applied sciences

MDPI

Article

Trusted Third Party Application in Durable Medium e-Service

Grzegorz Bazydło [1,*], Kamil Kozdrój [2], Remigiusz Wiśniewski [1] and Aniruddha Bhattacharjya [3,†]

[1] Institute of Control & Computation Engineering, Division of Information Systems and Cybersecurity, University of Zielona Góra, 65-417 Zielona Góra, Poland; r.wisniewski@issi.uz.zgora.pl
[2] Perceptus Sp. z o. o., 66-002 Zielona Góra, Poland; k.kozdroj@perceptus.pl
[3] BCBRBAB Intercontinental Trading Solutions Private Limited, Kolkata 700084, India; li-an15@tsinghua.org.cn
* Correspondence: g.bazydlo@issi.uz.zgora.pl
† PhD Alumni, Department of Electronic Engineering, Tsinghua University, Beijing 100190, China.

Abstract: The paper presents a novel concept of applying a trusted third party (TTP) to the blockchain-based electronic service (e-service) in the form of a durable medium. The main aim of the proposed e-service is storing, managing, and processing sensitive electronic documents. The developed e-service meets the requirements of both Polish law (related to the durable medium) and market needs. Firstly, the functional requirements were defined. Subsequently, the adequate e-service was designed, and then implemented in a real company in Poland. Due to the nature of the durable medium e-service, the presented research combines scientific and implementation aspects. The designed and implemented e-service is secure (because of using the immutable blockchain technology merged with symmetric and asymmetric cryptographic algorithms) and trusted (by using TTP as the e-service provider, as well as an independent arbitrator monitoring the document storage and processing flow). Finally, the presented approach was experimentally verified using Hyperledger Besu—a blockchain implementation platform. During the realization of two designed test scenarios, over 30,000 transactions were added to the blockchain. Furthermore, security analyses were performed regarding inherent blockchain properties, the use of cryptographic algorithms, and potential cyberattacks and vulnerabilities.

Keywords: trusted third party (TTP); blockchain; e-service; durable medium; secure hash algorithms (SHA); interplanetary file system (IPFS); Rivest–Shamir–Adleman algorithm (RSA)

Citation: Bazydło, G.; Kozdrój, K.; Wiśniewski, R.; Bhattacharjya, A. Trusted Third Party Application in Durable Medium e-Service. *Appl. Sci.* **2024**, *14*, 191. https://doi.org/10.3390/app14010191

Academic Editor: Juan-Carlos Cano

Received: 30 October 2023
Revised: 10 December 2023
Accepted: 12 December 2023
Published: 25 December 2023

1. Introduction

Electronic documents are widely used in many areas, including business transactions, where contracts between various companies often go beyond national borders, and cooperations are concluded around the world. Electronic documents are convenient because they can be easily and cheaply stored, sent, and shared with other people and companies. In addition, there are many tools for their editing and processing. Therefore, paper documents are slowly being replaced by electronic data, and more and more business transactions are carried out using only electronic documents, which greatly facilitates conducting economic activity.

Many of the processed documents, especially official ones or business documents, often contain information that should be protected, and their publication may be harmful to enterprises or citizens (e.g., by disclosing their data), and even violate their personal and property rights. Users have many concerns about the security of their digital transactions. One of the greatest threats is cybercrime [1]. These may include activities such as computer hacking, theft of personal data, internet fraud, attacks on IT systems, etc. Another threat is the risk of losing access to electronic documents, for example as a result of computer failure, malware infections, or damage to the data medium. Users may also be concerned about the security of personal data that may be misused by third parties. That is why it is important to use secure and trusted tools to protect electronic documents from all these threats.

Moreover, there are also situations when the documents (or more broadly: data) should neither be made public nor changed (modified). This is the so-called non-repudiation problem [2], and covers situations when large corporations (e.g., banks, telecommunications companies, etc.) publish documents (e.g., on their websites or internal systems), but then make unauthorized changes to these documents. In such a situation, the user has no control over these changes (and often they are not even aware of them) and—as an individual—cannot prove irregularities in court. The crux of this problem is to assure all parties of the document that the data recorded in the electronic document will not be changed by any of the parties without the knowledge and consent of the others. This is especially important for documents that are used in business transactions.

Cryptography methods and blockchain technology can be used to face this problem. In the case of applying cryptography, this mainly involves encrypting the document (using symmetric or asymmetric cryptography). On the one hand, the point is to make the encrypted data unreadable for third parties (without the secure key, the data cannot be decrypted), so even if they are shared or leaked, the risk of their disclosure is very small. On the other hand, by using the hash function, a hash of the document can be generated and shared to all parties. Thanks to that, if a document is changed by one of the parties, the other parties will be able to easily detect it, because the hash of the changed document will not match the original hash.

Blockchain is a technology that allows the creation of distributed and immutable records of data. It consists of a network of interconnected nodes (e.g., computers) that store copies of data stored in the blockchain. Each new entry in the registry (so-called block) is confirmed by most network nodes, which ensures that the data are safe and unalterable. Blockchain can be used to solve the non-repudiation problem because it ensures that the data contained in the register are immutable. Thanks to this, even if one of the parties would like to change the data in the electronic document, it will be impossible because this change will be detected by other network nodes and immediately rejected. Therefore, using cryptography and blockchain can ensure that the data contained in the electronic document remain unchanged and indisputable.

In response to the above-mentioned problems, several solutions for data protection have been developed. At this point, however, we would like to draw attention to the legal solutions existing in Poland. They are created to protect the rights of the client and impose the need to store documents regarding the client (e.g., contracts, regulations of services provided, etc.) on the so-called durable medium. This solution indicates that electronic documents should be stored in infrastructure independent of any of the parties, and the process of sharing these documents with all parties and their storage should be monitored. Therefore, there is a need to use a so-called trusted third party (TTP) that can provide infrastructure for storing and processing electronic documents, as well as act as an arbiter of processing operations of these documents.

In summary, there is a need for secure and trusted services for the storage and processing of electronic documents. It is very important to store data securely, in order to protect personal data and other confidential information from unauthorized access. Additionally, trusted storage of electronic documents ensures their integrity and immutability, which is important in business transactions. Safe storage of electronic documents also helps to protect them against loss, for example as a result of a computer failure or damage to the data medium. In addition, some legal regulations (e.g., in Poland) force companies (especially banks) to store and process documents using a TTP. Therefore, secure and trusted electronic document storage services are very important in today's world. This is reflected in the market demand for e-services for the safe and trusted transmission, processing, storage, and sharing of electronic documents, especially those that meet the requirements of a durable medium. The use of cryptographic methods and a trusted third party allows for the development of a secure and trusted e-service of a durable medium proposed in the paper.

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

- A novel, secure, and trusted e-service as a durable medium is proposed;
- The presented approach is secure because it utilizes cryptography combined with blockchain technology, and is trusted thanks to the use of trusted third party infrastructure and an immutable database;
- The proposed e-service is designed to meet the requirements of Polish law, related to the durable medium;
- The key feature of the presented approach is a unique combination of decentralized blockchain with the TTP, which increases the security and reliability of electronic document storing and management;
- The presented solution is oriented toward big financial institutions or telecommunications companies that provide services to thousands of users (however, it can be applied in other industrial areas where there is a need for processing electronic documents with large numbers of customers);
- The case-study example was designed and experimentally verified by the implementation of the blockchain using the Hyperledger Besu platform;
- The proposed e-service was developed based on real market needs and was implemented in the company's real environment;
- The presented solution is focused on practical implementation and therefore is supported and developed in cooperation with the "Perceptus Sp. z o. o." [3]–IT company from Poland.

The research methodology presented in the paper is based on theoretical foundations and scientific analyses, as well as on practical experience regarding e-service implementation. The main context of the research was derived from market and industry needs. In 2018, the Polish Office of Competition and Consumer Protection (OCCP, UOKIK in Polish) inspected banks in terms of the method of transmitting information on changes to contracts on a durable medium [4]. The results of this audit showed that in the years 2015–2018, banks provided information about changes in documents (e.g., increases in customer costs) only in their electronic banking systems, which did not meet the requirements of a durable medium (regarding Polish law). Documents made available through the bank's system could be freely changed, replaced, or even permanently deleted. Additionally, there was no certainty that the bank's customers even knew that they had such information in the system. If the customer rarely logged in to the banking system, they sometimes could not even react to changes in a particular document (e.g., contract, price list). After the above-mentioned inspections, the Office of Competition and Consumer Protection imposed various penalties on banks—e.g., obligations to refund any overpayments and exemptions from selected fees for customers who were incorrectly informed about changes in documents under the law. In that situation, banks started looking for other solutions to meet the requirements of the law regarding a durable medium. So, the market need to design new, trusted, and secure electronic services was the main motivation for starting this research. Then, the in-depth market, law regulations, and literature analysis were made to indicate existing approaches, solutions, and products. It is worth emphasizing that from the very beginning, the main goal of the research was to develop a service that would be practically implemented in a real company. Therefore, based on the state-of-the-art analysis, as well as on the technical capabilities of the company, functional requirements were developed. Then the e-service was modeled, designed, practically verified, and finally implemented in a real company in Poland. Thus, the presented research combines both scientific and implementation aspects.

The rest of the paper is organized as follows: Section 2 describes the related works regarding applying trusted third parties in electronic documents e-services. Section 3 presents the proposed approach, where the e-service assumptions (including graphical representation) as well as the blockchain structure and security analysis are described in detail. The exemplary blockchain generation process is described in the case study section (Section 4). Finally, Section 5 is devoted to the conclusions.

2. Related Works

The main aim of this section is to present selected solutions using TTP (very often combined with blockchain technology). In the beginning, it is worth explaining what a trusted third party is. TTP is an institution or organization that acts as a trusted intermediary in the process of exchanging data or information between (two or more) parties. TTP can be used in various solutions, for example, to ensure the security of financial transactions, to authenticate users' identities, or to ensure the immutability and integrity of data.

