




Article

Blockchain Technologies: Smart Contracts for Consumer Electronics Data Sharing and Secure Payment

Alfred Daniel John William ¹, Santhosh Rajendran ¹, Pradish Pranam ¹, Yosuva Berry ¹, Anuj Sreedharan ¹, Junaid Gul ² and Anand Paul ^{3,*}

¹ Department of Computer Science and Engineering Karpagam Academy of Higher Education, Coimbatore 641021, India

² Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea

³ The School of Computer Science and Engineering, Kyungpook National University, Daegu 41566, Republic of Korea

* Correspondence: paul.editor@gmail.com

Abstract: Blockchain may be an optimal solution when a detailed and transparent record of assets is necessary. It is imperative to manage and safeguard digital interactions or maintain a decentralized and shared system of records in applications, such as those used for electricity production, transmission, distribution, and consumption and those used for data sharing and secure payments. Such applications can benefit from blockchain technology to resolve these problems. In the proposed blockchain-based consumer electronics data sharing and safe payment framework, an innovative IoT meter detects monthly consumption and transmits the data to a decentralized application that is stored in the blockchain. This decentralized platform will generate the bill and provide incentives for legitimate consumers. Finally, the end-to-end latency and throughput were used to evaluate the performance of the proposed approach.

Keywords: smart contract; consumer electronics; blockchain; data sharing; secure payment; dApp



Citation: John William, A.D.; Rajendran, S.; Pranam, P.; Berry, Y.; Sreedharan, A.; Gul, J.; Paul, A. Blockchain Technologies: Smart Contracts for Consumer Electronics Data Sharing and Secure Payment. *Electronics* **2023**, *12*, 208. <https://doi.org/10.3390/electronics12010208>

Academic Editor: Tuan-Vinh Le

Received: 24 November 2022

Revised: 26 December 2022

Accepted: 26 December 2022

Published: 31 December 2022



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Blockchain is a system for storing data in a manner that makes system alterations, hacking, and cheating difficult or impossible [1]. A blockchain is a network of computer systems that duplicates and distributes a digital ledger of transactions across the entire network [2,3]. A blockchain is a decentralized, distributed, and open digital ledger utilized for logging transactions across numerous computers in a way that prevents changes from being made retrospectively without affecting all blocks behind them and the network's consensus [4–8].

In contrast to traditional methods for storing data on third-party computers or servers, often supervised by a single authority, blockchain provides enhanced security concerning consumer electronics data sharing and secure payments. Users can carry out transactions without waiting for banks or credit card companies to authorize them. Because the blockchain is decentralized, there is no single point of failure, increasing its resistance to attacks, and once data is recorded on the blockchain, it cannot be manipulated. Blockchain is often used to secure data sharing because it allows multiple users to share data without a central authority. This makes it an ideal data sharing platform because it is secure, transparent, and immutable.

Blockchain may be the best option for maintaining an extensive, transparent record of assets while maintaining a decentralized shared system of records, or managing and securing digital interactions. In particular, “Smart Contracts” on a blockchain are excellent for streamlining digital interactions and transactions [9], wherein automated payments are released through a smart contract when participants agree that their criteria are satisfied.

Most accommodation providers generally communicate with visitors through a centralized aggregator site [10,11]. Blockchain can alter such application perspectives. For instance, owing to the potential of blockchain technology, travel businesses are developing novel strategies to link guests and hotels directly. This enables them to trade via blockchain in a simple, secure, and reliable manner rather than through a central booking site [12]. Blockchain is a better and safer way to track activity, keep data current, and preserve data history [13]. A traditional database could help keep track of upfront exchanges between both parties; however, under complex conditions, a blockchain can eliminate delays and streamline connections [14–17]. For instance, in the supply chain market, a few private blockchain networks link their numerous partners and clients via a secured blockchain consensus for data sharing and secure payment [18].

Generally, a decentralized system's increased security makes the blockchain perfect for transactions [19–22]. A user benefits from having a historical data record and an instantly updated record; additionally, the data cannot be corrupted by anyone or unintentionally erased [23]. Clearly, the advantage of blockchain technology is substantial concerning consumer electronics. Blockchain offers a higher degree of protection for consumer devices, data sharing, and secure payments [24]. Users can conduct transactions without requiring authorization from banks or credit card issuers. Blockchain's decentralization ensures no vulnerability, increasing its resilience to assaults; moreover, once information is added to the blockchain, it cannot be altered [25–28].

Blockchain is a decentralized, immutable log of transactions comprising a group of independent computer controls [29]. Each data block is protected and connected through cryptographic principles. The Ethereum blockchain aims to build a vast network of personal computers that can independently run internet applications [30–33]. Because Ethereum is programmable, developers can create new types of apps with it, unlike previous blockchains. When specific circumstances are met, smart contracts based on Ethereum automatically transfer virtual currency between the two parties [34]. Simultaneous alerting and open sourcing by all parties prevent the alteration of smart contract codes.

