legal force. However, it is very possible to use it for small- value business transactions or to increase the security of printed signatures in the administration of government or private institutions. It is possible that this signature protocol can replace the validity of a wet (conventional) signature, of course after going through a series of scientific tests.

The protocol that we want to present in this paper rests on the power of a distributed and decentralized blockchain. Hopefully, every printed signature verification involves security standards in the chain of encryption blocks in the blockchain. Several agencies have implemented this blockchain technology, such as the application of blockchain for postage stamps [8], application to digital certificates [9], [10], [11].

In general, the idea in this paper relies on verification of printed signatures on open, distributed and decentralized verification so that the problem of security verification that is

centered on a URL link is that there is a danger of hacking the site that can cause tampering of the resulting printed signature can be reduced.

In further development, the idea of adding a time element as a time-stamp for the metadata of the document to be signed opens the possibility for historical records of all printed

signatures so that the legal traces of each signature can be traced properly and provide stronger security. Not only are printed signatures anti-tampering but the entire history of printed signatures is also anti-tampering. This idea prevents and detects signature forgery in history. Zhang et al (200?), put forward the idea of blockchain-based time-stamping which might be a reference for implementing the expansion of this idea [12]. As also stated by W. Detho in his thesis [13].

2. BLOCKCHAIN: AN OVERVIEW

Since bitcoin was first discovered and introduced by Satoshi Nakamoto, bitcoin as a new way of online payments using electronic money where payments are made directly peer-to-peer using blockchain [14], this has been the inspiration that sparked the growth of blockchain technology as a technology which can replace various systems in various fields. Blockchain then has strong implications in the economy and business, changing the ways in which the financial and trading system, bringing the economy and business to a token-based system with blockchain as a supporting platform [15]. Research on blockchain is growing in this area. The need to make all physical transactions into transactions on a cryptographic-based blockchain with strong security. Such as research [16] which proposes a transaction pricing mechanism scheme in transactions on blockchain. Blockchain has also penetrated the health sector [17], pharmaceuticals

[18] supply chain in various industries [19], underpinning IoT technology and its network [20], government and policy management [21], energy management for example using smart grids [22], finance dan marketing [23].

This paper proposes one application of blockchain, that is the application of the technology for printed signatures that are commonly used in various government and private institutions. Printed signatures are usually in the form of a Qr-Code or barcode that is printed on a physical document as a form of signature that replaces a conventional signature (wet signature). This paper proposes a printed signature protocol that places blockchain as the main support for the strength and security of printed signatures, so that it is expected to be reliable for use in various high-value transactions and transactions.

3. PROPOSED PROTOCOLDESIGNFOR PRINTED SIGNATURE

The following is a draft of a printed signature protocol which is expected to be a solution to the weaknesses of printed signatures. This protocol starts with some basic assumptions. With the hope, that the assumption is sufficient to guarantee the security of the protocol mechanism. This protocol involves the blockchain as the backbone that underpins the traceability and anti-tampering nature of the printed signature. This protocol must have some weaknesses, but it is hoped that by initiating the beginning for its development, in the future this protocol can still continue to grow and improve.

3.1. Print Signature Protocol BasicAssumptions

The design protocol for printed signatures proposed in this paper is based on the following assumptions:

- **Basic assumptions for creating a printed signature:**
  a. The user who creates the printed signature is an institution, either a government or private institution, hereinafter referred to as an Institution.
  b. The institution determines to use an asymmetric encryption algorithm and then generates the public key and private key either permanently or periodically.
  c. The private key is used for encryption.
  d. The public key is used for decryption.
  e. The public key is published on the Institute's official website.
  f. The institute defines a hash algorithm to be used for hashing within the print signature protocol mechanism.
  g. Physical or digital document metadata is a detailed identity record and important points about the document to be signed in print added with photo, video and audio evidence of the physical document if needed.
  h. The printed signature backing blockchain can be an institution's private blockchain, or a consortium with other institutions or using a third-party public blockchain.

- **Basic assumptions for users of documents signedbyusing a printed signature:**
  a. Document users are anyone, either individuals or in theform of an institution.
  b. Documents used may be physical or digital.