Many solutions use TTP, which differs in terms of the scale of operation, method of implementation, and competencies. The most important TTP solutions include:

- Financial institutions, such as banks or insurance companies, which act as trusted intermediaries in the process of exchanging data and information related to financial transactions;
- Certification systems such as Public Key Infrastructure (PKI), which verify the identity of users and ensure the security of transmitted data;
- Electronic document management platforms that allow the storing, processing, and exchanging of electronic documents securely.

It is worth noting that when a service is provided involving conflicting parties, consensus can be achieved by including TTP in digital transactions. On the other hand, if the problem concerns the need to trust one selected party (here TTP), the blockchain network can decentralize trust (trust is spread over many nodes). However, the problem resulting from the use of blockchain technology is that there is no native mechanism to securely manage the identity of the actors involved [5]. In our deliberations, a blockchain is considered a section of middleware that comprises built-in services. Such services are used for the expansion of distributed applications deprived of the participation of a component (like, an authentication or a database server) performing as a central control. The outstanding facilities given by a blockchain include ineffaceable append-only storage, public key-based access control for the carrying out of operations, unrestricted auditability of records, and remarkably, consensus services of a few disciplines.

Many varieties of applications are being created based on blockchain; smart contracts are the most identified. During the implementation stage, a blockchain can be well-defined as a distributed data structure (also called the ledger) comprised of an ordered, back-linked list (chain) of blocks. Particular blocks are added to the list based on an append-only model, and only when several nodes holding local copies of the present state of the blockchain attain consensus about its afterward global state. Furthermore, blocks are customarily used for storing records of transactions completed by parties that may not trust each other and reinforce the peer-to-peer (P2P) execution prototype of the transactions. The transactions are actions intended to shift the current state of the blockchain and are not inevitably bank transactions. Smart contracts can be set up on TTP. In particular, a TTP is considered an institution that—along with having the technical structure for accommodating smart contracts—has received trust, reputation, and authority. Time-stamping services, certification authorities, payment gateways, settlement services, custodian services, and various brokerage services are examples of e-commerce applications that customarily use TTP services. For smart contract applications, a TTP is logically positioned in the middle of the two business associates, and it is trusted for hosting and running a single instance of the smart contract. A smart contract witnesses all the actions that associates perform, and retains undisputable records about them. In our assumptions, a TTP–based structure is trustworthy, preventing the modification of smart contracts and securing sensitive data that the corresponding contractual parties uncover. This problem can be resolved with the support of newly evolving trusted hardware technologies like Intel SGX [6] and ARM TrustZone [7], where the contract code might be deployed in trusted environments (so-called trusted world in TrustZone and enclaves in SGX). The trusted hardware stops the TTP from modifying the integrity of the contract program and prevents the investigation of sensitive data. Some solutions apply the TTP in the digital data models of data security. In such techniques, the TTP is responsible for data authentication, confidentiality, and data integrity. For this purpose, one-time passwords (OTP) are used to provide authentication.

In addition, data confidentiality is ensured by the cryptography algorithms used for data encryption and decryption, and data integrity is ensured using data hashes [8].

Another interesting application of a semi-trusted third party is presented in [9], where authors introduce a buyer-seller watermarking protocol that can be very useful for copy deterrence and privacy preservation in the cloud environment. The proposed solution combines services of cloud infrastructure as a service (IaaS), a cloud service provider (CSP) considered as a semi-trusted third party, a privacy homomorphism cryptosystem with Diffie–Hellman key exchange algorithm, and robust and fair watermarking techniques. The proposed approach addresses the problems of piracy tracing, anonymity, tamper resistance, or customer rights problems. The cloud plays a crucial role because it reduces communication overhead and supports the watermarking process.

In [10], the authors propose a TTP scheme based on signcryption using the session key exchange protocol (symmetric cryptography is used here). Thus, the session key exchange protocol prevents eavesdropping during cyberattacks such as denial of service (DoS) or man-in-the-middle (MITM) attacks. Because the encryption process is performed by the cloud service user (CSU), and the decryption is made by the CSP, the additional overhead of TTP encryption and decryption has been reduced. Moreover, the main role of TTP is to resolve a dispute between CSU and CSP. The proposed solution provides seven security functions, such as data integrity, data confidentiality, authenticity, non-repudiation, transmission secrecy, non-falsification, and non-traceability.

Approaches and solutions based on the TTP have been widely known and used over the last several decades. In the 1990s, research was already being conducted around the TTP concept, and a solution was sought for the problem of providing TTP services [11], such as managing cryptographic keys for end-to-end encryption in a way that meets legal requirements. The authors also present other possibilities and problems in the use of TTP; e.g., the need for a certification hierarchy to define a common point of trust for different TTPs, sharing keys between TTPs, and proposing a bidirectional communication scheme in which two keys are used–one for each direction (it is also possible to combine both of these keys into one session key or use only one of them) [11].

The authors in [12] present a key exchange scheme and data encryption between users with the use of TTP. The main aim is to ensure the security of the exchanged data, as well as shift most of the computational load to the TTP. A trusted third party may also be responsible for storing and periodically renewing public key certificates. The proposed solution combines TTP with symmetric and asymmetric cryptography, ensuring a high level of data security.

Another interesting solution is a protocol proposed in [13], which combines advantages of security, scalability, simplicity of application, and the possibility of real implementation. The protocol uses a lightweight TTP, available online. Thanks to this, the end user requires only a standard e-mail reader and a web browser. The proposed solution also does not need a public key infrastructure.

In [14], the authors used a TTP to develop a secure sum protocol to improve the privacy and security of data (if they are collected from various sources) by performing secure multi-party computations. The authors state that the computational process that is performed by a TTP provides greater security and achieves lower computational complexity than existing secure sum protocols.

Research on the application of TTP also appears in quantum computing. In [15], the authors propose a trusted third-party e-payment (TPEP) protocol based on a quantum signature without entanglement. In the protocol, to improve the security of information transmission, both the sender and the receiver of information will perform eavesdropping detection. Moreover, all participants in the whole transaction process only need to operate with a single-particle quantum H gate. According to the authors, the protocol consumes less resources and is easier to implement than other protocols with entangled states. A similar TTP application area can be found in [16]. Authors propose an innovative dynamic multiparty to multiparty quantum secret sharing scheme, where two distant groups of

participants can share common secrets. In the presented solution, a TTP is required to reliably prepare all quantum resources. It means that all participants in the scheme do not need to prepare any quantum entangled resources, which effectively reduces the number of qubit generators. In the authors' opinion, the proposed protocol can be more conveniently realized in real applications and can resist various common attacks like intercept-and-resend attacks, Trojan horse attacks, collusion attacks, and entangle-and-measure attacks.

In the design of smart home systems, TTP can also be applied. In such solutions, TTP plays a framework role for communication and data transmission [17]. This results in increased energy efficiency, a longer system lifetime, and faster data delivery. With the help of TTP and the event timer, the packet reception ratio (PRR) is high, at around 91%. In addition, network overhead is diminished, average packet latency is greatly reduced, and bandwidth is increased.

The TTP concept is also well known and is applied to ensure security in medical applications [18]. It involves the use of a TTP to verify the authenticity of messages sent, manage cryptographic keys for end-to-end encryption, and protect against MITM or DoS cyberattacks. It is an alternative system to the well-known PKI solution.

A trusted third party can also be used effectively in audio steganography. In [19], the authors use an indexing key with TTP, which increases the confidentiality of the secret message and adds another layer of protection for the decoder module. The presented methodology is used for audio files and is best suited for 32-bit files, because in their structure there are more available so-called least significant bits (LSBs), which can be used to transmit a secret message. It is worth noting that according to the definition of steganography, not only the message is encrypted, but the fact of its transmission is also kept secret.

The authors in [20] present an interesting and effective approach to improving the security of data stored in the cloud for the cloud client (CC) using a half-trusted third-party auditor (TPA). The proposed concept adopts the advanced encryption standard (AES) to support the privacy of the data owner as well as a cryptographic hash function to maintain the integrity of the data owner. In addition, it uses elliptic-curve cryptography (ECC) to ensure data confidentiality, correctness, and security when data is transferred over unsecured channels. Moreover, AES encryption is also used here to secure data during the audit. This means that a half-trusted TPA cannot reveal or extract the contents of the data file. TPA is responsible for auditing cloud data integrity on behalf of CC, as TPA has knowledge and capabilities that CC does not. According to the authors, the advantage of the approach is that TPA is not able to extract the content of data stored on the cloud server during the audit process, which eliminates potentially costly auditing burdens and alleviates CC fears of data leakage.

The trusted third party is also present in many other areas. For example, the combination of TTP and agent systems can help to control the quality-of-service contracts and guarantee transparency and symmetry regarding the service level agreement (SLA) between potential signatories [21].

Research on applying TTP in the management of services in automotive clouds is also very interesting [22]. The authors compare two algorithms: service latency sensitive mode (SLSM) and neutral mode for connecting vehicles to the cloud using TTP to provide services. As a result, delays in connecting vehicles with TTP are smaller (depending on the number of suppliers, vehicles, and available service providers). On the other hand, services such as video and audio have a greater improvement in service latency than "lighter" services such as fuel price.

From the general point of view, the usage of an open or permissioned blockchain can be effective only in the case of many conjointly mistrusting entities that intend to interact and alter the state of the system. Those entities are not eager to reach an agreement on an online TTP. In such a situation, it is assumed that one or many parties relate to an entity with admittance in a distinctive database structure or to a consensus member in a blockchain architecture. In the case where no data ought to be kept, the database is not obligatory at

all; that is, a blockchain-form database is useless. Analogously, in the case where there is only one writer, a blockchain does not make extra guarantees available, and an ordered database is much more suitable as it offers better enactment of throughput and reduces latency. Additionally, if a TTP is applied, there are two possibilities. The first one refers to the TTP that is continuously online. Then, tasks regarding storing data can be passed on to it and it can work as a verifier for state transitions. The second possibility relates to the situation where the TTP is typically offline. It can work as a certificate authority in environments of permissioned blockchain, and all writers of the system are identified.