Blockchain technology and smart contracts have recently been used in many applications [35–38]. Although it uses blockchain and cryptocurrency, Ethereum offers a decentralized architecture [39]. However, several challenges exist, including high bandwidth, computational expense, and storage requirements. The proposed system model uses the Ethereum blockchain because programmable smart contracts may accept cryptocurrency and permit owners to withdraw from the consumer electronic perspective [40].

Blockchain has emerged as one of the essential strategies for decentralized cryptocurrency systems. Both academic and industrial circles have shown considerable interest. However, most contemporary blockchain-based systems only handle transactions between parties [41–44]. In several real-world circumstances, a transaction may include multiple entities; if these entities execute their activities according to the rules of the classic blockchain, the communication cost will increase dramatically. This article proposes a blockchain-based safe peer-to-peer multiparty transaction mechanism. Using a technique for exchanging coded information allows numerous users to simultaneously participate in a single transaction [45,46].

On a blockchain, smart contracts store programs that are only activated when specific criteria are met. They are often used to automate the implementation of an agreement to enable all parties to ensure an immediate conclusion without the need for an intermediary or extra delay. They can also automate a workflow, causing subsequent actions to be taken when specific criteria are satisfied. When the predefined conditions are met and validated, a network of computers performs the necessary activities. These can entail data sharing on consumer electronics between B2B and B2C functional models, sending or releasing payments, and providing rewards for valid customers, as shown in Figure 1.

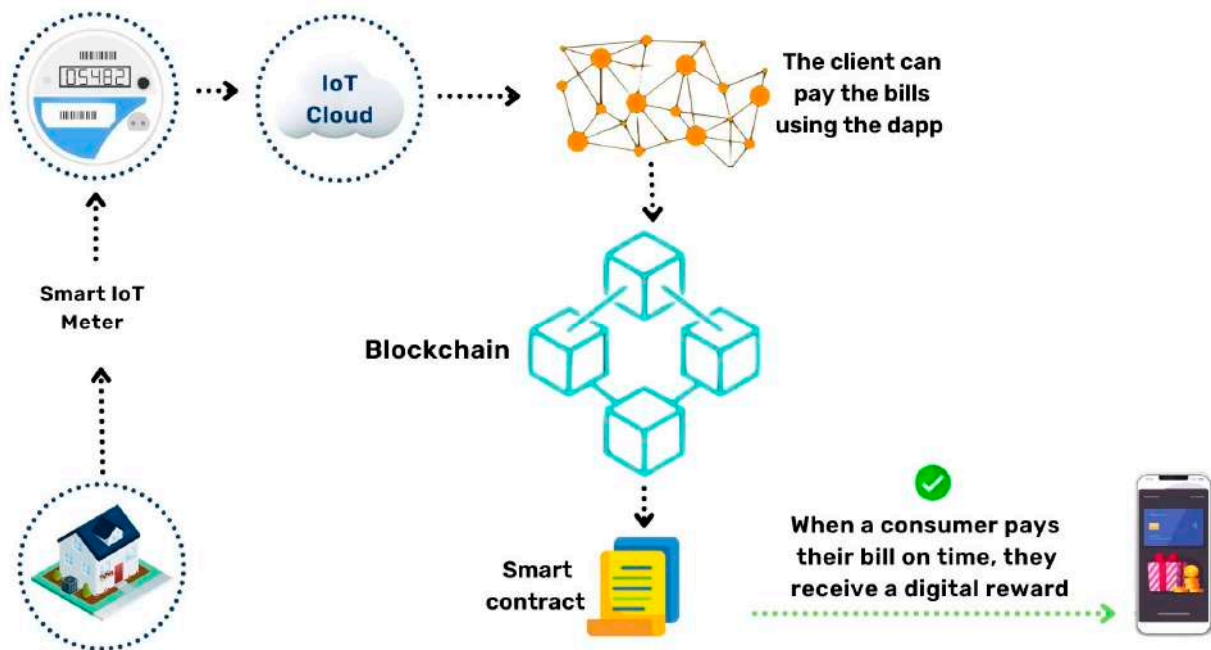


Figure 1. Proposed Blockchain-Based Consumer Electronic Data Sharing and Secure Payment.

After the transaction is completed, the blockchain is updated. Hence it indicates that the transaction is final and only parties to whom permission has been granted can view the outcome. The subsequent stage of a transaction or process is automatically initiated after the specified requirements are satisfied. Thus, with smart contracts, transactions can be automated, enhancing productivity and accelerating the procedure from a consumer electronic application perspective. Smart contracts lessen the need for human intervention and rely less on outside parties to confirm that a contract's provisions have been adhered to for specific applications. For instance, when a consumer files a request to close the connection, the request may be settled and paid once the customer has submitted all the required evidence.