- **Basic assumptions for print signature verifier:**
  a. Verifier is anyone either individual or institution.
  b. The verifier checks the validity of the printed signature.

3.2. Protocol for Generating of ThePrinted Signatures (PTC)

The following is based on some of the basic assumptions put forward in section A. A protocol algorithm for the generation of printed signatures is proposed. This protocol is implemented by the institution that makes and then prints the printed signature. Algorithm This protocol is called the PTC protocol and is expressed in the following steps:

PTC Protocol
Step 0. Start
Step 1. The institution creates a physical or digital document for the agency to sign and generates the metadata.
Step 2. The institution implements the metadata storage protocol to the blockchain using the PMB protocol (a separate protocol stated in clause C).
Step 3. Institutions retrieve block addresses and transaction numbers from the metadata that has been stored on the blockchain.
Step 4. The block address and transaction number are then encrypted using the Institution's private key.
Step 5. The results of the encryption are then made a Qr-Code.
Step 6. The QR-Code is then printed as a digital signature on a physical document or attached to a digital document.
Step 7. End.
Figure 1 provides a flowchart of how the protocol algorithm works.

3.3. Metadata Storage Protocol on Blockchain (PMB)

The following is based on some of the basic assumptions put forward in chapter A. A protocol algorithm for storing metadata on the blockchain is proposed.

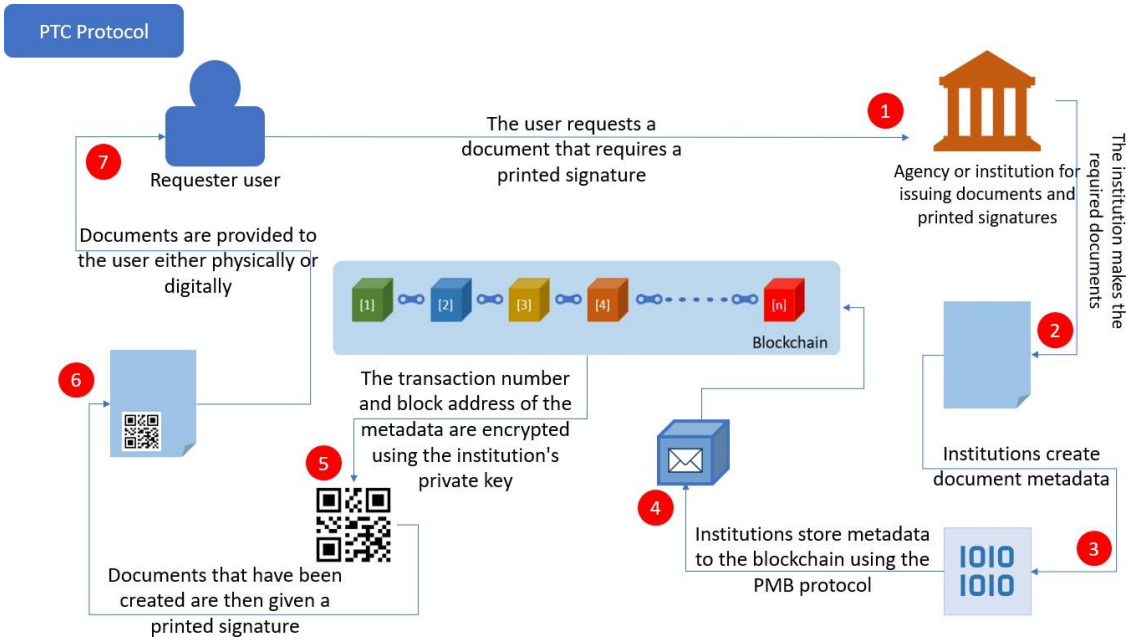

Fig 1: PTC Protocol Design provides a flowchart of how to add a printed signature to a documen

