cryptography

MDPI

Article

Trusted and Secure Blockchain-Based Durable Medium Electronic Service

Grzegorz Bazydło, Remigiusz Wiśniewski * and Kamil Kozdrój

Institute of Control & Computation Engineering, University of Zielona Gora, 65-516 Zielona Gora, Poland; g.bazydlo@issi.uz.zgora.pl (G.B.); k.kozdroj@issi.uz.zgora.pl (K.K.)
* Correspondence: r.wisniewski@issi.uz.zgora.pl; Tel.: +48-68-3282-248

Abstract: A novel, trusted, and secure durable medium electronic service is proposed in the paper. The proposed idea joins cryptographic methods (such as signing with an electronic seal and data encryption) with blockchain techniques. The e-service and blockchain databases were implemented on the TTP side, which made the presented concept trusted and secure. The proposed electronic service was oriented towards practical implementations, and it has commonly been developed together with a company from the cybersecurity field (which is considered a TTP in the proposed approach). The concept has been designed to meet the requirements of Polish law (i.e., the conditions and regulations related to the implementation of the durable medium in Poland); nevertheless, it can easily be adapted for other regions. The functionality of the presented e-service is illustrated by the example case study.

Keywords: e-service; durable medium; blockchain; trusted third party (TTP)

Citation: Bazydło, G.; Wiśniewski, R.; Kozdrój, K. Trusted and Secure Blockchain-Based Durable Medium Electronic Service. *Cryptography* **2022**, *6*, 10. https://doi.org/10.3390/cryptography6010010

Academic Editors: Josef Pieprzyk and Seyit A. Camtepe

Received: 30 December 2021
Accepted: 15 February 2022
Published: 21 February 2022

1. Introduction

The production and processing of documents is a hallmark of the modern world. From an ecological point of view, positive changes have be seen in the decreasing utilization of paper documents (in favor of electronic versions). More and more documents exist in only digital form and are stored in electronic circulation systems. Moreover, the COVID-19 pandemic has accelerated the transformation of documents from paper into digital forms. However, the generated documents often have to be accepted and returned by the customers (especially those in the financial sector). Therefore, a special electronic service (e-service) is needed to secure the document and to provide the customer's decision (i.e., feedback on the acceptance or rejection). Furthermore, such an e-service should prevent both modification of the document and tampering with the customer's decision. A so-called durable medium [1,2] is one of the approaches which is strictly focused on addressing these aspects. This technique meets the requirements and additionally fulfils the obligations for effectively informing customers about the issuing of new documents or changes to existing files (e.g., agreements, contract annex, regulations, price lists, etc.). In contrast, traditional solutions require the sending of thousands of letters with notifications about changes in documents, which is very expensive, as well as not being ecologically friendly. This leads to the conclusion that dedicated, trusted, and secured electronic services are essential nowadays.

This paper proposes a blockchain-based electronic service which is aimed at ensuring the secure storage and delivery of digital documents to customers. The security of the presented e-service is guaranteed using cryptographic methods and algorithms, whereas the application of a trusted third party (TTP) guarantees the document's immutability and transparency of its approval process (i.e., the opening, viewing, and acceptance or rejection of the document). The proposed approach has been developed for and directed toward the Polish market; therefore, it is strictly related to the requirements specified by Polish law and standards. The discussed topic is important and relevant in Poland,

which has additionally been confirmed by the decision which was issued by the Office of Competition and Consumer Protection in November 2018 on the penalizing of three Polish banks regarding the manner of changing the terms and conditions of their contracts with consumers [3].

2. Related Studies, Motivation, and Main Contributions

The section presents the current state of the art. Firstly, the most popular blockchain techniques are briefly described and compared. Next, the selected approaches that are related to the durable medium and electronic services are outlined. Finally, the most popular e-services based on the durable medium which are used in Poland are presented. The overview is summarized by the motivation and main contributions of this study.

Recent years have witnessed the growing popularity of blockchain technology. Such techniques, supported by tamper-proof solutions, have successfully been applied both in business and cryptocurrencies. The idea of a chain of connected blocks firstly appeared in 1991 [4], where such a database was applied to marking documents with timestamps. However, the real advancement in blockchain technology came with the advent of Bitcoin cryptocurrency in 2009 [5]. Over the last 12 years, this technology has been strongly developed; nowadays, there are many different versions and types of blockchains.

There are several blockchain-based solutions. One of them is the so-called Multi-Chain [6], which is an extended open-source Bitcoin solution. This technique offers a well-selected set of features for business users and can be used to build blockchains with both private and public access permissions. MultiChain supports the processing of a large number of data, and it is known for its speed of operation and ease of implementation.

Another interesting and very popular blockchain-based solution is Hyperledger Fabric (HLF) [7], developed by IBM. This technique enables the creation of applications with a modular architecture. HLF allows many components to run at the same time and supports membership services. Moreover, the proposed consensus solution is unique and enables high-scale performance while preserving privacy.

Quorum is an open-source blockchain protocol [8], with its methodology derived from Ethereum [9]. Quorum supports private blockchain networks with a single member owning all the nodes, as well as a consortium blockchain network, where multiple members each own a portion of the network.