The rest of the article is organized as follows. Section 3 discusses the overview of the proposed Blockchain-based Consumer Electronics for Data Sharing and Secure Payment Framework. Following this, the algorithm for smart contracts for consumer electronics and smart contract interaction with dApp is presented in Section 3. Additionally, the deployment of the stablecoin using ERC-20 for proposed consumer electronics is elaborated in Section 3. The experimental results and performance analysis is discussed in Section 4. Finally, in Section 5, we have the conclusion.

2. Proposed Blockchain-Based Consumer Electronics for Data Sharing and Secure Payment

In the proposed blockchain-based data sharing and secure payment framework for consumer electronics, an innovative IoT meter measures and sends the monthly usage to the decentralized application (dApp), which is stored in the blockchain. This dApp generates a bill and sends it to an IoT cloud. Here, the generated invoice is sent to the consumer, through which they can pay the bill amount using a web3 wallet that contains the stablecoin. Once the transaction is verified, it is stored permanently in the blockchain. Rewards are given to users whenever they pay their bills on time.

The data is stored using cryptography, which encodes the message, allowing only the intended recipient to read it. Generally, this is performed using PGP (Pretty Good Privacy) or GPG (GNU Privacy Guard) [14] encryption standards. It uses a public-key cipher to share a key for the symmetric cipher. The actual data is then encrypted using the key and sent to the recipient. The recipient can use this key to decrypt the data. This removes the need for trust because the data is stored in blocks and cannot be manipulated. The

decentralized nature of blockchain means that there is no central point of control, which makes it more resistant to tampering and corruption. Cryptography also adds a security layer. A blockchain can be used to create a secure and transparent payment system. By using blockchain, payments can be processed quickly and securely without the need for a third party, such as a bank. This could potentially reduce the cost and make them more accessible to everyone. The use of blockchain in payments also has the potential to help mitigate fraudulent activities, such as money laundering. This is because the blockchain provides a permanent and tamper-proof record for all transactions. This could make it easier to track down and prosecute criminals.

Smart contracts enable actions that require gas, which costs ether, the native coin of Ethereum. The more complicated its business logic, the more gas the smart contract must send to the network. This is because the contract's byte code size grows with the source code size. The proposed system uses an Ethereum stable token to avoid high gas prices, and the transaction can be conducted from a wallet to a smart contract.

2.1. Proposed Smart Contracts in Consumer Electronics

Smart contracts are digital contracts that enable collaboration between two or more independent parties. The appeal of a smart contract is that no external or third party is required to supervise the transactions. This has clear advantages in terms of price and speed for data sharing and secure payments in consumer electronic applications, as depicted in Figure 2.

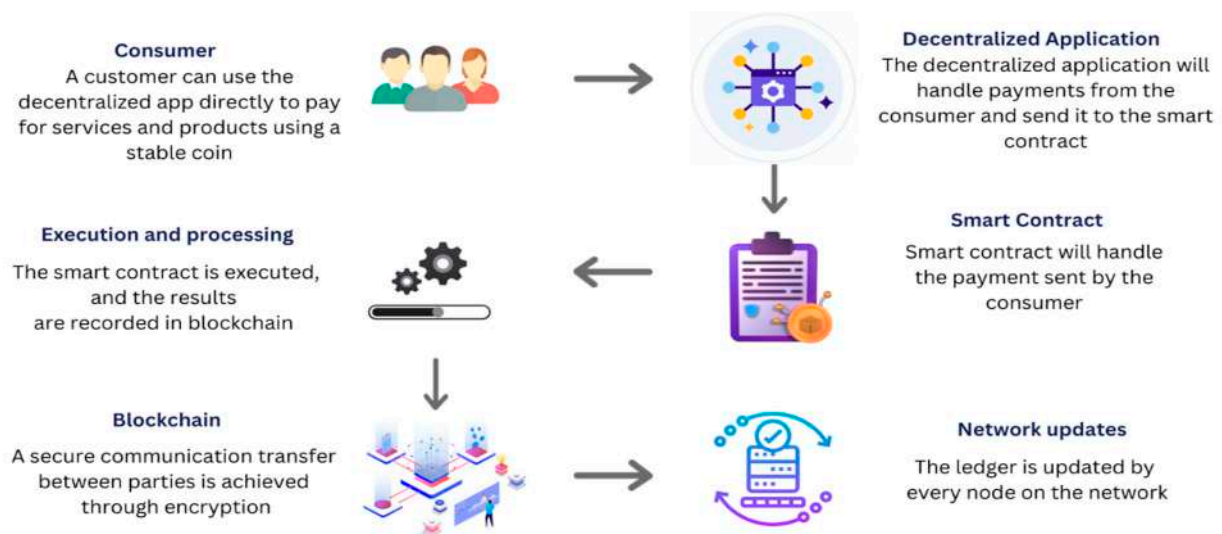


Figure 2. Proposed Smart Contract for Data Sharing and Secure Payment in Consumer Electronic Applications.