This protocol is implemented by the institution when storing the metadata of the document to be given a printed signature. As stated earlier, the print signature metadata contains the identity of the recipient of the printed signature and all the important points that summarize the document to be signed. It is not closed that a complete digital copy of the document can be attached as a complement to the proof of the printed signature. This protocol is called the PMB (Metadata Storage on Blockchain) protocol and is stated as follows:

PMB Protocol

Step 0. Start
Step 1. The institution has created the metadata of the document to be signed.
Step 2. The metadata is then encrypted using the institution's private key.
Step 3. The results of the metadata encryption are then made a hash code.
Step 4. Metadata and hash codes are then stored as one or more transaction items and then stored in a candidate block.
Step 5. Candidate blocks are added to the blockchain according to the blockchain protocol chosen by the institution. The blockchain protocol is at the institution's choice, whether it is a private blockchain, consortium blockchain or public blockchain.
Step 6. The institution then records the block address and transaction number in a large table including the hash value of the proof document. Overall, the table in one record at least states the identity of the person who is given a printed signature, the block address and transaction number and the hash value of the proof document.
Step 7. The institution then stores the large table in another block of the blockchain according to the blockchain storage protocol or procedure the institution chooses
Step 8. End.
Figure 2 describe the PMB protocol design.

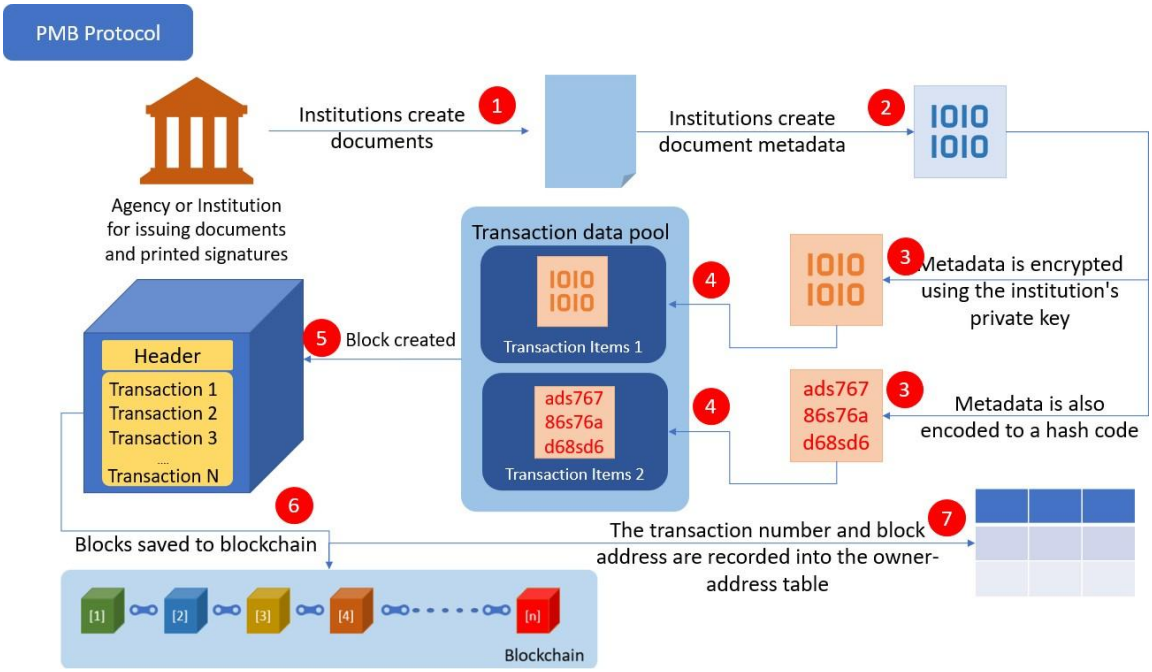

Fig 2: The PMB Protocol Design provides a flowchart of how to store print signature metadata to the blockchain

3.4. Printed Signature VerificationProtocol (VTC)

The following is based on some of the basic assumptions put forward in section A. An algorithmic protocol for verification of printed signatures is proposed. This protocol states the steps for performing print signature verification. Verification can be done by anyone. Verification is not closed to one of the other institutions that receive the document or anyone, but is open to the public, whether the document with a printed signature is addressed to it or not. It is hoped that this protocol will maintain openness and traceability of printed signatures (traceability). Furthermore, in this protocol, the party conducting the verification is referred to as a verifier. This protocol is referred to as the VTC (printed signature verification) protocol and is stated as follows:

VTC Protocol

Step 0. Start

Step 1. The verifier extracts the printed signature into a series of data.