In the scenario where all the writers mutually trust each other, it is considered that no member is malicious. In such a case, the database with shared write authority seems to be the best option. Alternatively, if there is no mutual trust between the writers, the permissioned blockchain is a better option. It is liable if public verifiability is obligatory. Then, anyone can be accepted for reading the state (public permissioned blockchain), or several readers can be limited (private permissioned blockchain). If the number of writers is not static, nor identified to the members (like in the case of many cryptocurrencies, such as Bitcoin), a permissionless blockchain is an appropriate resolution. In the area of cryptocurrencies and blockchain technology, researchers point out the problem of lacking the trust associated with transactions in the Bitcoin network. As these transactions are irreversible, consumers may be wary of entering into them [23].

In [24], interesting research is presented. The authors propose the T^3AB framework to address the transparency and trustworthiness of third-party authorities (TPAs) and honest-but-curious entities in functional encryption (FE) or attribute-based encryption (ABE)-enabled applications, as well as other schemes that have components similar to TPAs. The framework employs the Ethereum blockchain as the underlying public ledger infrastructure, and incorporates a novel smart contract to support accountability with an additional incentive mechanism that motivates participants to engage in auditing and punish misbehaviors or malicious behaviors in the environment. The authors' evaluation shows that T^3AB is efficient in the simulated Ethereum, and achieves the security, privacy, and trustworthiness goals. The authors suggest that one future direction is to establish a more complete theoretical framework for transparency with security and privacy guarantees that incorporate FE and ABE-type schemes as well as other cryptographic infrastructures that have different architectural components.

Interesting studies of the blockchain application from the trust point of view are shown in [25]. The authors present a taxonomy and a wide review of blockchain-based trust management approaches in cloud computing systems. They classify these approaches into different taxonomies according to three phases: blockchain-based basic trust framework, blockchain-enhanced trust interaction framework and mechanisms, and data management. Moreover, to improve the efficiency and adaptiveness of trust-enabled cloud computing, a novel cloud-edge hybrid trust management framework along with a double-blockchain-based cloud transaction model are proposed. The paper also points out the huge gap between the theory of the method and the actual application. Finally, the authors suggest that utilizing the blockchain technique to build a more credible and safe cloud transaction environment is a promising research direction.

Paper [26] presents research on blockchain-based decentralized trust management in the Internet of Things (IoT). The IoT has greatly enhanced various aspects of daily life, including managing homes, cities, transportation, healthcare, and industries. Despite its advancements, IoT faces challenges, and the authors in the paper propose blockchain technology as a promising solution to address limitations in traditional IoT, especially in trust management (TM). The research emphasizes a shift towards distributed TM due to weaknesses in centralized systems, and highlights the benefits of blockchain's decentralization, security, immutability, and traceability in addressing TM issues in IoT. The big value of the paper is a comprehensive and comparative analysis of blockchain-based decentralized trust management systems for different IoT classes, along with the identified requirements

and challenges in the context of using blockchain for efficient and secure TM solutions for IoT.

The paper [27] points out the lack of interoperability among different blockchain platforms. Even though the underlying technology is similar, it relies on centralized third-party mediators to exchange or retrieve information from other blockchain networks. Therefore, the authors propose a mechanism that provides cross-chain interoperability using transactions. The proposed model emphasizes the advantage of multiple interoperable blockchains, allowing seamless exchange of crypto assets and demonstrating better performance compared to other blockchain-based models in cross-communication processes between distinct blockchain systems. Moreover, the authors predict a future where diverse blockchains operated by a variety of enterprises, both public and private, interact across the network, anticipating a change in the way we engage with governments, businesses, and institutions.

There are also some commercial solutions available, like DocFlow [28] from PixelPlex or the group of products from Scalable Solutions AG [29]. DocFlow is a blockchain-based document management software that digitizes the entire paperwork cycle and uses advanced smart contract mechanisms to guarantee data security and authenticity. The authors of DocFlow emphasize the trusted side of the developed solution (e.g., secure client registration process, multi-tier role-based and coded access, immutable and decentralized ledger, etc.). Scalable Solutions AG company points out that its products use decentralized, transparent, and blockchain-based systems, as well as apply cryptography and automation of data exchange.

Another interesting piece of research that integrates blockchain technology with trust management is presented in [30]. Because of the decentralized nature of the blockchain network, identity management demands different trust requirements. Therefore, the authors provided a critical analysis of existing research, which sheds light on various opportunities for enhancing the security and privacy of blockchain-based self-sovereign identity management. Finally, the authors conclude by presenting research gaps and suggestions for future work in this area.

Nowadays, electronic portfolios (e-portfolios) are being increasingly used (especially by students) as digital online multimedia résumés that showcase their skillsets and achievements. E-portfolios require secure and reliable verification mechanisms to prove learning achievements. Therefore, existing systems provide private institution-wide centralized solutions that primarily rely on TTP. Paper [31] proposes a consortium blockchain-based e-portfolio management scheme that is decentralized, secure, and trustworthy. Thanks to the use of immutable ledgers and smart contracts, the proposed system guarantees the authenticity and integrity of user credentials and e-portfolio data. Moreover, the authors implemented their solution using the Quorum blockchain platform and made e-portfolio certificate issuance and verification performance analysis.

Finally, in [32], the authors indicate that despite many advantages of the blockchain technology with its decentralized ledger storing blocks, there may appear problems related to the replacement of trust represented by a physical entity or person. In some cases, the involvement of the other party to verify certain predicates is necessary. In general, predicates depending on e.g., sensor measurements, remain external, because sensors are physical objects that cannot be fully represented in a digital system [23]. This leads to the conclusion that although blockchain technology has great potential for new uses, it very often requires a TTP to be secure and trusted.

The proposed approach is focused on practical implementation, and is based on real market needs. Moreover, the approach is based on theoretical foundations, reliable cryptographic methods, and secure blockchain technology. The key feature of the presented approach is a unique combination of decentralized blockchain (usually with untrusted nodes) with a trusted third party. In the literature, there are many blockchain-based approaches, but usually, they apply blockchain technology to empower communication among non-trusting members devoid of the third party [33]. However, there also can be

several solutions similar to the presented one. Some of them implement the third party in a way that is not fully trusted (so-called semi-trusted solutions [9])—some of the other solutions store documents in unencrypted form. But, to the best of the authors' knowledge, none of the analyzed solutions used a hardware security module to store the critical cryptographic data and generate necessary symmetric and asymmetric keys. Moreover, only a few of the available solutions use an external IPFS network to store documents (in the blockchain, it is very hard due to the limitation of blockchain technology). The smart combination of all mentioned features (i.e., decentralized blockchain, TTP, cryptographic algorithms, HSM, and IPFS) makes the designed and implemented e-service trusted and secure.

3. The Proposed TTP Application

The first step in the design process of the durable medium e-service was to develop functional requirements based on the state-of-the-art analysis (presented "related works" section), as well as on the technical capabilities of the real company. The designed e-service should meet the following functional requirements:

- data of one entity (e.g., bank, internet service provider–ISP) should be stored in a non-public database limited only to the data of a given entity,
- data should be stored in a way that prevents their modification (once saved in the database, it should not be possible to delete or modify them),
- data (including sensitive electronic documents) should be stored in an encrypted form so that in the event of a possible leak, they (and the personal data contained in them) are useless to cybercriminals or third parties,
- access to data should be, on the one hand, convenient (especially for users/customers), and on the other hand, secure and controlled,
- a fast symmetric encryption algorithm (e.g., AES) should be used to encrypt documents,
- the e-service should be developed for entities (e.g., financial) with a large number of clients (the entity plays a dominant role) that need to store and process documents, meeting the requirements of a durable medium (by Polish law regulations),
- data should be saved in a decentralized database, allowing data to be distributed between nodes;
- the service should offer the ability to generate an AES symmetric key and encrypt/decrypt it using an asymmetric key pair generated by the Rivest–Shamir–Adleman (RSA) algorithm.

To meet all the above-mentioned functional requirements, in the proposed approach, a TTP plays the role of a trusted intermediary in the process of transmitting, exchanging, and processing electronic documents between several parties. Thanks to this, electronic documents will be processed securely, and their integrity and immutability will be maintained. Additionally, the presented electronic service (e-service) uses immutable and secure blockchain technology [34].

The next stage in the design process was to model the e-service. The main idea of the proposed e-service on a high level of abstraction is presented in Figure 1. The approach assumes that two business sides and one TTP participate in the process. Moreover, one of the business parties is the dominant entity over the other (e.g., a bank towards its clients) due to the fact that the proposed solution is dedicated to large business entities or institutions that offer services to a large number (e.g., tens of thousands) of clients. Nevertheless, the technique can be easily adapted to other business scenarios where more than two business parties are involved, and they may even be equivalent to each other (e.g., three entrepreneurs processing a common, tripartite business agreement).