Hyperledger Besu is another interesting open-source solution [10]. It is based on the Ethereum [9] client written in Java (under the Apache 2.0 license), implementing Enterprise Ethereum Alliance (EEA) specifications. Hyperledger Besu can be launched in both public and private Ethereum networks. The technique offers two consensus mechanisms: Proof of Work (PoW) and Proof of Authority (PoA).

The analyzed blockchain technologies are summarized in Table 1. Hyperledger Besu is supported by public and private permissioned networks, as well as by different types of consensuses (especially PoA). Therefore, this solution was finally selected for further development of the durable medium e-service presented in the paper.

Table 1. Comparison of the analyzed blockchain technologies.

Solution	Type of Blockchain	Type of Consensus
Multichain	Private, Permissioned	PBFT
Quorum	Private, Permissioned	Raft, QuorumChain, IBFT
Hyperledger Fabric	Private, Permissioned	Raft
Hyperledger Besu	Public, Private, Permissioned	PoW (Ethash), PoA (IBFT, QBFT, Clique)

Moving on to the techniques related to the durable medium and e-services, first, the method shown in [11] is outlined. The idea is based on a public blockchain that applies a proof-of-existence technique. Such a solution involves the registration and verification of documents through a distributed ledger. In particular, each operation is marked by a

timestamp signature. Any modification (or new information) is immediately visible to all the users of the system (blockchain platform). Therefore, the complete lifecycle of electronic documents can be audited and traced. The discussed architecture consists of eight layers that are used in order to build a so-called "enterprise blockchain platform". The realization of the presented idea is based on the IBM Blockchain platform and Hyperledger Fabric 2.0 [7]. The main advantage of the proposed solution is the application of the open-source blockchain framework, which is relatively popular and additionally supported by the proof-of-existence service. On the other hand, the publicly accessible database can be an easy target for cyber-attacks.

The application of the peer-to-peer technique based on symmetric cryptography is proposed in [12]. The method uses an Ethereum blockchain, where so-called "smart contracts" are created to secure the communication between the data provider and data consumer. In particular, the data provider registers the authorized users by means of the access control list. Such data are further validated by the consumers, which results in the accessing of the smart contract. The communication is performed within the Ethereum blockchain methodology. The main benefit of the proposed method relies on restricted and secured access to sensitive data, which are protected against unauthorized access. However, due to the maintenance of the technical resources, such a solution can be expensive in the long run.

The survey paper [13] is focused on an overview of the consensus methods in blockchain-based methods. In general, there are two aims of such a consensus. The first one is related to the order of transactions stored in the ledger, while the second technique is aimed at the prevention of doubles (that is, storing an identical transaction two times). The authors describe 69 different solutions split into four categories, including proof-of-work, proof-of-concept, proof-of-resources, and "permissionless" consensus. The analysis of this paper has shown that most of the existing (reviewed) methods do not meet the required conditions (assumed by the authors). Moreover, the paper concluded with the statement that there are no clear future directions for the analyzed consensus techniques.

Another survey paper [14] analyzes the current usage of electronic services and e-governance applications. In particular, the work focuses on the blockchain technique and studies its effectiveness in e-services. According to the authors, the role of electronic services has increased in several countries. Furthermore, the possible areas of the blockchain are discussed, including cryptocurrencies, data storage frameworks, cloud computing, and others. It is worth underlining that e-governance applications are not limited nor restricted to particular methods or techniques. Finally, a case study of the blockchain-based e-service is analyzed. In particular, electronic services used in Saudi Arabia were studied and compared to those used in the region's countries (United Arab Emirates, Bahrain, Kuwait, Oman, Qatar, Iran, Egypt, Jordan, Iraq). Such a wide analysis resulted in the conclusion about the logic of moving from traditional methods and services to electronic ones.

The decentralized group signature scheme (DGSS) is considered in [15]. The idea is based on blockchain technology, while the user identity privacy is secured by the discrete logarithm concept. As the authors state, existing group signature schemes are insufficiently secure from privacy leakage. The proposed idea consists of four algorithms (initiation, signing, verification, and implementation). The main benefit of the proposed algorithms relies on the polynomial computational complexity. Although the idea seems to be interesting and usable, the paper mostly focuses on the mathematical aspects.

The survey paper [16] focuses on the utilization of blockchain technology in the healthcare sector. The paper considers several possible medical applications, pointing out the main advantages of blockchain-based methods. In particular, neuroscience, pharmaceutical, biomedical, genomic, and clinical medicine is discussed, among others. For example, such technology is successfully implemented in the remote treatment and diagnosis of cancer tumours, where blockchain-based smart contacts are used. Another method described in the paper refers to teledermatology, where the blockchain is utilized for online consultation. Moreover, the idea of DNA data storage within the blockchain database is presented. The

work presents a broad overview of the possible applications and challenges of blockchain technology. However, this is a typical survey paper; thus, no new ideas are shown nor new techniques proposed.

Finally, let us briefly discuss the most popular e-services based on the durable medium that are used in Poland. From the general point of view, a stand-alone digital signature (itself) and the timestamp can be considered as the durable medium. However, such an idea does not meet the criteria of Polish standards and fulfils just a part of the e-service standard. Therefore, Polish banks (e.g., PKO Bank Polski, BNP Paribas Bank Polska) introduced methods offered and provided by the National Clearing House (in Polish: Krajowa Izba Rozliczeniowa, KIR). Such a technique utilizes a private blockchain network that is secured by a TTP, such as KIR [17].