Step 2. The verifier accesses the public key of the issuing agency whose signature is printed on the document. The public key of the institution is accessed on the official website of the institution.

Step 3. The extracted data is then decrypted using the public key of the issuing institution for the printed signature.

Step 4. The block address and transaction number obtained as a result of the decryption are then used to access the blockchain.

Step 5. The contents of the block in the transaction number on the blockchain are then decrypted using the public key of the issuing institution of the printed signature.

Step 6. The verifier then verifies the signed document usingthe decrypted transaction data.

Step 7.End.

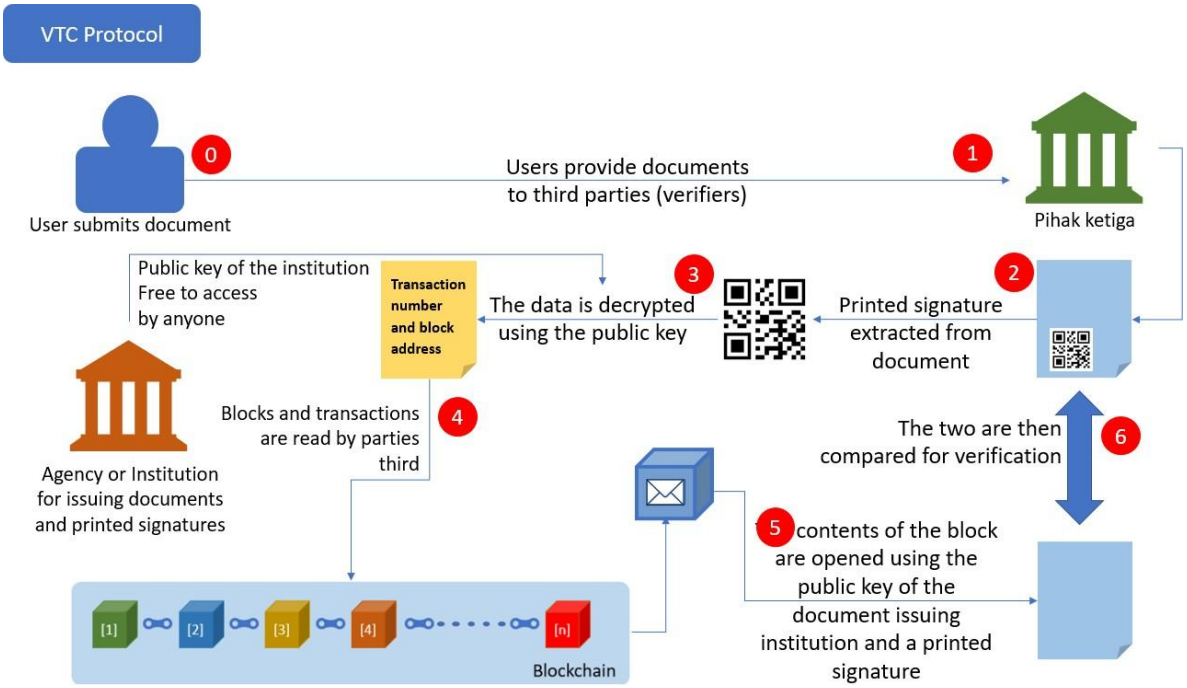

Fig 3: The VTC Protocol Design provides a flowchart of how to verify printed signatures on documents

3.5. Analysis

The analysis of the proposed protocol is an analysis of the security of the printed signature protocol based on the blockchain. Since the signature protocol is based on the blockchain, the security of the printed signature means the security of the blockchain system that supports it. Therefore, the security of the printed signature protocol depends on the choice of the blockchain type used to support it. Table 1 presents the blockchain types [24] that can be selected as blockchain types to support the print signature protocol. A private blockchain is a blockchain built by an organization and write rights are controlled by that organization [24] so this type of blockchain is not actually decentralized, and therefore could be tampered with [25].