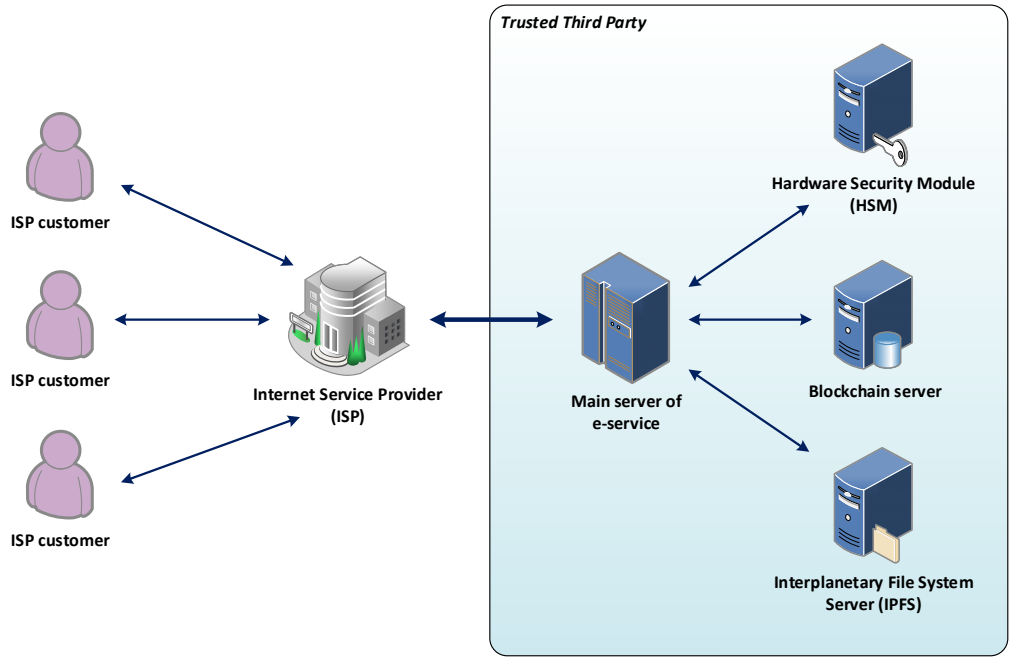

Figure 1. The main idea of the proposed e-service on a high level of abstraction.

The proposed approach is mainly focused on two important aspects. The first one is related to security, implemented through the use of blockchain technology and cryptographic methods securing the process on the TTP side. Blockchain ensures that data is immutable and cannot be modified by any party, which also ensures data integrity and reliability. The second aspect refers to trust, which is achieved by using a TTP as an impartial arbiter independent of any parties, managing the electronic document processing. Moreover, the TTP stores the blockchain database in its infrastructure. This means that only the TTP can perform block addition operations, as well as encrypt, sign, and share documents. This approach significantly reduces the possibility of interference by one party in the document flow, even if it is the dominant entity in the business relationship (e.g., a financial institution towards its customers).

3.1. The Main Algorithm of the Proposed e-Service

The proposed e-service concept is presented in Figure 2, in the form of an activity diagram from a unified modeling language (UML). The diagram presents the electronic documents flow and processes such as encrypting and signing documents, storing hashes of documents in the blockchain infrastructure, decrypting and sharing documents between parties, etc. Within the above-mentioned concept, three business actors are distinguished, two of them are connected by a business relationship, and the third one (TTP) is a neutral arbiter monitoring the entire process and offering several functionalities, ensuring the security and confidentiality of the sensitive documents transmitting process as a part of the durable medium service [35]. It is assumed that one of the parties is dominant (here, it is the ISP) and only the ISP is entitled to start the new document processing flow. The second party is represented by ISP customers. Moreover, one ISP can have thousands of clients. The diagram in Figure 2 presents the exemplary process of changing the price list by the ISP. Let us assume further that each customer can accept or reject the new price list (note that the consequences of accepting or rejecting the price list are not considered in this work).

The entire process begins on the ISP side by sending a document (here: new price list) and a list of customer identifiers to the TTP, who should accept or reject this document. This transmission of data can be realized using a previously established secure communication channel. In the next step, TTP signs the document (using an electronic signature) and uses AES to generate a 256-bit symmetric key. This key is used for the encryption of the

document. Let us underline that the generation of the AES key is performed in a hardware security module (HSM). Due to the limitations of blockchain technology (the size of data stored in one block), only the hash of the document and the identifier of the entity that sent the document (here: ISP) are saved in the blockchain. The fully encrypted document is stored on an external IPFS. It is worth noting that both HSM and IPFS belong to the TTP infrastructure.

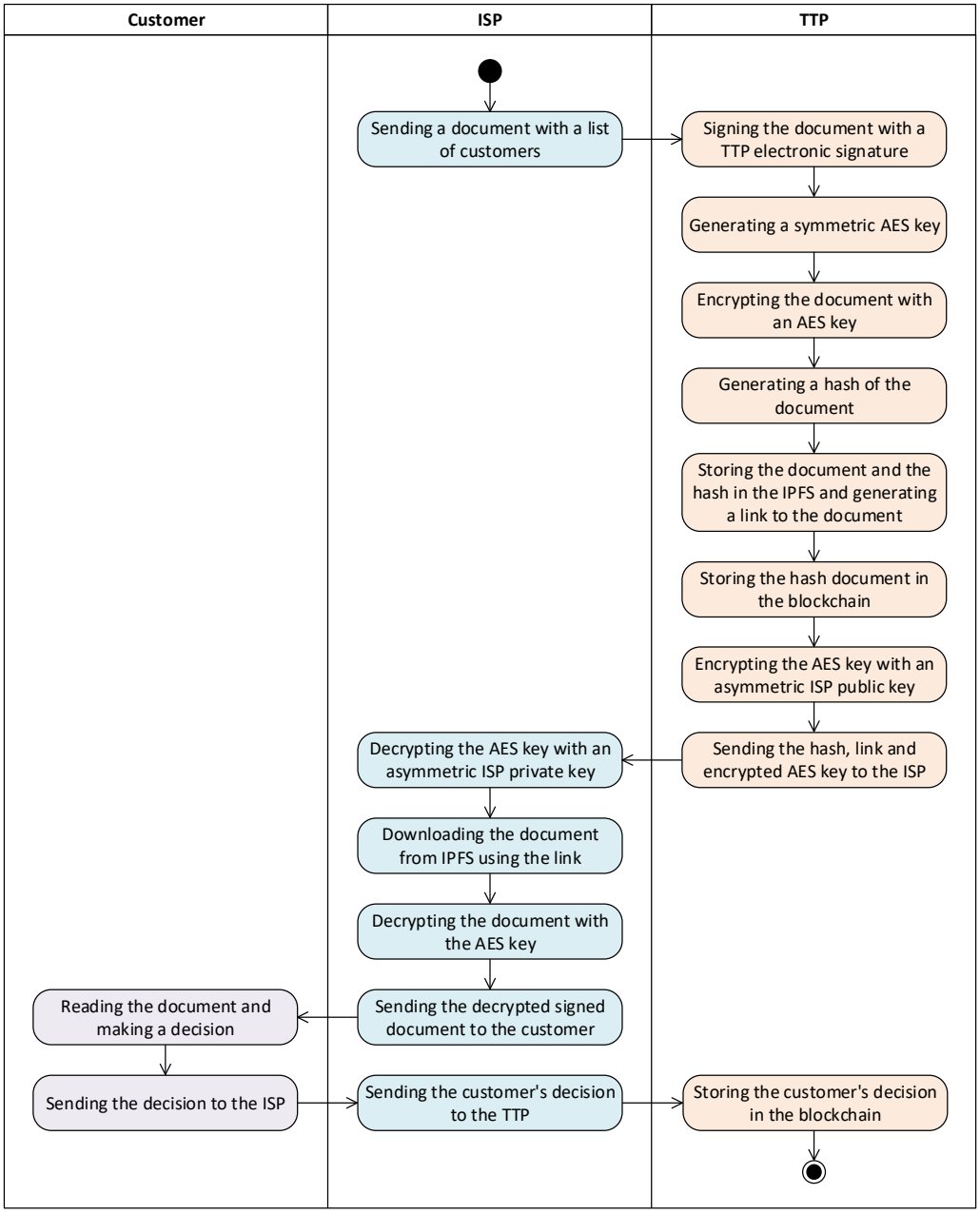

Figure 2. The proposed durable medium e-service in the form of a UML activity diagram.

At the next step, a 256-bit hash of the document is generated by the IPFS (it is assumed that the SHA-256 algorithm is used). The TTP stores both the document and hash in the IPFS network, and creates the link to the document. This link is used further to obtain access to the encrypted document. Moreover, the hash of the document is added to the blockchain as a new transaction. Finally, the generated AES key is encrypted by an ISP public key with the application of the asymmetric algorithm RSA. This operation is handled by the TTP, and it is executed within the HSM.

In the next stage, the following data are sent to the ISP: hash of the document; link to the encrypted document stored in IPFS, and encrypted AES key. Based on those data, the ISP is able to decrypt the obtained AES key with its private RSA key. The AES key is applied to decrypt the document downloaded from the IPFS. Finally, the document is sent to the selected clients in an unencrypted form (e.g., using the secure channel established with the client, strengthened by two-factor authentication or multi-factor authentication, for example). It is worth mentioning that the document is signed by the TTP, proving its authenticity and integrity.

The client reads the document and decides to accept or reject it. This decision, along with the client identifier and document hash, is transferred back to the TTP and placed by the TTP in the blockchain as a new transaction. This operation is repeated for each client (note that for more readability, the diagram shows the activities for one customer only). Finally, each of the n clients makes a decision, and n+1 transactions appear on the blockchain. It is assumed that the first transaction related to the particular document is provided by the ISP, while the remaining blocks are related to n transactions committed on the clients' decisions.

The presented algorithm assumes that there is one (the same) document for all clients. Of course, another scenario can be considered. Assume that there is a need to send annexes to the customers' agreements. In such a situation, a separate document for each client is prepared by an ISP. This means that for 10,000 clients, 10,000 documents ought to be generated. Nevertheless, the algorithm of the e-service looks similar to the one presented above. The only differences remain in the type and amount of transferred data. In the early stage of the process, the ISP sends not one document, but a set of documents with customers' identifiers assigned to them. Each document is signed by the TTP, and for each document, the TTP generates a separate symmetric AES key used for encryption. These AES keys (in an encrypted form) are sent to the ISP together with document hashes, links, and lists of customers' identifiers.