2.1.1. Functionalities of Smart Contracts

The following are just a few of the many advantages of smart contracts:

- They can assist in automating procedures and minimizing the demand for manual intervention in consumer electronics.
- Avoiding the need for paper records can contribute to increased efficiency and accuracy in consumer electronics.
- They can help reduce consumer electronics expenses by eliminating the need for middlemen.
- They can aid in accelerating transactions by offering a clear and impenetrable record of transactions. Further, the smart contract can assist in lowering the risk associated with consumer electronics.

Smart contracts enable trusted transactions and agreements between dispersed and anonymous parties without necessitating a centralized authority, a legal system, or an

external enforcement mechanism. In a smart contract, the conditions of the agreement between the buyer and seller are directly encoded into lines of code, making it a self-executing contract. The agreements and underlying codes are spread throughout the decentralized blockchain network. Transactions are traceable and irreversible, and the code regulates their execution. The tokens sent by customers are held in an executable token storage system called a smart contract. When a customer uses a decentralized application to pay a bill, the asset is immediately transmitted to the smart contract, from which the owner can withdraw at any time.

Building an application on Ethereum requires a contract, a fundamental building component, as mentioned in Figure 3. The smart contracts are how Solidity's code is contained. Therefore, a contract in Solidity is a group of functions and state-related data stored at a particular address on the Ethereum blockchain. The entire quantity of cryptocurrency that can be withdrawn for each entity can be divided using specific functions that can be placed into smart contracts. Wallets are frequently used to store cryptocurrencies; however, in this framework, smart contracts are employed instead because they interact directly with dApp. Therefore, they are safer to use to store cryptocurrencies than wallets. Hacking into cryptocurrency wallets is possible, but it is impossible to hack into smart contracts.

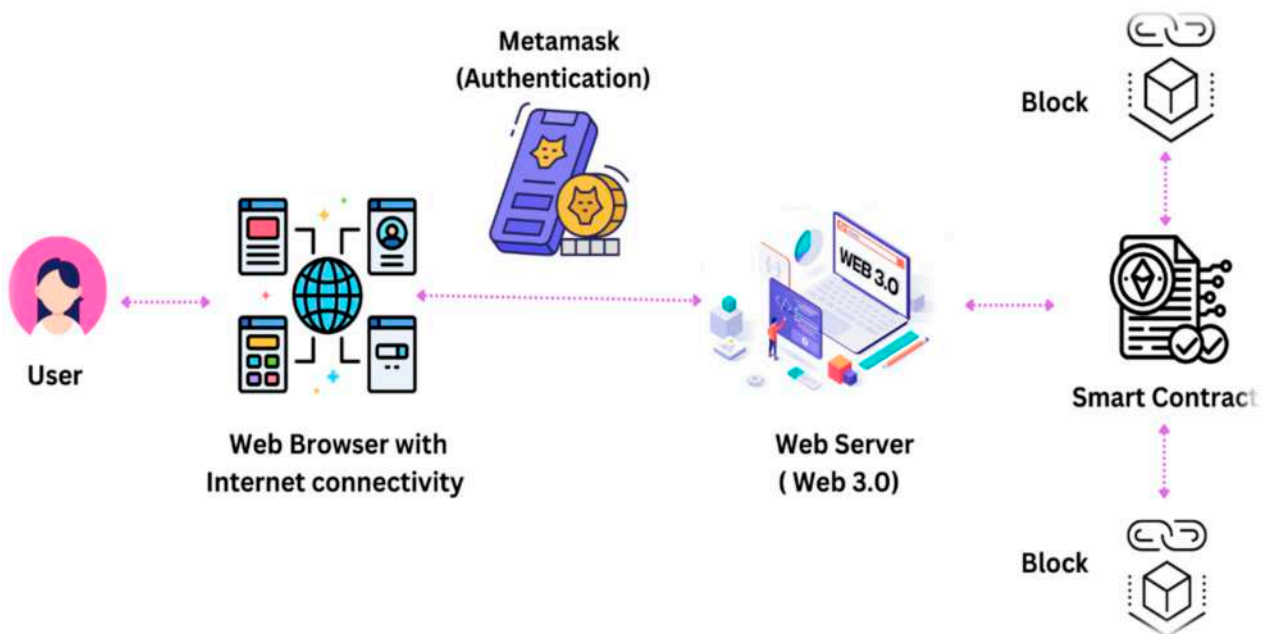


Figure 3. Interaction of dApp and Smart Contract for Consumer Electronics.

The two main functions in the suggested smart contract are:

1. Withdraw
2. Receive

2.1.2. Withdraw() Function

A specific corporate organization may stipulate the number of wallet addresses that can withdraw cryptocurrency by defining this function. It is one of the primary functions of data sharing and securing payment for a consumer application framework.