Print signature protocols based on private blockchains certainly have a higher computational complexity to tamper print signatures than print signatures that do not use blockchain. Therefore, they are relatively safer than print signatures that do not use blockchain. However, the population of blockchain copy holders on consortium blockchains is relatively larger than private blockchains, so the computational complexity for tampering is higher on consortium blockchains. But public blockchains due to their highly decentralized nature, thus having a larger population of blockchain copy holders than consortium and private blockchains, then public blockchains have greater computational complexity than consortium and private blockchains. Thus, public blockchains are the safest choice of all blockchain types on which to base printed signature protocols.

Table 1. Classification of Blockchains

Types	Describe	SoC	Scenarios
Public Blockchain	Anyone can participate and is accessible worldwide	Slow	Global decentralized scenarios
Consortium Blockchain	Controlled by pre-selected nodes within the consortium	Slight Fast	Businesses among selected organizations
Private Blockchain	Write rights are controlled by an organization	Fast	Information sharing and management in an organization

If the print signature protocol is based on a blockchain private, consortium or public then the print signature security analysis means the computational complexity of tampering the printed signature. This computational complexity can be seen in attacks on user credentials using print signature applications, on private keys for asymmetric signature security, on blockchain hashing chains, and on the population of blockchain copy holders to attempt to form new forks in the blockchain so that signatures print can be used more than once legally for purposes other than the original purpose (double spending – double using of print signature).

The computational complexity analysis for the print signature protocol security is as follows:

a. Computational complexity for attacking non blockchain-based print signature protocol

For non blockchain-based print signature protocols, the attack that occurs is an attack on user credentials on the client side of the signature application or on the server side that stores print signature validation. The computational complexity of this attack is only equivalent to the computational complexity of hacking user passwords on the client side or passwords on the server side. Suppose the total number of symbols in the universal set of symbols used to create a password on the client side is N and the length of the password created is L1 characters, then the number of computational steps is NL1. So the computational complexity is $O(N^{L1})$. For example, on the server side using the universal symbol set is M and the

character length is L2, then on the server side it is $O(M^{L2})$, so the overall complexity is $O(\max(M,N)^{Max(L1,L2)})$. Say $O(Mx^{Lx})$.

b. Computational complexity for attacking blockchain-based print signature protocol

However, in the blockchain-based print signature protocol, there are K computers that hold a copy of the blockchain (miner or verifier) so the computational amount to hack the credentials of all users on the blockchain, is $M_1^{L1} + M_2^{L2} + M_3^{L3} +...+ M_k^{Lk}$ eg Mx is $\max(M_1,M_2,M_3,...,M_k)$ and Lx is max(L1,L2,L3,..,Lk) then the computational complexity to hack all users' credentials in blockchain-based print signature protocol is $O(K.Mx^{Lx})$, K times more complicated than non blockchain-based print signature protocols.

However, apart from having to hack user credentials, hackers also have to hack all the hashes that are interlinked between blocks. Suppose the computational complexity to hack a SHA256 hash is O(SHA256), and the chain length in the blockchain is W blocks then the overall computational complexity to hack a blockchain file is O(W.SHA256). But there are K users holding a copy of the blockchain. To hack the blockchain system, it is only necessary to hack 51% of the number of users holding a copy of the blockchain, which is 1/2K + 1 user. So the computational complexity for hacking a blockchain is O((1/2K+1).W.SHA256). so the overall computational complexity to hack or tamper print signatures on a blockchain-based print signature protocol is $O(K.Mx^{Lx})$ and O((1/2K+1).W.SHA256).

However, $K_{private} \leq K_{consortium} \leq K_{public}$ so that the highest computational complexity is in the blockchain-based print signature protocol which is based on the public blockchain.

3.6. The Advantages Of Proposed Protocol

The proposed protocol is expected to solve the following intended security problems:

Problem 1:
Print signature verification addressed to a link issuing agencyor print signature maker.