The entire process is supervised by the TTP, and the blockchain is stored in the TTP infrastructure. Therefore, if there are any doubts regarding the correctness of the document processing flow or if there is a suspicion of manipulation by the ISP, then the client may gain access to the blockchain network on demand. In such a situation, it is possible to verify the document and obtain the particular decision stored in the blockchain. Such an approach greatly reduces the risk of document manipulation in the process by each party, making the proposed e-service secure and trusted. Moreover, it should be underlined that the presented e-service meets the requirements of Polish law regarding the durable medium, including the need for permanent and safe storing of electronic documents in infrastructure independent of either party, as well as the need to monitor the process of documents' storing, processing, and making them available to the customer.

3.2. The Applied Blockchain Structure

Nowadays, blockchain is one of the most commonly used solutions for storing data in structures that are difficult to manipulate. In the proposed e-service, a private version of the blockchain is used. This means that access to specific data (stored in blocks) is only possible with the appropriate access rights. Moreover, a separate blockchain is created by the TTP for each large entity (e.g., bank, ISP, financial institution). Thanks to this, data from different entities (e.g., bank and their customers) are not stored in the same blockchain.

It should be noted that the security of a blockchain increases with the number of blockchain nodes. As the presented algorithm shows, the number of created nodes depends on the type of document and the number of clients. Because the presented e-service is dedicated to large entities (mainly financial), a large number of customers causes a large number of transactions. Moreover, it positively affects the security of the blockchain, and significantly reduces the possibility of manipulation (note that the blockchain is stored and managed by the TTP, not by the ISP). It is also worth noting that the generation of documents for clients (and storing documents' hashes in the blockchain) is iterative, and

hence predictable in contrast to the clients' decisions (individual clients gain access to the document and make decisions at a random time).

To effectively store the data in the blockchain, it was necessary to develop the structure of a single block (Figure 3). Several fields in the presented blockchain structure are typical for the blockchain network (e.g., "index", "timestamp", "block hash", "previous block hash", etc.), while the authors proposed the remaining fields:

- customer ID (CID)–this numerical field is used to identify the transaction side that operated on the document (e.g., adding, accepting, rejecting). If an ISP adds a document for processing, this field assumes a value identifying an ISP. In other cases, these are numerical identifiers of the ISP customers;
- document ID (DID)–this is a generated hash of the signed document;
- operation ID (OID)–a numerical field where a specific value is assigned for each operation on the document (e.g., adding, accepting, rejecting);
- additional data–a field added for development purposes, and is not used yet.

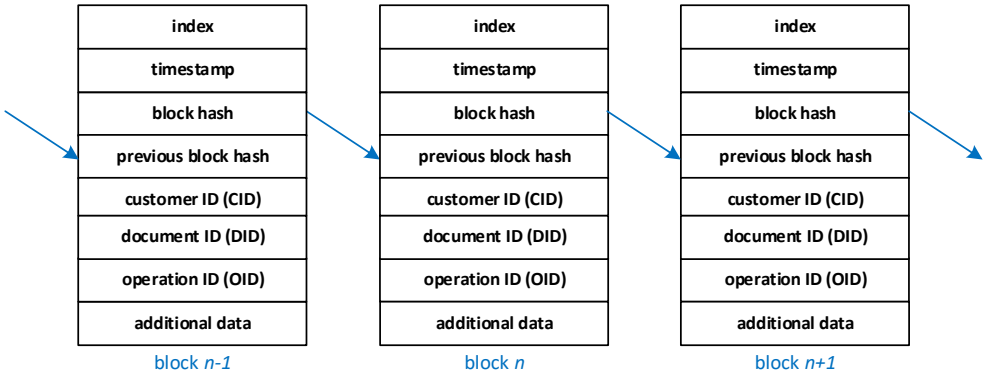

Figure 3. The proposed structure of the blockchain.

The proposed structure is flexible and allows for easy definition, for example, of new types of document operations (e.g., signing, requiring corrections, withdrawing, etc.)—only the expansion of the OID dictionary is needed. Moreover, the above structure can also be successfully used in an e-service in which the number of parties is not limited to three (e.g., there may be several equal entrepreneurs and each of them can initiate the document processing flow).

Another important aspect related to the blockchain refers to the choice of the consensus mechanism–i.e., the technique of reaching an agreement on adding new blocks between the nodes of the network maintaining the blockchain. Since the blockchain is managed by the TTP, instead of using the proof-of-work (PoW) mechanism, which requires large computational resources, the more effective proof-of-authority (PoA) mechanism is used to mine blocks. Thanks to this solution, computing power is not required to create new nodes. In particular, the proposed e-service utilizes the Istanbul byzantine fault tolerance (IBFT) PoA algorithm. In private networks, where participants are known and trusted, PoA allows for much faster transaction processing compared to more decentralized consensus algorithms such as PoW or proof-of-stake (PoS). The lack of competition for block mining, as in the case of PoW, eliminates the need to solve complex mathematical problems, which speeds up the transaction verification process. Moreover, PoA is more scalable than PoW, and allows for more controlled blockchain management, making it easier to comply with regulations and legal requirements.

3.3. The Role of TTP

In the proposed approach, a trusted third party is a very important element because it has the greatest impact on the trust of future customers to the solution. On the one hand, security issues (including cryptographic algorithms, electronic data signing, and private type of blockchain) build users' trust in the service. However, their greatest concerns are

focused on the possibility of data manipulation by the dominant entity (e.g., ISP, bank). Hence, among the others, one of the requirements regarding a durable medium is that the infrastructure in which the e-service is implemented should be independent of each entity (especially of the dominant entity) so that none of the parties has legal or technical possibilities of tampering with stored data. Therefore, in the proposed solution, the blockchain network is stored in the server infrastructure owned and managed exclusively by the TTP. Of course, other solutions are also possible. For example, the role of the TTP may be limited solely to an arbitrator who only supervises the processes of storing and processing documents by both parties. Moreover, in case of a dispute, TTP can make binding decisions. However, it seems that the approach applied in this work–to make TTP not only an independent side but also an e-service provider–is the most effective solution also from the cost point of view. Therefore, in the implemented e-service, the role of TTP is played by the "Perceptus sp. z o. o." company, which implemented the presented solution and whose infrastructure is used.

Moreover, the research on blockchain technology presented in the paper also leads to an interesting conclusion, that in some cases substituting trust with a ledger (e.g., blockchain) can be dreadful, and it comes with the necessity to involve another party for the authentication of definite predicates. As a concern, while ledger technology bears perspective for new applications, many use cases will require a TTP.

3.4. The Security Analysis of the Proposed e-Service

Finally, let us briefly analyze the security aspects of the proposed technique. Note that experimental verification (based on the case-study example) is presented in Section 4 in detail. An important part of the presented approach refers to the security. Blockchain technology offers the prospective property for handling numerous security attacks, as it can disregard the prerequisite of a centralized authority for performing various operations. In the presented technique, users that participate in the transaction verification and validation utilize a structurally distributed database that stores data from all nodes in an encrypted form authorized by various checks; such as Merkle hash tree (MHT), and ECC. The database is distributed; thus, there is a threat of crashing or corruption. Therefore, the transactions are linked together with cryptographic keys and immutable ledgers, which create much more difficulty for invaders towards the manipulation or deletion of the recorded information.

According to the current state of knowledge on the application of blockchain technology, many blockchain-based applications are strongly protected from DoS/DDoS attacks due to their decentralized design [36–40]. Here, all the services are copied and placed on various network nodes. In other words, we want to emphasize that if an attacker disables one node, they will never be able to disable all the other nodes. Also here, using blockchain, we have ensured that all transactions are expensive, which of course discourages the attacker from directing huge transactions.

Our approach is to have message replay protection due to the use of blockchain technology [36–40]. Here all messages are considered to be a transaction. Every transaction is always timestamped, and every transaction has to go through the consensus part to be well thought out and considered legal. Therefore, the attacker will never be able to respond to the messages, because the consensus procedure will discard them.

Our approach is also protected against Sybil attack [41]. In our approach, everyone can only have one identity at a time, and each identity will have only one key pair. Each communication message must be signed with the private key associated with this identity. Moreover, our blockchain-based approach requires the validation of all IDs, so an attacker cannot use a fake identity at all.

Man-in-the-Middle (MITM) attack is also impossible because there is no single thread of communication to be intercepted. Therefore, by using blockchain technology, our system can be more secure and protected against MITM attacks.

Furthermore, authentication and message integrity are perfectly preserved here. The certificate is used by each follower (for the first transaction). Initially, during the first

process, the certificate is directed only to valid participants. All exchanged transactions are signed using private keys. As a result, signatures protect the authenticity of each signature and the integrity of the message. In other words, we can say that it guarantees that no one can join the network without a certificate.

Moreover, the TTP signs the document with an electronic signature, and additionally applies AES to generate a 256-bit symmetrical key. Such an AES key is used for encryption of the document. Then ISP decrypts all the AES keys using the corresponding private RSA key. So, these cryptographic keys ensure enhanced security in our approach.

The data is always stored in an immutable manner using timestamps, public audits, and consensus mechanisms. Furthermore, the IPFS uses the Secure Hash Algorithm (SHA) 256-bit version to generate the 256-bit hash of the document. Moreover, the SHA-256 algorithm guarantees data integrity. These techniques make the proposed approach secure by assuring data integrity and privacy, and make our approach protected from DDoS and MiTM attacks too.

Another interesting issue regarding blockchain is the use of formal verification of smart contracts and blockchain code [42,43], which can be very helpful in the prevention of costly errors and security breaches. These formal verification methods are very often based on documenting vulnerabilities or model-checking techniques. The authors in [42] made a detailed analysis and review of the applied state-of-the-art formal methods on smart contracts specification and verification. The main criteria of this analysis were minimizing the risk of faults and bugs occurrence, and avoiding possible resulting costs. Regarding formal methods, in [43], a worthwhile approach is proposed. The authors propose a new approach to model smart contracts and blockchain execution protocol along with users' behaviors based on a formal model checking language. Based on this model implementation, and given their expected behavior, design vulnerabilities of the smart contracts can be analyzed using a statistical model checking tool.