2.1.3. Receive() Function

The receive() function is one of the most critical roles for the consumer application framework concerning the safe exchange of data and processing of payments. By defining this function, any consumer may pay for a product or bill by transferring cryptocurrency to the smart contract via dApp. The following algorithm illustrates smart contracts concerning consumer electronics.

2.1.4. Algorithm for Withdraw() and Receive() Functions

1. Define the withdraw and receive functions in the smart contract.
2. In the withdraw function, retrieve the sender's account balance from the contract's storage.
3. Check if the sender has enough funds to complete the withdrawal. If not, return an error message.
4. If the sender has sufficient funds, calculate the amount to be withdrawn and subtract it from the sender's balance.
5. The receive function retrieves the recipient's account balance from the contract's storage.
6. Add the amount received to the recipient's balance.
7. Update the contract's storage with the updated balances for the sender and recipient.
8. Return a success message to indicate that the withdrawal and receiving operations were completed successfully.

This algorithm outlines a method for implementing withdraw and receive functions in an Ethereum smart contract. The withdraw function retrieves the sender's account balance and checks if they have sufficient funds. If so, it calculates the amount to be withdrawn and updates the contract's storage with the updated balances for the sender and recipient. The receive function retrieves the recipient's account balance, adds the amount received, and updates the repository. It would return a success message if the operations were completed successfully. This algorithm provides a secure and accurate way to manage funds transferred between accounts in a smart contract.

2.2. *dApp for Consumer Electronics*

A distributed open-source software program known as a "decentralized application" (dApp) runs on a peer-to-peer (P2P) blockchain network as opposed to a single computer. dApps are comparable to other software programs used on websites or mobile devices but feature P2P. Due to the decentralized structure of dApps, others are free to build on top of a developer's public codebase. The application is not under the administration of a single body.

Applications for decentralized finance, online browsing, gaming, and social media are only a few of the many dApps that can be developed. The dApps are constructed on a decentralized network backed by a distributed ledger called a blockchain. A dApp can process data through distributed networks and conduct transactions using a blockchain. dApps are frequently developed on the Ethereum platform. dApps have gained popularity owing to distributed ledger technologies such as the Ethereum blockchain. One of their main advantages is that dApps are always accessible and do not have a single point of failure. In the proposed paradigm, dApps, through which users may use their crypto tokens to pay their bills, play a significant role. A smart meter delivers a reading to the cloud storage and sends this information to the dApp. A user with a private key can pay bills using the dApp, which calculates the amount of cryptocurrency that has to be paid. After payment, the user's data is automatically erased from the dApp, making it more private. The transaction hash, which includes the date, time, transaction ID, number of assets sent, and receiver's privacy key, can be used to confirm that the user has paid the bill.

2.3. *Interaction of dApp and Smart Contract for Consumer Electronics*

Consumers can access decentralized applications (dApps) by using a browser with an internet connection. To use a dApp, the user must first log in using an Ethereum wallet such as MetaMask or Rainbow. These wallets allow the consumers to interact with the Ethereum blockchain and perform actions such as sending and receiving Ethereum and other tokens. Once the consumers are logged in to the dApp using their Ethereum wallet, they can begin using its various features. These may include fetching data from a web server, retrieving consumer bills from the blockchain, and storing other data in the Ethereum blockchain.

A smart meter is a device that measures and records the consumption of electricity, gas, or other utilities. To use a smart meter with a blockchain-based billing system, the owner of the meter must have reliable internet access and a cryptocurrency wallet. The dApp allows the owner of the smart meter to interact with a smart contract, which is a self-executing contract with the terms of the agreement between the meter owner and the utility provider written into lines of code. The smart contract can automate the billing process, allowing the meter owner to pay their bills using a stablecoin, a type of cryptocurrency pegged to a stable asset such as the U.S. dollar. The block containing the current transaction must be validated to complete the transaction. This means that the network must verify the block to ensure that it meets the requirements of the blockchain protocol and contains valid transactions. The transaction will be approved and added to the blockchain if the block is successfully validated. The transaction will not be processed or added to the blockchain if the block is not validated.

The default method of interacting with contracts in the Ethereum ecosystem, both from outside the blockchain and for contract-to-contract communication and communication with a dApp, is the Contract Application Binary Interface (ABI). This defines how data is encoded in accordance with its type. As encoding is not self-descriptive, a schema must be used to decode it. We assume that a contract's interface functions are strongly typed, predetermined at compilation time, and static. We assume that all contracts have access to the interface definitions of any contracts they call at build time, as shown in Figure 3. This specification does not cover contracts whose interface is dynamic or otherwise only known at runtime.