Scenario:
Verification addressed to a URL link is a verification that relies on a server as a central verification of all printed signatures issued by the institution. This condition is very vulnerable when someone can hack the server then all printed signatures issued by the institution become dubious. Where someone out there can forge a printed signature freely by validating every fake signature.

Solution:
The protocol proposed in this paper does not place signature verification in a centralized and closed manner. But placing a signature verification center on the blockchain. So that the information that certifies the signature becomes distributed and decentralized and is open to anyone.

If someone wants to hack all the information used to verify the printed signature then that person has to hack the distributed and decentralized blockchain. This reduces the possibility that someone can hack and forge an agency's printed signature.

Problem 2:
Someone who forged the agency's printed signature and redirected the verification to a look- alike URL.

Scenario:
Someone creates a printed signature, but the URL link in the printed signature redirects to a URL that is similar to the URL of the agency's verification site. So that other people think that the forged signature is legitimate.

Solution:
The information that verifies the signed document is stored on the blockchain and locked using the public key of the issuing agency of the printed signature. This causes someone with malicious intent to not be able to falsify the identity of the agency issuing the printed signature, because the information is locked using the agency's private key which is confidential and only held by the institution.

Problem 3:
Someone who can use a printed signature to redirect to a malicious site.

Scenario:
Someone creates a malicious site and creates a fake printed signature in the form of a Qr-Code that points to the malicious site. If the signature is scanned by a Qr-Code reader application, there is a possibility that the applicationdirectly redirects people to the malicious site. This becomes even more dangerous if someone who is doing this malicious thing creates a Qr-Code reader application. The application freely redirects other people to malicious sites, and opens those sites automatically.

Solution:
This protocol does not direct the printed signature verification to a site, but to a block address and transaction number on the blockchain. The information stored there is also locked using the private key of the issuing institution. So that the hazard conditions that lead directly to dangerous sites are reduced.

4. CONCLUDING REMARKSANDDISCUSSION

At a certain degree of security, this protocol may be used by various institutions to sign business transactions with the masses who interact with these institutions. This institution can be a company that sells something and must issue aninvoice or purchase receipt.

The creation of a printed signature system using a Qr-Code or Barcode whose verification is based on a centralized server has a weakness due to its centralized nature, namely that once someone can enter and intervene on the centralized computer, all transactions and affairs involving printed signatures are easy to manipulate and become invalid. So that the existing print signature technology can only be used for documents that are not too important and not critical. This is because of its weak power in guaranteeing the two parties either the undersigned or the one who receives the signature.

However, by relying on the print signature protocol to the blockchain, the power of signatures lies in encrypted, decentralized, distributed storage. So as to provide a stronger guarantee for the security of both parties when a printed signature occurs.

5. ACKNOWLEDGMENTS

Our thanks to the research team who have contributed towardsdevelopment of this paper.

6. REFERENCES

[1] N. Sargunaraj, "Electronic & Digital Signatures in ASEAN," ASEAN, p. 5, 2020.

[2] PRESIDEN REPUBLIK INDONESIA, "UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK," LEMBARAN NEGARA REPUBLIK INDONESIA NOMOR 4643. TAMBAHAN LEMBARAN NEGARA REPUBLIK INDONESIA NOMOR 4843, 2008.

[3] PRESIDEN REPUBLIK INDONESIA, "PERATURAN PEMERINTAH REPUBLIK INDONESIA NOMOR 82 TAHUN 2012 TENTANG PENYELENGGARAAN SISTEM DAN TRANSAKSI ELEKTRONIK." TAMBAHAN LEMBARAN NEGARA REPUBLIK INDONESIA NOMOR 5348, 2012.

[4] Kemkominfo, "Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik," UU No. 19 tahun 2016, no. 1, pp. 1–31, 2016.

[5] D. Ankaa Wijaya, F. Junis, and D. Ariadi Suwarsono, "SMART STAMP DUTY," in Seminar Nasional Perpajakan 2018, 2018, pp. 1–12.