4. Experimental Verification of the Proposed e-Service—A Case Study

The presented solution was experimentally verified using a few test scenarios. Two of them are presented in the paper. In the presented scenarios, the e-service of a durable medium was implemented for the ISP, which plays a dominant role in the process (it means that only the ISP can initiate document processing), and the role of the ISP clients is limited only to accepting or rejecting the document. TTP plays the role of the e-service provider and a supervisor, which monitors the flow of document storage and processing (including management of the blockchain and IPFS network). The blockchain was implemented using the Hyperledger Besu [44] platform. Besu is an Ethereum client designed to be enterprise-friendly for both public and private permissioned blockchains. Moreover, it includes several consensus algorithms including PoS, PoW, and PoA (IBFT 2.0, QBFT, and Clique). This platform also supports smart contracts, which have a significant impact on the security of the entire solution [45]. Table 1 presents the selected configuration parameters of the blockchain implementation (please note that some of them are specific only for the Besu environment).

Table 1. The selected configuration parameters of the blockchain implementation.

Parameter	Value
blockchain type	private with IPFS
consensus algorithm	IBFT
number of nodes allowed to approval new blocks	4
block period seconds (in seconds)	2
request timeout seconds (in seconds)	4
gas limit	9,007,199,254,740,991
contract size limit	2,147,483,647
minimum gas price	0

In the first test scenario, it was assumed that the ISP wanted to introduce a new document (e.g., an annex to the contract) for each of its 10,000 customers. Each of these documents are personalized and dedicated only to one of the ISP clients and must be agreed with the client (accepted or rejected). As a result, the e-service must process 10,000 various documents that need to be agreed with 10,000 ISP customers.

In the first step, the ISP selects the 10,000 documents and customers to which this document concerns and sends the documents and 10,000 identifiers of the ISP clients to whom these documents refer to the TTP. TTP first signs all the documents with an electronic TTP signature and generates 256-bit symmetric AES keys–one for each document. Then using the AES keys, each of the 10,000 documents is encrypted (each document has a corresponding different AES key).

Then, TTP sends the encrypted (signed) documents to the IPFS server, which generates a hash using the SHA-256 algorithm for each document and stores it in the IPFS network together with the encrypted document. For each stored document, IPFS also generates a link which, together with the hash, is sent back to the TTP. In the next step, TTP adds 10,000 transactions to the blockchain (one transaction for each document). Each transaction contains a hash of the document (DID field in the blockchain structure), the identifier of the entity that sent the document (this is a numerical value identifying the ISP–CID field), and the identifier of the document addition operation (OID field). Due to the limitations of the data limit that can be stored in the blockchain, the document itself is not saved in the block. The right, encrypted documents along with their hashes are stored in the IPFS network.

In the next step, TTP encrypts each of the AES keys with a 2048-bit ISP public key using the asymmetric RSA cryptographic algorithm. Then, a list containing 10,000 items is sent back by TTP to the ISP. Each item in the list contains the following information: a hash of the document, a link to the encrypted document in the IPFS network, an encrypted AES key, and the client identifier to which the document relates. Then, the ISP decrypts all the AES keys using his private RSA key. Next, using links to the documents, the ISP downloads documents from the IPFS network and decrypts them using encrypted AES keys. In the next stage, the ISP makes these documents available to his clients (in decrypted form so that customers can easily read them). After reading the document, each customer decides to accept or reject it. The client's decision is forwarded to the ISP, which forwards it further to the TTP (along with the customer ID and hash of the document). Then, the TTP places each decision (treated as an operation on the document and stored using the OID field) along with the customer identifier (CID) and document hash (DID) in the blockchain as a new transaction in the block. Ultimately, after each of the 10,000 customers makes a decision, 20,000 new transactions will appear in the blockchain (10,000 transactions with documents added by the ISP and 10,000 transactions with decisions of 10,000 customers regarding these documents), as shown in Figure 4. This figure presents a summary of the number of transactions after execution of the test scenario, and is recorded using Sirato Explorer (blockchain monitoring tool). As can be observed in Figure 4, there are two more transactions. This is because adding a smart contract is itself registered as a new transaction. So, there is one more transaction for a smart contract regarding adding documents, and one more for a smart contract regarding adding customers' decisions.

Figure 5 presents a selected block (no. 610) from the blockchain recorded using Alethio Lite Explorer—a blockchain monitoring tool. This block contains, among others: the information about the number of the block (610), block approval status (the "Confirmed" green message means that the block was fully approved by nodes responsible for the consensus algorithm), hashes of the current block and parent block, size of the block (23,262 bytes), number of included transactions (63), information about the node, which confirmed the block ("mined by" field), gas limit, the amount of used gas (<1%), and difficulty in mining block (1 h).

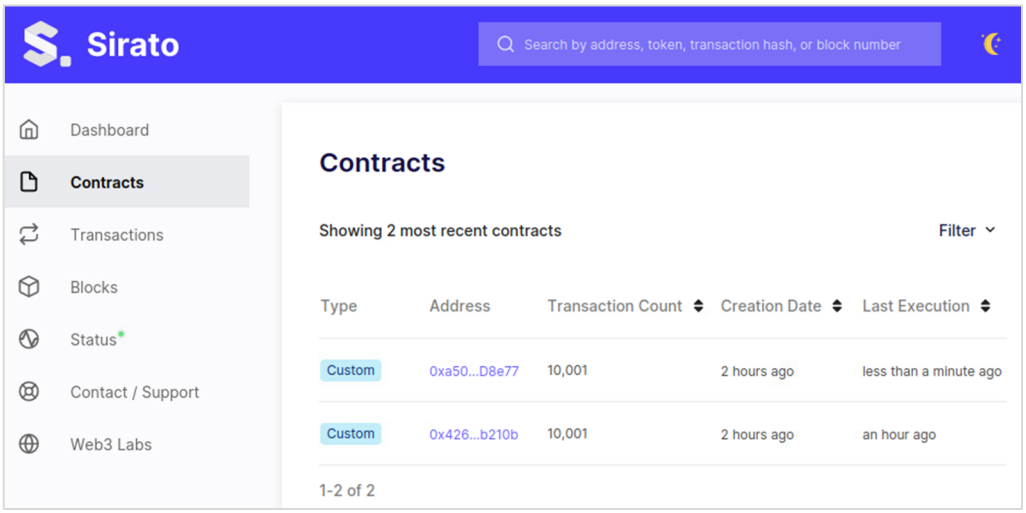

Figure 4. Summary of the number of transactions after execution of the first test scenario.

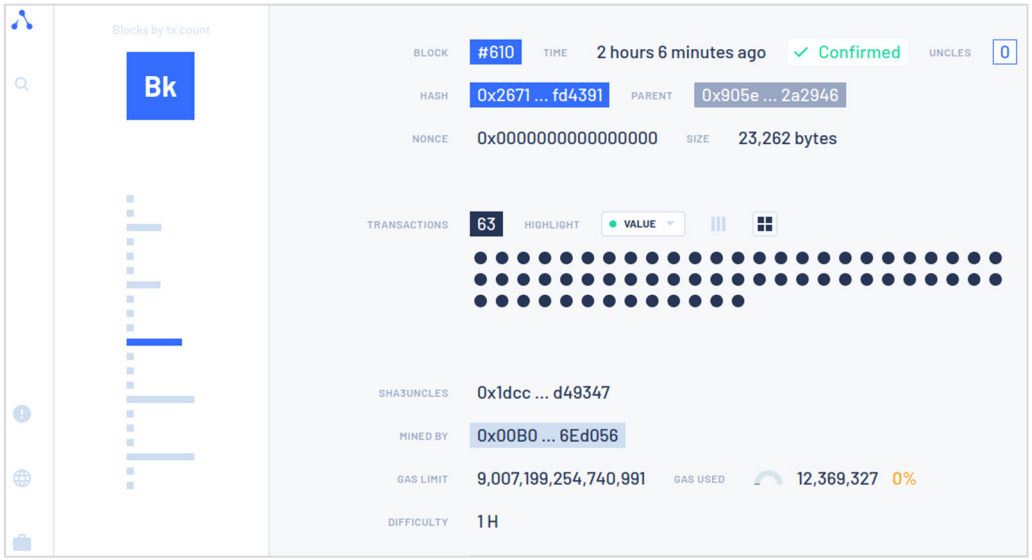

Figure 5. Detailed information about one selected block from the blockchain.

The second case study test scenario presents a situation in which the ISP introduces a new document, but is common for all clients (e.g., new regulations, price list, etc.). This document must be agreed upon with each of the 10,000 ISP customers. In the first step, the ISP sends the document and a list of 10,000 identifiers of the ISP customers to whom this document applies to the TTP. Next, the TTP electronically signs the document with its digital signature and generates a symmetric 256-bit key using the AES-256 algorithm. The document is encrypted using this AES symmetric key, and the AES key is encrypted using an RSA 2048-bit ISP public key. It is worth noting that the generation of the AES key is performed in the secure HSM hardware module.

Then the TTP sends the encrypted (signed) document to the IPFS server, where a hash using the SHA-256 algorithm is generated. Next, the document is stored in the IPFS network and a link to the document is generated. Then, the link together with the hash of the document is sent back to the TTP, and the TTP adds a new transaction in the blockchain. The transaction contains a hash of the document (DID field in the blockchain structure), the identifier of the entity that sent the document (an identifier of the ISP stored in the CID field), and the identifier of the document addition operation (OID field). The document itself is not saved in the blockchain, but it along with its hash is stored in the IPFS network.