There are various blockchain technologies involved, including cloud techniques and object matrices, such as Write Once, Read Many (WORM), Hyperledger Fabric [7,18], etc. Furthermore, combined methods that integrate a blockchain with the durable medium are available. Paper [19] describes the so-called "S3DOC Witness" technique, which offers electronic signing of documents. This method applies the TTP idea without transferring personal data. The method proposed in [20] is based on splitting the data between the blockchain nodes; thus, the complete documents are stored within the database. It is worth mentioning that such a solution is used by various Polish companies, such as Tauron or Syneriz, as well as scientific institutions (e.g., Polish Section of the IEEE, Kielce University of Technology). Furthermore, the idea of the blockchain-based e-service is described in [21]. The presented technique is supported by the European Union, and it applies the durable medium. The idea is based on the blockchain implementation in [21], which is supported by the European Union. Finally, the WORM matrices are utilized by the technique shown in [22]. The proposed idea involves a TTP, while the sensitive data are handled and stored by WORM.

To summarize the above discussion, it can be noticed that blockchain-based techniques are very popular in the various fields of cybersecurity, including electronic services. On the other hand, the proposed ideas are usually strictly restricted to the specific application or rules and standards of the particular country. This paper introduces a new idea of the trusted and secure durable medium e-service. The proposed technique is supported by cryptographic methods combined with blockchain technology. Let us underline that the presented approach is strictly oriented toward the needs, requirements, and assumptions indicated by the Regulation of the European Parliament and the Council (EU) No 910/2014 (23 July 2014) on "Electronic Identification and Trust Services (eIDAS) for Electronic Transactions in the Internal Market (. . .)" [23].

The main contributions proposed in the paper can be summarized as follows:

- A novel, original, and durable medium e-service is proposed. The e-service is described by the business process model and notation (BPMN) [24] diagram.
- The proposed approach utilizes cryptographic methods combined with blockchain technology.
- Both the e-service and blockchain database are implemented on the TTP side, which makes it trusted and secure.
- The e-service is strictly designed according to the requirements of Polish law, especially in order to meet conditions and regulations related to the implementation of the durable medium in Poland.
- The proposed approach is mainly oriented toward banks or larger companies. However, it can also be applied in other industrial areas where there is a need for agreement on documents with large numbers of customers.
- The proposed technique is oriented toward practical implementation; thus, it is supported and developed in cooperation with the "Perceptus Sp. z o.o." company [25].

The rest of the paper is organized as follows. Section 3 presents the proposed approach, where both the trusted and secure e-service and the blockchain structure are described in detail. The introduced e-service is presented in the form of a BPMN diagram. The

exemplary blockchain generation process is described in the case study section (Section 4). The limitation and scope of the proposed solution are presented in Section 5. Finally, the last section is devoted to the final remarks and conclusions.

3. The Proposed Secure Blockchain-Based Durable Medium e-Service

A novel idea of a trusted and secure blockchain-based durable medium electronic service is proposed in the paper. The solution is trusted thanks to the qualified eSign service provided by TTP (namely by the "Perceptus Sp. z o.o." company [25]). Furthermore, it is also secure due to the applied blockchain technique (supported by symmetric and asymmetric cryptography), together with the electronic signature of the documents (with the use of an eSign seal). Finally, in order to increase the security of the proposed method, the keys used for encryption/decryption are stored in a hardware security module (HSM) on the TTP side. Let us underline that the choice of blockchain was also not accidental. The popularity of this technology (as well as its application) has been growing significantly in recent years. Currently, a blockchain is one of the best solutions to store key data in safe structures that cannot be interfered with or changed. Therefore, it is successfully used in cryptocurrencies and other business applications [15]. Let us now describe the proposed idea in more detail.

3.1. Trusted and Secure e-Service

The scheme of the proposed e-service is presented in Figure 1 in the form of a business process model and notation (BPMN) diagram [24]. In general, there are three business actors in the diagram that exchange trusted and secured data: the bank, customer, and trusted third party (denoted as TTP or eSign). The legend placed in the diagram presents the meaning of the most important elements used in the process (more detailed explanations can be found in the BPMN standard [24]).

The realization (procedure) of the e-service starts on the bank side (the business actor "Bank" is represented as a pool on the BPMN diagram), denoted by the start event "Start of the whole process". It is assumed that the Bank intends the procedure (for example, the agreement of a new version of an existing or new document, such as regulation, agreement, pricelist, etc.) with the customer (or with a group of the customers; however, to clarify the presentation, we will follow a single user). Moreover, it is assumed that the Bank possesses the customer's data (e.g., personal data, such a name, residential address, telephone number, e-mail) and these data have been transferred to the bank offline or through other procedures strictly related to the Bank). Note that the Bank is responsible for the customer's data management, and this issue is beyond the scope of the proposed approach.

Subsequently, the Bank selects a client (or clients) and selects a document (e.g., a personalized agreement, contract annex, etc.) to be approved by the customer. This document, together with the customer identity (denoted as CID) are sent to the TTP (eSign). Let us underline that except for those data (that is, the particular document and CID), no other information (including personal data) is transferred.