Pseudocode for Interacting Smart Contracts with dApps

1. The dApp sends a request to the blockchain network requesting access to the smart contract.
2. The network validates the request and grants access to the dApp if it is deemed valid.
3. The dApp interacts with the smart contract by calling its functions and passing necessary arguments.
4. The smart contract processes the request and performs the appropriate actions, such as updating its internal state or triggering other smart contracts.
5. The dApp receives a response from the smart contract indicating the result of the interaction.
6. The dApp updates its user interface to display the interaction results.
7. The dApp continues to interact with the smart contract, allowing the user to perform a wide range of actions within the decentralized application.

The dApp allows users to pay for goods and services directly using a stable token that adheres to the ERC-20 [4] standard. A web3 wallet, such as MetaMask [43], Rainbow [43], or Exodus [43], will be used by the customer to make payments to the decentralized application, which will then send the transaction to the smart contract. The smart contract then verifies the transaction, and the payment is sent to the merchant. This transactional data is encrypted using GPG/PGP and stored on the blockchain permanently. Each blockchain node is updated if the transaction is successful.

3. Deployment of the Stablecoin Using ERC-20

A stablecoin is a type of cryptocurrency designed to maintain a stable value, unlike most highly volatile cryptocurrencies. The value of stablecoin is typically fixed to a stable asset, for example, a fiat currency such as the U.S. dollar. This means that the value of the stablecoin will remain relatively stable, even if the value of other cryptocurrencies fluctuates. Stablecoins are often used to store value and make transactions, especially in situations where the volatility of other cryptocurrencies would be undesirable. The Ethereum blockchain network, used to create tokens, has become the de facto technical standard for building smart contracts. All tokens built on Ethereum must adhere to a set of guidelines called ERC-20. Tokens are assets built on the blockchain that may be

transmitted and received and have value, according to ERC-20. ERC-20 tokens share many characteristics with Bitcoin [4] and Litecoin [4]. The main distinction is that ERC-20 currencies employ gas as the transaction cost and utilize Ethereum's blockchain network instead of its own. The ERC-20 standard governs token development. A user begins by giving their token a name and symbol and mentioning its decimal level of divisibility. A smart contract must implement the functionalities listed in the standard. The ERC defines the following more complicated necessary functions, which are described below:

- Total Supply: A method that specifies the overall supply of a user's tokens; once achieved, the smart contract forbids the creation of additional tokens.
- Balance of: This method returns the number of tokens stored at a wallet address.
- Transfer: This technique involves taking specific tokens out of circulation and giving them to the user.
- Approve: Considering the overall supply, this approach determines whether a smart contract is authorized to provide a user with a specific number of tokens.
- Allowance: This technique is precisely the same as the accepted method, except that it also determines whether a user has a sufficient balance between giving another user a specific number of tokens.

Smart Contract and ERC-20 Interface Algorithm

1. The contract creator sets the initial supply of the stablecoin and the price at which it is fixed through a stable asset, such as U.S. currency.
2. A user can purchase the stablecoin by sending the appropriate amount of the stable asset to the smart contract.
3. The smart contract automatically mints the corresponding amount of stablecoins and sends them to the user's wallet.
4. A user can redeem their stablecoins for the stable asset by sending the stablecoins to the smart contract.
5. The smart contract automatically calculates the redemption amount and sends the corresponding amount of the stable asset to the user's wallet.
6. The smart contract updates its internal state to reflect the current supply and price of the stablecoin.
7. The contract creator can adjust the price of the stablecoin if necessary to maintain its peg to the stable asset.

This process is depicted in Figure 4.

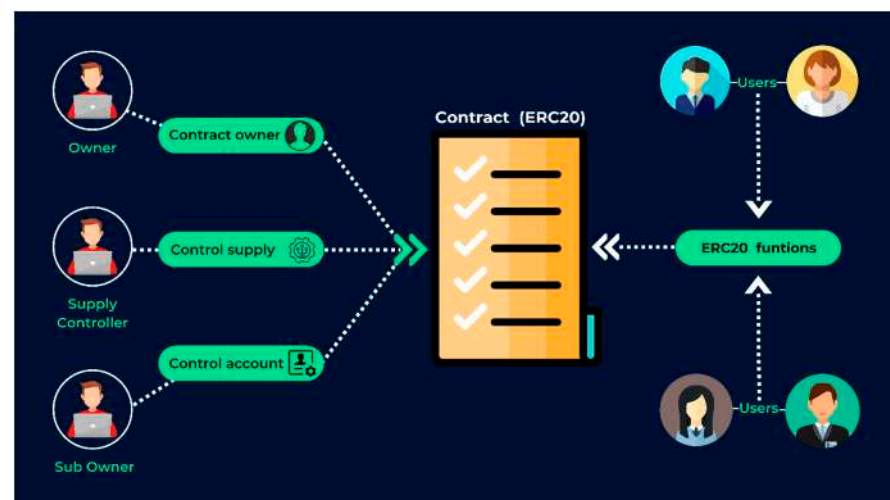


Figure 4. Contract ERC-20 Interface.