In the next step, the hash of the document, a link to the document in IPFS, and the encrypted symmetric AES key are sent back to the ISP. Then, the ISP decrypts the AES key using its private RSA key. Next, using the link, the ISP makes the document available to all clients. After reading the document, each of the customers decides to accept or reject it. The client's decision is forwarded to the ISP, which forwards it to TTP. Then, the TTP places this decision, along with the customer identifier (CID) and document hash (DID), in the blockchain as a new transaction in the block. The process of acceptance or rejection of the document by other customers is analogous and iteratively repeated by the ISP. Ultimately, after each of the 10,000 customers makes a decision, 10,001 transactions will appear in the blockchain (the first transaction with the document provided by the ISP and 10,000 transactions with the decisions of 10,000 customers regarding this document), as shown in Figure 6. The figure represents the total number of transactions after the implementation of both scenarios within the same blockchain, therefore the number of transactions added in the second test scenario is 20,001 − 10,001 + 10,002 − 10,001 = 10,001.

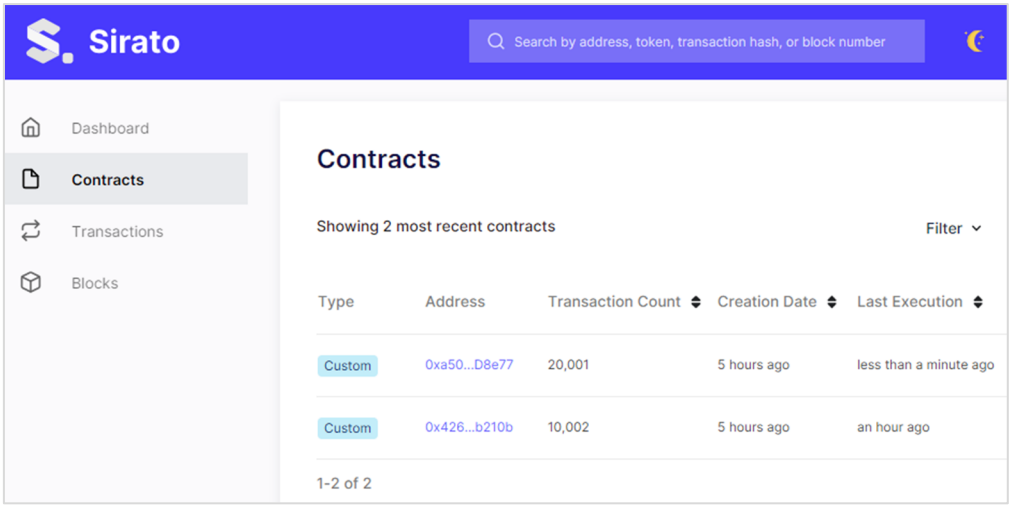

Figure 6. Summary of the number of transactions after execution of the both test scenario.

Moreover, in the first test scenario, it was assumed that approximately 80% of customers would accept the document and the remaining 20% would reject it. In the second scenario, the accepted level of acceptance was 90%. Therefore, in the implementation of both scenarios, special randomization functions were added to implement the above assumptions. In practice, it turned out that the level of acceptance differed slightly from the assumed level (81.63% in the first scenario and 91.08% in the second scenario). The remaining performance results obtained during the realization of both test scenarios are summarized in Table 2. Compared to Figure 4, there are 10,001 more transactions (1 for the added new document and 10,000 for customer decisions).

Table 2. Summary of selected experimental results.

Parameter	Obtained Value (First Scenario)	Obtained Value (Second Scenario)
The level of acceptance of the document by customers	81.63%	91.08%
Average time of adding a document transaction to the blockchain (in milliseconds)	23.073	202.164
Average time of adding a customer's decision transaction to the blockchain (in milliseconds)	0.0358544	0.0486139

According to the conducted test cenarios where over 30,000 transactions were added to the blockchain, the implemented e-service worked properly, and the initial requirements were met. The obtained performance results are also acceptable. In the first scenario, the

average time of adding the transaction responsible for adding a new document (by the ISP) to the blockchain was approximately 23 milliseconds, which for 10,000 documents is less than 4 min. In the second scenario, the time of adding a document was approximately 202 milliseconds, which is quite a lot compared to the first scenario; however, it is worth remembering that there was only one added document in the second scenario, so the obtained result is also acceptable. The average time of adding transactions with customer decisions was only about 0.036 milliseconds in the first scenario, and 0.049 in the second scenario, which are also fully satisfactory results.

Although the experimental verification finished with success, the authors faced several issues. One of them was the problem of working out error-free smart contracts. This is a real challenge, since adding a contract containing errors to the blockchain results in serious consequences for the entire blockchain network. Another issue is related to the asynchronous technique of adding a transaction (i.e., without confirmation whether the transaction has been added or not). However, an in-depth analysis allowed us to find a solution to this problem (the detailed description is considered for future work).

It is worth noting that the dataset used in the experimental verification was prepared by the authors. The dataset includes more than 10,000 documents (in portable document format, PDF) specially generated for both test scenarios. These documents contain information regarding provisions from typical contracts concluded between the ISP and its customers (only the customers' data are fictitious). Also, the transactions and smart contracts were prepared specifically for the needs of the implemented e-service.

5. Conclusions

The paper proposes a novel concept of TTP application in the form of a durable medium electronic service. The main research problem relates to the design and implementation of a trusted and secure e-service for processing and managing sensitive electronic documents. The presented solution applies blockchain technology combined with cryptographic methods. Moreover, an independent company playing the role of a TTP is considered. The application of blockchain technology ensures that once stored, documents cannot be changed nor deleted in the future. In the presented solution, the TTP acts as a trusted, impartial arbitrator who monitors the process of storing and processing documents, and in the case of disputes, makes final and binding decisions. TTP is also a provider of a safe and trusted durable medium e-service, thanks to which documents are stored in a server infrastructure independent of other parties (e.g., a bank and its customers). Due to the nature of this work, the presented research combines both scientific and implementation aspects. The possibility of the application of a trusted third party (combined with blockchain technology) is also analyzed. The experimental verification results confirmed the correctness of the developed e-service.

The key feature of the presented approach relies on a unique combination of decentralized blockchain with TTP, which increases the security and reliability of electronic document storage and management. Moreover, the proposed e-service meets all the requirements and law regulations regarding durable media, and was developed based on real market needs. Finally, it was implemented in the real company "Perceptus sp. z o. o." from Zielona Góra (Poland), expanding its product offer.

Despite the above-presented advantages, the proposed solution also has limitations. One of them is the fact that the presented e-service requires continuous operation. This means that the servers on which the e-service is implemented require continuous availability, and therefore may generate significant costs. Moreover, the need to ensure the availability of nodes in various locations (decentralization of the service) may also enlarge maintenance expenses. Another disadvantage of the developed solution can also be the large number of generated cryptographic keys. In the proposed approach, a symmetric AES key is generated for each processed document, which—given a large number of documents (numbered in millions)—means the need to store and manage a very large amount of critical cryptographic material in the HSM, whose capacity is also limited. On the other hand, it

is worth emphasizing that such a large number of symmetric keys positively impacts the security aspect of the proposed solution (e.g., interception or leakage of one AES key will result in access to only one document, while the rest are safe).

Further work will focus on improving the efficiency of the developed solution, reducing transaction costs and increasing both the scalability and the bandwidth of the e-service (i.e., communication with the blockchain, IPFS, and HSM). Moreover, the performance analysis of the blockchain is planned to be carried out to observe how the transaction execution time changes under various conditions. Based on the performance analysis results, there is a plan to compare with other existing approaches and products; however, access to the performance data of other solutions (especially commercial ones) is very difficult. Research plans also involve developing a new consensus protocol that would be more effective and use fewer resources. Additionally, the possibility of using blockchain technology in other areas of the industry will also be investigated.

Author Contributions: Conceptualization, G.B., K.K. and R.W.; methodology, G.B., K.K. and R.W.; validation, R.W. and A.B.; formal analysis, G.B., R.W. and A.B.; investigation, G.B., K.K. and R.W.; resources, K.K.; data curation, G.B. and K.K.; implementation, K.K.; experimental verification, G.B., K.K. and R.W.; writing—original draft preparation, G.B., K.K., R.W. and A.B.; writing—review and editing, R.W. and A.B.; visualization, G.B. and K.K.; supervision, G.B. and R.W.; project administration, G.B.; funding acquisition, G.B. and R.W. 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 grant number DWD/4/90/2020.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Restrictions apply to the availability of these data. Data was obtained from Perceptus sp. z o.o., Zielona Góra, Poland and are available from the authors with the permission of Perceptus sp. z o.o.

Conflicts of Interest: Author Kamil Kozdrój was employed by the company Perceptus Sp. z o. o. Author Aniruddha Bhattacharjya was employed by the company BCBRBAB Intercontinental Trading Solutions Private Limited. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Phillips, K.; Davidson, J.C.; Farr, R.R.; Burkhardt, C.; Caneppele, S.; Aiken, M.P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sci.* **2022**, *2*, 379–398. [CrossRef]
2. Wright, C.S. Chapter 21—Information systems legislation. In *The IT Regulatory and Standards Compliance Handbook*; Craig, W., Ed.; Syngress: Waltham, MA, USA, 2008; pp. 609–671. ISBN 9781597492669. [CrossRef]
3. Perceptus Sp. z o.o. Available online: https://perceptus.pl/ (accessed on 8 October 2023).
4. Polish Office of Competition and Consumer Protection (Urząd Ochrony Konkurencji i Konsumentów, UOKIK in Polish). Trwały Nośnik—Decyzje Wobec ING, Getin Noble i PKO BP, Durable Medium—Decisions regarding ING, Getin Noble and PKO BP. (In Polish). Available online: https://uokik.gov.pl/aktualnosci.php?news_id=14909&news_page=4 (accessed on 20 November 2023).
5. Argento, L.; Buccafurri, F.; Furfaro, A.; Graziano, S.; Guzzo, A.; Lax, G.; Pasqua, F.; Saccà, D. ID-Service: A Blockchain-Based Platform to Support Digital-Identity-Aware Service Accountability. *Appl. Sci.* **2020**, *11*, 165. [CrossRef]
6. Costan, V.; Devadas, S. Intel SGX Explained. Available online: https://eprint.iacr.org/2016/086.pdf (accessed on 27 October 2023).
7. Pinto, S.; Santos, N. Demystifying Arm TrustZone: A Comprehensive Survey. *ACM Comput. Surv.* **2019**, *51*, 130. [CrossRef]
8. Thamizhselvan, M.; Raghuraman, R.; Gershon Manoj, S.; Victer Paul, P. A Novel security model for cloud using trusted third party encryption. In Proceedings of the 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 19–20 March 2015; pp. 1–5.
9. Kumar, A. A Cloud-Based Buyer-Seller Watermarking Protocol (CB-BSWP) Using Semi-Trusted Third Party for Copy Deterrence and Privacy Preserving. *Multimed. Tools Appl.* **2022**, *81*, 21417–21448. [CrossRef] [PubMed]
10. Ullah, S.; Li, X.-Y.; Lan, Z. A Novel Trusted Third Party Based Signcryption Scheme. *Multimed. Tools Appl.* **2020**, *79*, 22749–22769. [CrossRef]