Once the data are received by the eSign system (top of the diagram), the document is signed with an electronic eSign seal. Moreover, an adequate identity for the document is generated (denoted as DID). Moreover, a symmetric key for the document is also generated. This key is used for encryption of the document and stored securely in the HSM. Additionally, two complementary asymmetric keys (private and public) are generated as well (for each customer separately) and stored in the HSM. These keys will be used in future stages of the e-service. Finally, the signed and encrypted document, as well as the CID and DID, are added to the blockchain database. In particular, a new node of the database is generated and added to the structure (the proposed blockchain is described in Section 3.2 in detail). In the next step, a special link to the document is generated (actually, the link points to the particular block in the blockchain). This link, together with the public key (for the customer), is sent back to the Bank.

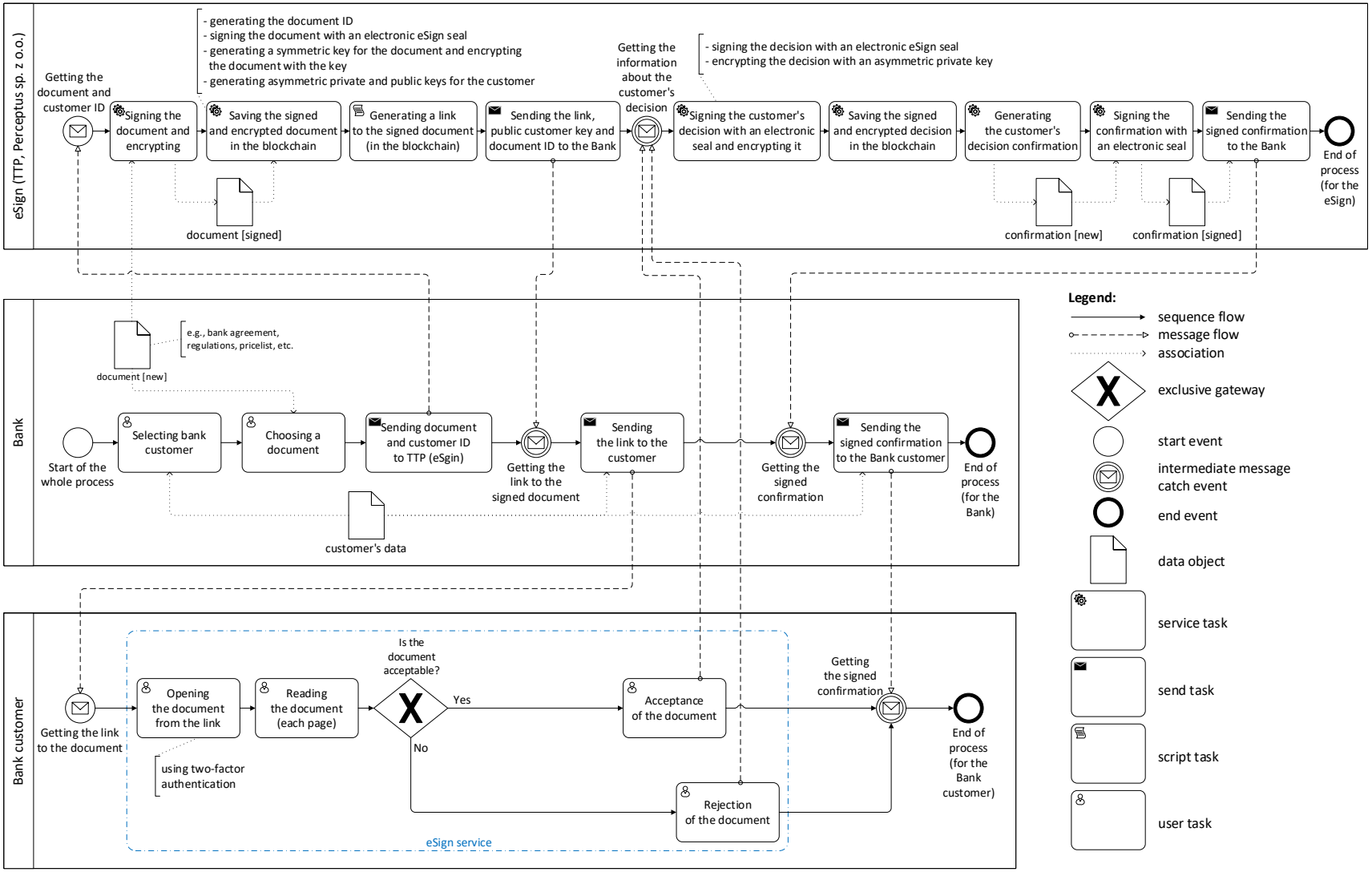

Figure 1. The proposed e-service in the form of a BPMN diagram.

In the subsequent step, the Bank sends an e-mail to the customer with the link to the signed and encrypted document. The customer opens the document using the received link. It is worth noting that the opening of the document could be additionally protected by two-factor authentication (2FA). In practice, the Bank sends a special verification code (with time-limited validity) to the customer using a short message service (SMS) or a special authorization application. In this step, a special eSign service is used that decrypts the documents online and allows the customer to read them (the information about the opening of each page of the document is also stored). The decryption process applies the symmetric key (the keys are stored with the related DIDs in HSM on the TTP side), and the encrypted document is taken from the given blockchain node (located by the CID and DID). Finally, the customer can freely read the document and decide whether to accept or reject it. The customer's decision is then signed with the eSign electronic seal and encrypted using the private key (stored with the CID in the HSM). The signed and encrypted decision is stored in a blockchain as a new block. This node also holds the CID and CID values, enabling the future verification of the approval process (by the customer or Bank side). Let us underline that the customer decision is stored directly by eSign, bypassing the Bank, in order to reduce the possibility of manipulation of the customer's decision.