4. Performance Analysis

The performance of the proposed blockchain-based consumer electronic data sharing and secure payment framework is evaluated based on end-to-end latency and throughput metrics. The analysis is determined based on the existing framework [47] without blockchain and the proposed framework with a blockchain mechanism. The existing architecture makes use of an internet of things (IoT) smart energy meter, which monitors energy use by way of a GSM module. By this method we receive up-to-date information on the amount of energy that has been used without the influence of blockchain. The end-to-end latency is minimal compared to the existing model. The latency of Ethereum transactions from inception to delivery is determined by two factors: the transaction fee that the sender must pay to the mining communities in the form of gas and the volume of transactions that the mining communities must meet. Therefore, end-to-end latency decreases as gas costs keep rising. This indicates that offering higher gas costs would bring greater service quality, which implies that transactions are more likely to be verified with fewer delays with respect to consumer electronic data sharing and a secure payment framework. Hence, in relation to end-to-end latency, the proposed blockchain Based Consumer Electronic Data Sharing and Secure Payment Framework latency is minimal compared to the existing method [47], as mentioned in Figure 5.

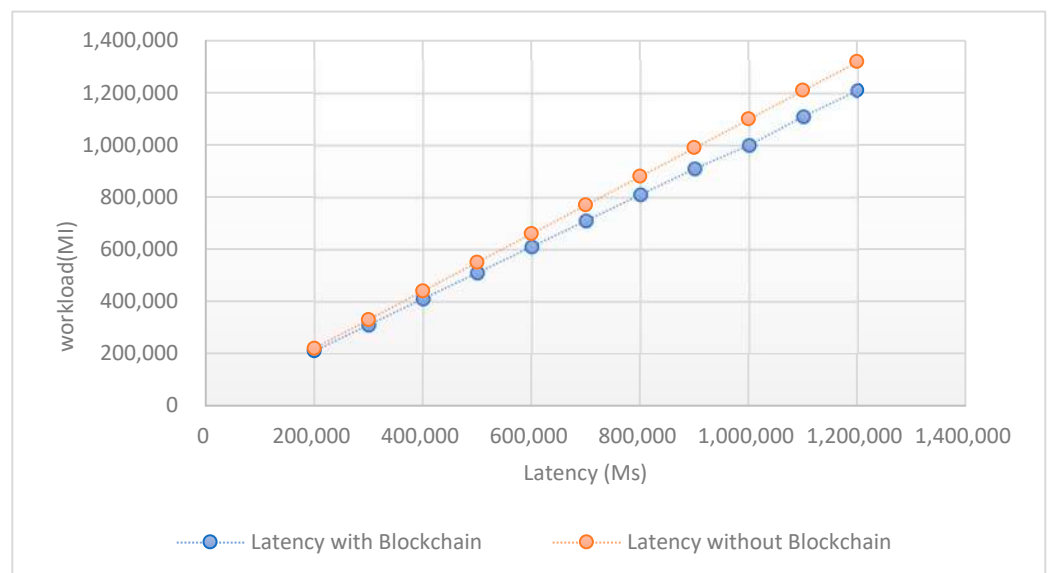


Figure 5. End-to-End Latency.

End-to-end throughput is the essential factor that can affect the total efficiency of the network. In the proposed framework, when a transaction has to be verified, it must first be broadcast to all the nodes, and then the responses from those nodes must be compiled to reach a consensus based on a majority vote. As a result, the suggested architecture, which includes a dedicated network capacity, significantly reduces the time the network takes to process data and increases its total throughput as mentioned in Figure 6. On comparing full workload vs. throughput, the proposed model outperforms the existing model [47] regarding end-to-end throughput.

Moreover, the performance of the proposed model is determined based on the access control mechanism and the data query operations by comparing the conventional data sharing method with the blockchain-enabled data sharing process concerning consumer electronics. Compared to the existing method [47] of data sharing, the blockchain-enabled process will increase the amount of computation and network communication overhead, as illustrated in Figures 7 and 8. This is because the blockchain-enabled system necessitates a lengthy and time-consuming encoding procedure and a transactional consensus latency.