[6] Zakiyah, R. A. Insyirah, and A. Maulana, "Kajian Yuridis Keberadaan Tanda Tangan Yang Dibuat Dengan Menggunakan Alat Pemindai (Scanner) Dalam SebuahPerjanjian," pp. 1–60, 2019.

[7] H. Hudzaifah, "Keabsahan Tanda Tangan Elektronik Dalam Pembuktian Hukum Acara Perdata Indonesia," Katalogis, vol. 3, no. 5, pp. 194–204, 2015.

[8] Y. Yanovich, I. Shiyanov, T. Myaldzin, I. Prokhorov, D. Korepanova, and S. Vorobyov, "Blockchain-based supply chain for postage stamps," Informatics, vol. 5, no. 4, Nov. 2018.

[9] A. Argani and W. Taraka, "Pemanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertifikat Pada Perguruan Tinggi," ADI Bisnis Digit. InterdisiplinJ., vol. 1, no. 1, pp. 10–21, 2020.

[10] S. N. Billah, R. Pollobe, F. Hossain, N. M. Abir, A. Z. Zarin, and M. F. Mridha, "Blockchain Based Architecture for Certificate Authentication," SSRN Electron. J., 2021.

[11] M. Garriga, M. Arias, and A. De Renzis, "Blockchain and Cryptocurrency: A comparative framework of themain Architectural Drivers," 2018.

[12] Y. Zhang, C. Xu, N. Cheng, H. Li, H. Yang, and X. Shen, "Chronos+: An Accurate Blockchain-Based Time- Stamping Scheme for Cloud Storage," IEEE Trans. Serv. Comput., vol. 13, no. 2, pp. 216–229, Mar. 2020.

[13] W. Detho, "Developing a system for securely time-stamping and visualizing the changes made to online news content Master Thesis," Universitat Konstanz, 2016.

[14] S. Nakamoto, "Bitcoin : A Peer-to-Peer Electronic Cash System," pp. 1–9, 2008.

[15] P. Freni, E. Ferro, and R. Moncada, "Tokenomics and blockchain tokens: A design-oriented morphological framework," Blockchain Res. Appl., vol. 3, no. 1, p. 100069, 2022

[16] Z. Wang, Q. Hu, Y. Wang, and Y. Xiao, "Transaction pricing mechanism design and assessment for blockchain," High-Confidence Comput., vol. 2, no. 1, p. 100044, 2022.

A. Abadeh, "Blockchain and medicine : From digital promise to frontline practice," Ann. Med. Surg., vol. 76, no. April, p. 103555, 2022.

[17] Haq and O. M. Esuka, "Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs," no. April, 2018.

[18] M. A. N. Agi and A. K. Jha, "Blockchain technology in the supply chain: An integrated theoretical perspective of organizational adoption," Int. J. Prod. Econ., vol. 247, no. June 2021, p. 108458, 2022.

[19] M. T. Al Ahmed, F. Hashim, S. Jahari Hashim, and A. Abdullah, "Hierarchical blockchain structure for node authentication in IoT networks," Egypt. Informatics J., no. xxxx, 2022.

[20] M. Foy, D. Martyn, D. Daly, A. Byrne, C. Aguneche, and R. Brennan, "Blockchain-based governance models for COVID-19 digital health certificates: A legal, technical, ethical and security requirements analysis," Procedia Comput. Sci., vol. 198, no. 2021, pp. 662 – 669, 2021.

[21] Y. Guo, Z. Wan, and X. Cheng, "When Blockchain Meets Smart Grids: A Comprehensive Survey," High- Confidence Comput., p. 100059, 2022.

[22] E. Maguire, D. Hicks, W. Keat Ng, T. Yew Chia, and S. Marshall, "Could blockchain be the foundation of a viable KYC utility?," KPMG Int., pp. 1–8, 2018

[23] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," ACM Comput. Surv., vol. 52, no. 3, 2019.

[24] R. Stephen and A. Alex, "A Review on BlockChain Security," IOP Conf. Ser. Mater. Sci. Eng., vol. 396, no. 1, 2018.