Finally, eSign generates the confirmation of the customer's decision, signs it with an electronic seal, and sends it back to the Bank. The confirmation is forwarded by the Bank to the customer, which ends the described process. Let us emphasize that both sides (the Bank and the customer) can verify the data stored in the blockchain (e.g., the processed document, the decision made) using additional procedures (not described in this paper). Moreover, the presented e-service is focused strictly on durable-medium-related aspects. Therefore, it is assumed that any errors or mistakes are resolved directly between the customer and the Bank.

In order to increase the readability, the presented diagram presents the whole process only for a single customer (with a related document). Of course, the approach could be automated to facilitate the process with hundreds of thousands of bank customers (especially in the case of the stages related to the selection of customers and documents, generation of links, signing and encryption of documents, etc.). Moreover, the proposed approach can be applied not only by banks or financial institutions but also by other companies, which requires the processing of documents in a secure and trusted way.

3.2. Blockchain Structure

The proposed blockchain structure is presented in Figure 2. The network contains two types of blocks, which were designed directly for the implementation of the e-service. The first type of block ("document") is dedicated to storing the information about the processed document, while the second type of block ("decision") stores the customer's decision data. These two types of blocks can be freely connected with each other. It should be noted that the proposed approach is not limited to these two types of blocks only and can be freely extended to any number of block types.

In the proposed approach, the private version of the blockchain is used. It means that access to the data stored in the blockchain is possible only with the appropriate access permissions. Moreover, only one network is generated. Such a structure was selected due to security reasons. Data stored in one blockchain impedes the possibility of blockchain manipulation by the Bank; thus, it is safer than generating separate blockchains for each customer.

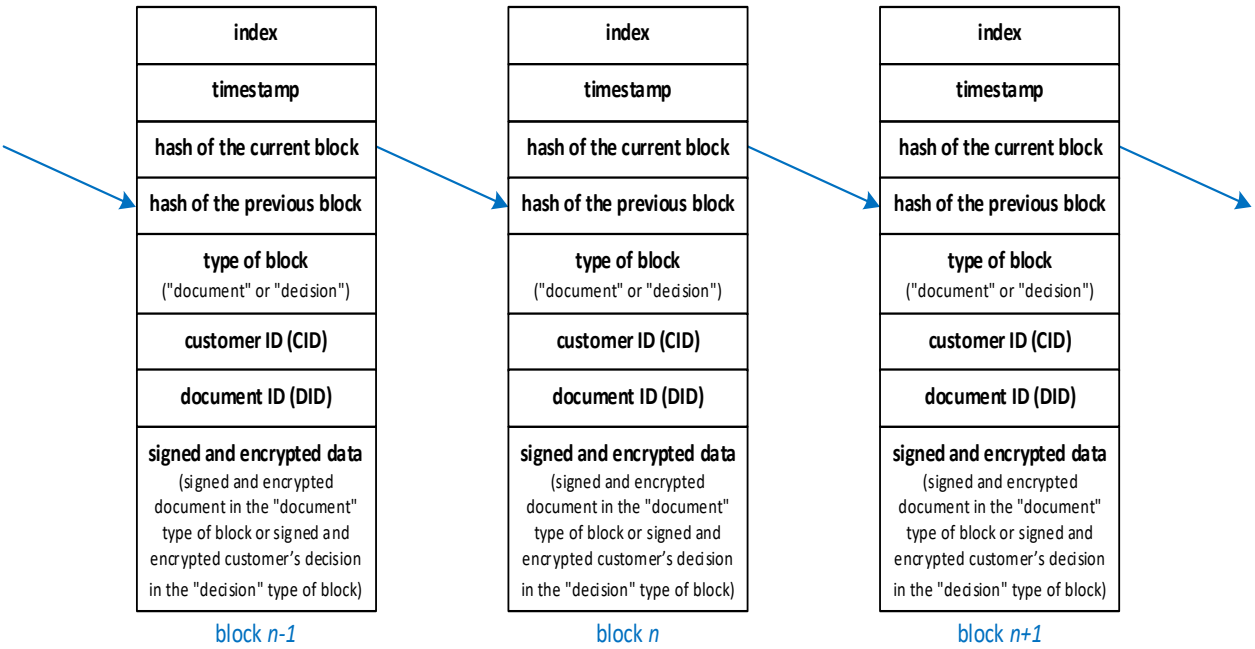

Figure 2. The proposed blockchain structure.

In the presented solution, data related to the particular document are stored twice in the blockchain: firstly, when the eSign prepares the link to the document (the CID, DID, and the encrypted document are stored in a "document" block type) for the customer and secondly, after the customer decides (the CID, DID, and the encrypted decision are stored in a "decision" block type). It is worth noting that the safety-critical data (e.g., the processed document or the customer's decision) are encrypted; thus, other customers do not have access to the decrypted data. The document (stored in the "document" type of block) is encrypted with the private symmetric key (stored with the related DID in the safe HSM on the TTP side), while the customer's decision (stored in the "decision" type of block) is encrypted with the use of a private asymmetric key (stored with the public key and the related CID in the safe HSM on the TTP side). Furthermore, the public key is also sent to the Bank. Therefore, verification of the customer's decision, which is stored in a blockchain, is possible also for the Bank side.