11. Jefferies, N.; Mitchell, C.; Walker, M. A Proposed architecture for trusted third party services. In *Cryptography: Policy and Algorithms*; Dawson, E., Golić, J., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, 1996; Volume 1029, pp. 98–104. ISBN 978-3-540-60759-5.
12. Rizvi, S.; Cover, K.; Gates, C. A Trusted Third-Party (TTP) Based Encryption Scheme for Ensuring Data Confidentiality in Cloud Environment. *Procedia Comput. Sci.* **2014**, *36*, 381–386. [CrossRef]
13. Abadi, M.; Glew, N. Certified email with a light on-line trusted third party: Design and implementation. In Proceedings of the 11th International Conference on World Wide Web, Honolulu, HI, USA, 7–11 May 2002; pp. 387–395.
14. Jahan, I.; Sharmy, N.N.; Jahan, S.; Ebha, F.A.; Lisa, N.J. Design of a secure sum protocol using trusted third party system for secure multi-party computations. In Proceedings of the 2015 6th International Conference on Information and Communication Systems (ICICS), Amman, Jordan, 7–9 April 2015; pp. 136–141.
15. Jiang, D.-H.; Hu, Q.-Z.; Liang, X.-Q.; Xu, G.-B. A Trusted Third-Party E-Payment Protocol Based on Locally Indistinguishable Orthogonal Product States. *Int. J. Theor. Phys.* **2020**, *59*, 1442–1450. [CrossRef]
16. Zhou, R.-G.; Huo, M.; Hu, W.; Zhao, Y. Dynamic Multiparty Quantum Secret Sharing with a Trusted Party Based on Generalized GHZ State. *IEEE Access* **2021**, *9*, 22986–22995. [CrossRef]
17. Panda, N.; Supriya, M. Efficient Data Transmission Using Trusted Third Party in Smart Home Environments. *EURASIP J. Wirel. Commun. Netw.* **2022**, *2022*, 118. [CrossRef]
18. Varvitsiotis, A.; Polemi, D.; Marsh, A. EUROMED-JAVA: Trusted third party services for securing medical java applets. In *Computer Security—ESORICS 98*; Quisquater, J.-J., Deswarte, Y., Meadows, C., Gollmann, D., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1998; Volume 1485, pp. 209–220. ISBN 978-3-540-65004-1.
19. Sharma, V.; Thakur, R. LSB modification based audio steganography using trusted third party key indexing method. In Proceedings of the 2015 Third International Conference on Image Information Processing (ICIIP), Waknaghat, India, 21–24 December 2015; pp. 403–406.
20. Hussien, Z.A.; Jin, H.; Abduljabbar, Z.A.; Hussain, M.A.; Abbdal, S.H.; Zou, D. Scheme for ensuring data security on cloud Data storage in a semi-trusted third party auditor. In Proceedings of the 2015 4th International Conference on Computer Science and Network Technology (ICCSNT), Harbin, China, 19–20 December 2015; pp. 1200–1203.
21. Maarouf, A.; Marzouk, A.; Haqiq, A. Towards a trusted third party based on multi-agent systems for automatic control of the quality of service contract in the cloud computing. In Proceedings of the 2015 International Conference on Electrical and Information Technologies (ICEIT), Marrakech, Morocco, 25–27 March 2015; pp. 311–315.
22. Aloqaily, M.; Kantarci, B.; Mouftah, H.T. Trusted third party for service management in vehicular clouds. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; pp. 928–933.
23. Jayasinghe, D.; Markantonakis, K.; Mayes, K. Optimistic fair-exchange with anonymity for bitcoin users. In Proceedings of the 2014 IEEE 11th International Conference on e-Business Engineering, Guangzhou, China, 5–7 November 2014; pp. 44–51.
24. Xu, R.; Li, C.; Joshi, J. Transparent and Trustworthy Third-Party Authority Using Blockchain. Available online: https://arxiv.org/pdf/2102.01249v2.pdf (accessed on 20 November 2023).
25. Li, W.; Wu, J.; Cao, J.; Chen, N.; Zhang, Q.; Buyya, R. Blockchain-based trust management in cloud computing systems: A taxonomy, review and future directions. *J. Cloud Comput.* **2021**, *10*, 35. [CrossRef]
26. Arshad, Q.U.A.; Khan, W.Z.; Azam, F.; Khan, M.K.; Yu, H.; Zikria, Y.B. Blockchain-based decentralized trust management in IoT: Systems, requirements and challenges. *Complex Intell. Syst.* **2023**, *9*, 6155–6176. [CrossRef]
27. Pillai, B.; Biswas, K.; Muthukkumarasamy, V. Cross-chain interoperability among blockchain-based systems using transactions. *Knowl. Eng. Rev.* **2020**, *35*, E23. [CrossRef]
28. PixelPlex. DocFlow. Available online: https://pixelplex.io/doc-flow/ (accessed on 20 November 2023).
29. Scalable Solutions AG. Blockchain for Documentation Management. 2020. Available online: https://scalablesolutions.io/news/blockchain-for-documentation-management/ (accessed on 20 November 2023).
30. Lim, S.Y.; Musa, O.B.; Al-Rimy, B.A.S.; Almasri, A. Trust models for blockchain-based self-sovereign identity management: A survey and research directions. In *Advances in Blockchain Technology for Cyber Physical Systems*; Maleh, Y., Tawalbeh, L., Motahhir, S., Hafid, A.S., Eds.; Internet of Things; Springer: Cham, Switzerland, 2022. [CrossRef]
31. Merlec, M.M.; Islam, M.M.; Lee, Y.K.; In, H.P. A Consortium Blockchain-Based Secure and Trusted Electronic Portfolio Management Scheme. *Sensors* **2022**, *22*, 1271. [CrossRef] [PubMed]
32. Locher, T.; Obermeier, S.; Pignolet, Y.A. When can a distributed ledger replace a trusted third party? In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1069–1077.
33. More, S.; Chaudhari, S. Third Party Public Auditing Scheme for Cloud Storage. *Procedia Comput. Sci.* **2016**, *79*, 69–76. [CrossRef]
34. Bhattacharjya, A.; Kozdrój, K.; Bazydło, G.; Wisniewski, R. Trusted and Secure Blockchain-Based Architecture for Internet-of-Medical-Things. *Electronics* **2022**, *11*, 2560. [CrossRef]
35. Bazydło, G.; Wiśniewski, R.; Kozdrój, K. Trusted and Secure Blockchain-Based Durable Medium Electronic Service. *Cryptography* **2022**, *6*, 10. [CrossRef]

36. Bhattacharjya, A.; Zhong, X.; Wang, J.; Xing, L. A Secure Hybrid RSA (SHRSA)-based lightweight and efficient personal messaging communication protocol. In *Digital Twin Technologies and Smart Cities*; Internet of Things (Technology, Communications and Computing); Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H., Eds.; Springer: Cham, Switzerland, 2020; pp. 191–212. [CrossRef]
37. Bachani, V.; Wan, Y.; Bhattacharjya, A. Preferential DpoS: A Scalable Blockchain Schema for High-Frequency Transaction. AMCIS 2022 TREOs. 36. 2022. Available online: https://aisel.aisnet.org/treos_amcis2022/36 (accessed on 20 November 2023).
38. Bhattacharjya, A. A holistic study on use of Blockchain technology in CPS and IoT architectures with focus on maintaining CIA triad of data communication. *Int. J. Appl. Math. Comput. Sci.* **2022**, *32*, 403–413. [CrossRef]
39. Bhattacharjya, A.; Wisniewski, R.; Nidumolu, V. A holistic research on major Blockchain's Consensus Protocols' working mechanisms with security aspects of CPS. *Electronics* **2022**, *11*, 2760. [CrossRef]
40. Bachani, V.; Bhattacharjya, A. Preferential Delegated Proof of Stake (PDPoS)—Modified DpoS with Two Layers towards Scalability and Higher TPS. *Symmetry* **2023**, *15*, 4. [CrossRef]
41. Platt, M.; McBurney, P. Sybil in the Haystack: A Comprehensive Review of Blockchain Consensus Mechanisms in Search of Strong Sybil Attack Resistance. *Algorithms* **2023**, *16*, 34. [CrossRef]
42. Krichen, M.; Lahami, M.; Al–Haija, Q.A. Formal methods for the verification of smart contracts: A review. In Proceedings of the 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 11–13 November 2022; pp. 1–8. [CrossRef]
43. Abdellatif, T.; Brousmiche, K. Formal verification of smart contracts based on users and blockchain behaviors models. In Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5. [CrossRef]
44. Hyperledger Besu Documentation. Available online: https://besu.hyperledger.org/ (accessed on 27 October 2023).
45. Kushwaha, S.S.; Joshi, S.; Singh, D.; Kaur, M.; Lee, H.N. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract. *IEEE Access* **2022**, *10*, 6605–6621. [CrossRef]