Let us underline that generation of the documents for clients (and storing them in the blockchain as "document" blocks) can be iterative and therefore predictable (contrary to the generation of the "decision" blocks because particular customers can access documents and make decisions at a random time). Moreover, the number of bank customers (even counted in millions) has an influence on the number of blocks in the blockchain. Such a (large) number significantly impedes the possibility of blockchain manipulation. Finally, the blockchain is managed by the TTP, and instead of using the Proof of Work (PoW) mechanism, the more effective Proof of Authority (PoA) is used. Thanks to this solution, the blockchain network does not require computing power to create new nodes.

4. Case Study Example of the Blockchain Generation Process

This section presents the proposed blockchain generation process by a simple case study example. Assume that the Bank introduces a new document (e.g., a contract annex), and requires a decision of acceptance or rejection of the document from one million individual customers. Initially, the Bank prepares one million personalized documents (for each separate client). Next, all documents are sent using the proposed e-service to the eSign (on the TTP side). Note that each document has assigned the customer identity (CID). In response, for each document, the eSign signs it using an electronic seal and generates its identity (DID). From this moment, the authenticity and integrity of the document (stored in the blockchain) can be verified with the eSign public key. Furthermore, for each document,

a random symmetric key is generated by the eSign. This key (together with adequate DID) is stored in the HSM on the TTP side. Note that if the Bank requires processing the same document for all customers (e.g., a new pricelist), only one symmetric key is generated.

In the subsequent step, the signed documents are encrypted with the generated keys (that is, each document is encrypted separately, with its key) and stored in the blockchain (together with the related DID and CID), as shown in Figure 3. This means that one million new "document" blocks are created in the blockchain database. Moreover, for each customer (actually for each CID), the complementary pair of public and private asymmetric keys are generated and stored (with the related CID) in HSM.

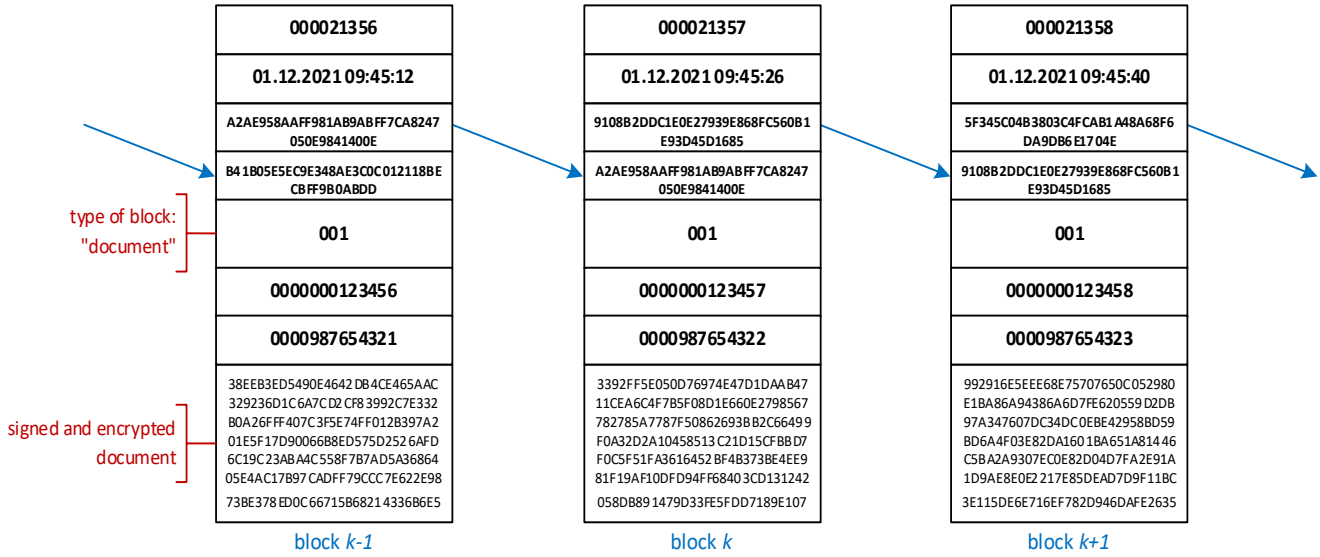

Figure 3. The part of an exemplary blockchain structure with the "document" blocks.

For each document stored in the blockchain, a special link is generated and sent back to the Bank, together with the DID, CID, and related customer's public key. In the next step, adequate links (hyperlinks) are distributed by the Bank to the particular customers. Each of the customers is able to open the document (with the use of the eSign service), read it, and decide whether to accept or reject the document. The decision is signed with the electronic seal from eSign and then encrypted with the customer's private key (stored in the HSM on the TTP side). Finally, the new "decision" block is generated and added to the blockchain (Figure 4). Note that Figure 4 presents the hypothetical situation in which the bank customer with CID 0000000123457 made the decision about the document with DID 0000987654322 (block $m - 1$ from Figure 4) earlier than the customer with CID 0000000123456 (block $m + 1$ from Figure 4), who obtains the link later.

After processing of all the documents by the customers, one million new "decisions" are generated, which results in one million new blocks in the blockchain. Note that they are inserted in a random way (there is no influence on the order in which customers make decisions). Summing up, during the whole process, two million new blocks are generated and added to the blockchain. Therefore, any attempt to manipulate such a large structure of connected blocks is very difficult, especially because the blockchain is stored and managed by the TTP, not by the Bank or customers.

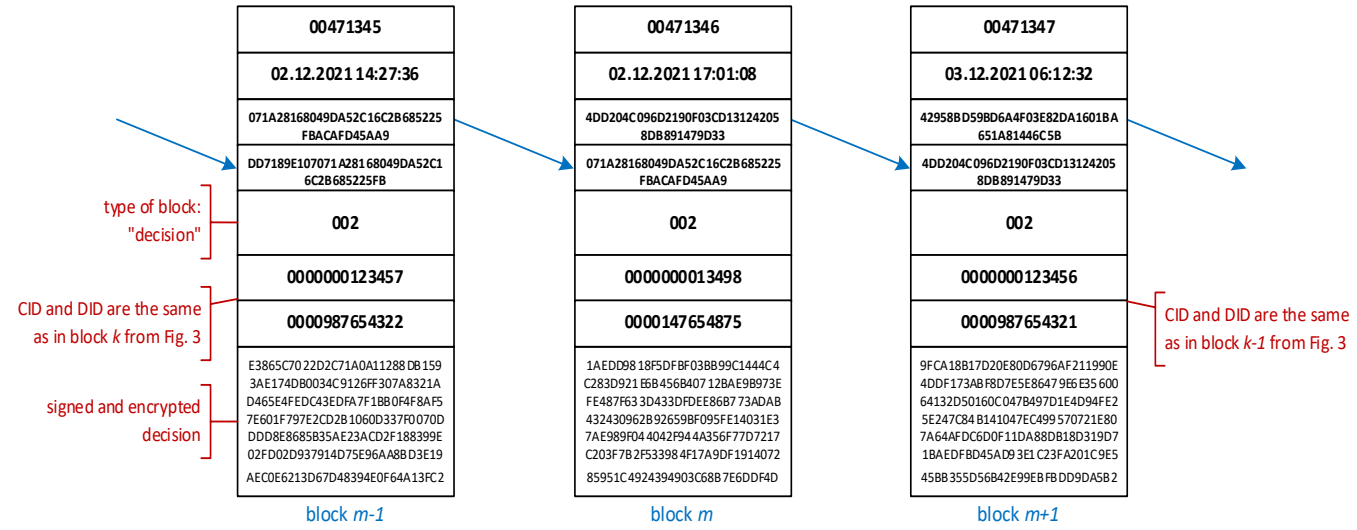

Figure 4. The part of an exemplary blockchain structure with the "decision" blocks.

5. Limitations and Scope

The proposed e-service was designed for companies or organizations (especially financial institutions) which have large numbers of customers. The advantage of the presented solution lies in the large number of blockchain nodes. In small companies, the number of blocks would be rather small, which increases the probability of blockchain tampering. Moreover, using asymmetric cryptography to encrypt the decision of the customer, which is stored in the blockchain, requires the use of computing power (the asymmetric algorithms are slower and less efficient than the symmetric ones). The optimization of generating and using the public and private keys is the subject of further research by the authors. Furthermore, the proposed solution was strictly designed for the Polish law regulations, which does not mean that it cannot be used in other countries or applications.

The proposed e-service was compared to the other, similar durable medium approaches. The comparison was made in terms of features such as the type of durable medium (WORM, blockchain, or just a digital signature), blockchain type (public, private, or hybrid), the use of a trusted third party, or other, unique features. Table 2 presents the results of the comparison. It can be noticed that most of the existing e-services apply blockchain technology (especially in a private version) as a durable medium type. This confirms the enormous potential and popularity of blockchain-based solutions.

Table 2. A comparison of the proposed e-service with other similar durable medium approaches.

Feature	S3DOC [19]	Atende [22]	KIR [18]	Autenti [21]	DoxyChain [26]	Billon [20]	Proposed e-Service
durable medium type	WORM, digital signature, blockchain	WORM, blockchain	WORM, blockchain	digital signature	digital signature, blockchain	digital signature, blockchain	digital signature, blockchain
blockchain type	private	private	private	–	hybrid	private	private
trusted third party (TTP)	for one node [1]	Yes [2]	no	for signing only	trusted entities [3]	for signing only	yes
unique features	distributed hash table	hash of document	Proof of Existence	–	Proof of Authority	Proof of Stake	Proof of Authority

[1] dedicated trusted "witness" node managed by the TTP. [2] one of the TTP nodes is managed by NASK (a Polish research and development organization and data networks operator). [3] instead of one trusted node, there are trusted entities that co-create the system.

Another interesting conclusion is that a trusted third party (TTP) is very often limited only to the digital signing of the processing data. Let us stress that the solution presented in this paper utilizes the role of TTP much more by shifting the responsibility of the entire process more towards the trusted third party. Furthermore, the analyzed solutions differ regarding the blockchain consensus mechanism. The proposed e-service (similarly to

the DoxyChain solution) applies Proof of Authority since it is one of the most effective approaches and does not require computing power to create new nodes. Concluding, the proposed e-service can be an interesting alternative for existing durable medium solutions.

6. Conclusions

In the paper, a trusted (because of using the TTP side) and secure (thanks to using the signing and encryption techniques) durable medium e-service is proposed. The core of the presented approach is the blockchain database, where critical data are stored, signed (with an electronic eSign seal), and additionally encrypted (using symmetric or asymmetric cryptography). Such a compilation of modern blockchain technology (managed by the TTP) and cryptographic methods prevents tampering with the blockchain database, which is the main concern of customers and one of the biggest disadvantages of currently used solutions.

The proposed e-service was designed especially for large financial institutions (e.g., banks), but it can also be applied within other companies or organizations where there is a need to process documents with a large number of customers. It is worth mentioning that the larger the number of customers, the larger the number of nodes in the blockchain, and the more difficult tampering with the blockchain structure would be. Let us underline that the presented technique is oriented toward practical implementation, and it is supported (and developed) together with the "Perceptus Sp. z o.o." company (which is considered as a TTP in the proposed approach).

Future research of the authors is focused on experimental realization and practical verification of the proposed idea. Moreover, the physical implementation (once the experiments are finished) of the presented e-sign is planned.

Author Contributions: Conceptualization, G.B., R.W. and K.K.; methodology, G.B. and R.W.; state-of-the-art review, K.K. and R.W.; investigation, K.K. and G.B.; writing—original draft preparation, G.B.; writing—review and editing, R.W.; supervision, G.B. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Ministry of Education and Science, Poland, "Industrial doctorate", under the grant number DWD/4/90/2020.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Financial Conduct Authority—FCA. Durable Medium. Available online: https://www.fca.org.uk/firms/durable-medium (accessed on 20 December 2021).
2. Law Insider. Durable Medium Definition. Available online: https://www.lawinsider.com/dictionary/durable-medium (accessed on 20 December 2021).
3. Office of Competition and Consumer Protection (UOKIK). Durable Medium-Decisions Regarding ING, Getin Noble, PKO BP. Available online: https://www.uokik.gov.pl/news.php?news_id=14910 (accessed on 20 December 2021).
4. Haber, S.; Stornetta, W.S. How to Time-Stamp a Digital Document. *J. Cryptol.* **1991**, *3*, 99–111. [CrossRef]
5. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 20 December 2021).
6. Content Blockchain Multichain. Available online: https://content-blockchain.org/research/multichain/ (accessed on 20 December 2021).
7. Hyperledger Fabric. Available online: https://www.hyperledger.org/use/fabric (accessed on 20 December 2021).
8. Quorum. Available online: https://consensys.net/quorum/qbs/ (accessed on 20 December 2021).
9. Ethereum. Available online: https://ethereum.org/en/ (accessed on 20 December 2021).
10. Hyperledger Besu. Available online: https://besu.hyperledger.org/en/stable/ (accessed on 20 December 2021).
11. Kaczmarczyk, A.; Sitarska-Buba, M. Enterprise Architecture of the Blockchain Platform. *J. Internet e-Bus. Stud.* **2020**, *2020*, 1–12. [CrossRef]
12. Ziar, R.A.; Irfanullah, S.; Khan, W.U.; Salam, A. Privacy preservation for on-chain data in the permissionless blockchain using symmetric key encryption and smart contract. *Mehran Univ. Res. J. Eng. Technol.* **2021**, *40*, 305–313. [CrossRef]
13. Nijsse, J.; Litchfield, A. A Taxonomy of Blockchain Consensus Methods. *Cryptography* **2020**, *4*, 32. [CrossRef]
14. AlMendah, O.M.; AlZain, M.A.; Masud, M.; Jhanjhi, N.Z.; Al-Amri, J.; Baz, M. A Survey of Blockchain and E-governance applications: Security and Privacy issues. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 3117–3125.

15. Devidas, S.; Subba, R.Y.V.; Rekha, N.R. A decentralized group signature scheme for privacy protection in a blockchain. *Int. J. Appl. Math. Comput. Sci.* **2021**, *31*, 353–364. [CrossRef]
16. Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. *Cryptography* **2019**, *3*, 3. [CrossRef]
17. National Clearing House KIR. Durable Medium. Available online: https://www.kir.pl/en/clients/durable-medium (accessed on 20 December 2021).
18. Hitachi in Europe. KIR Durable Medium. Available online: https://www.hitachi.eu/en/kir-durable-medium (accessed on 20 December 2021).
19. S3DOC. Witness is a Secure Durable Medium. Available online: https://s3doc.com/s3doc-witness-bezpieczny-trwaly-nosnik/ (accessed on 20 December 2021). (In Polish).
20. Billon. Trusted Document Management. Available online: https://billongroup.com/en/trusted-document-management (accessed on 20 December 2021).
21. Autenti. Available online: https://autenti.com/en/ (accessed on 20 December 2021).
22. Atende. Digitization of Private Documents. Available online: https://atende.pl/en/product-offer/blockchain/atende-chaindoc (accessed on 20 December 2021).
23. Electronic Identification and Trust Services Regulation (eIDAS, 910/2014/EC). Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910 (accessed on 20 December 2021).
24. OMG. Business Process Model and Notation (BPMN). Available online: https://www.omg.org/spec/BPMN/2.0/PDF (accessed on 18 January 2022).
25. Perceptus Sp. z o.o. Available online: https://perceptus.pl/ (accessed on 20 December 2021).
26. DoxyChain. Available online: https://www.doxychain.com/ (accessed on 18 January 2022).