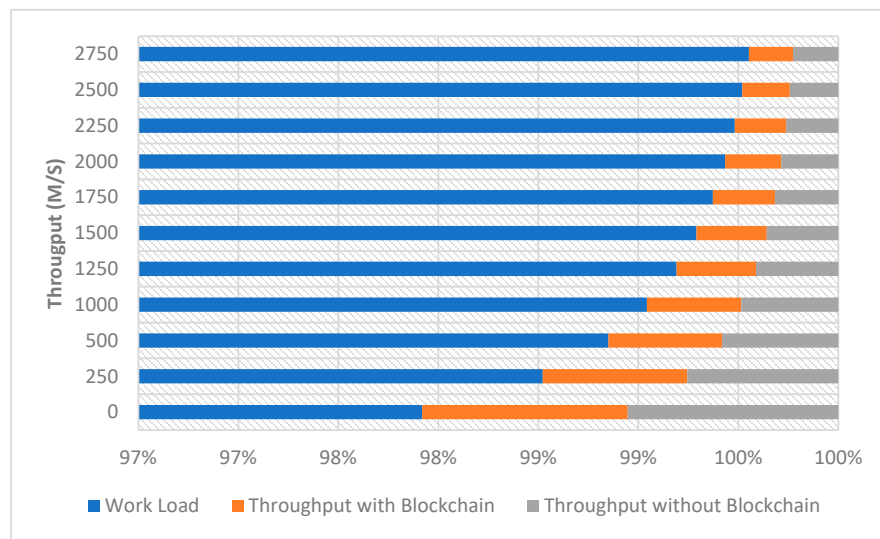


Figure 6. End-to-End Throughput.

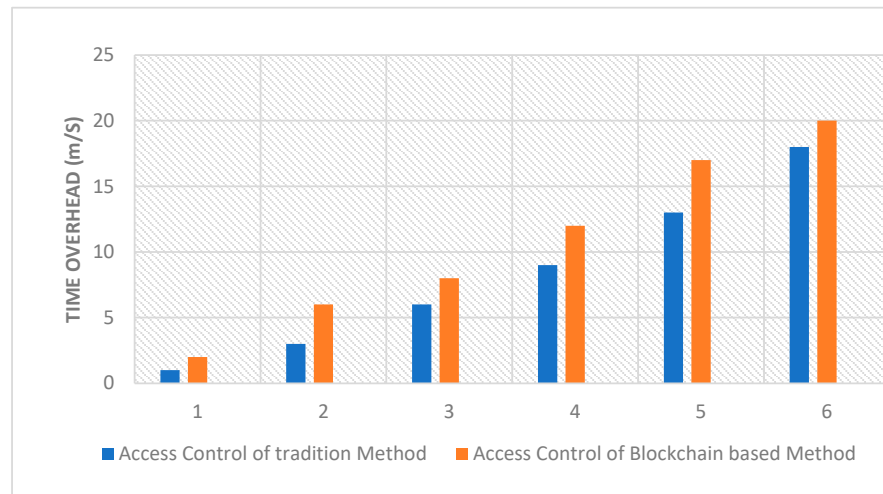


Figure 7. Comparison of Access Control.

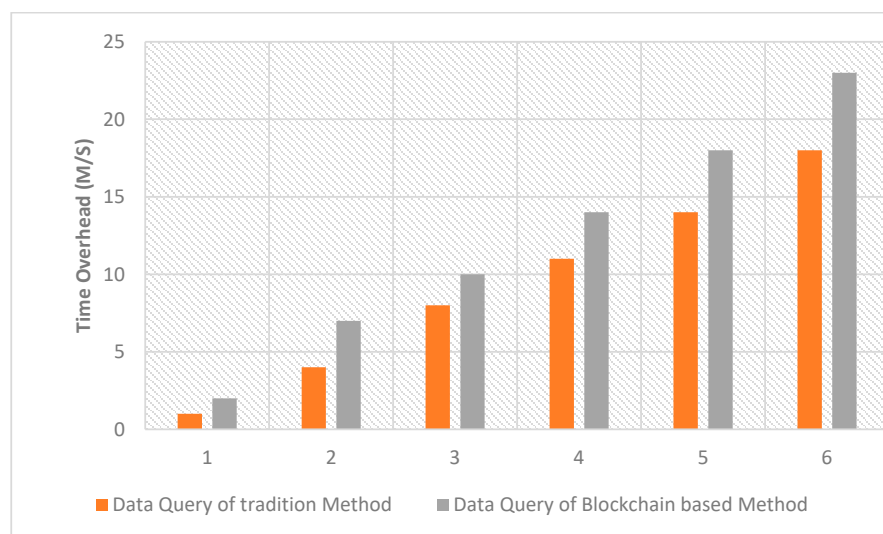


Figure 8. Comparison of Data Query.

The additional cost caused by the blockchain-enabled approach is estimated to be 50 ms in the most extreme scenario for the information-stored operation. An additional time overhead of 10 ms is caused by the access control method and data query operation.

5. Conclusions

With increasing data sharing and financial transactions online, it is necessary to manage and protect these digital interactions as well as keep a distributed and shared system of records. Blockchain technology could be the best option for maintaining a comprehensive and open record of assets. Multiple applications, such as those used for electricity production, transmission, distribution, and consumption, and those with data sharing and secure payment frameworks, can benefit from utilizing blockchain technology to resolve existing issues. Blockchain technology can also be used to assist in the development of new solutions. A cutting-edge IoT meter gathers information about monthly consumption and sends it to a decentralized application. The information is then saved in the blockchain as part of the framework proposed for blockchain-based consumer electronics data sharing and secure payment. This decentralized platform will create a bill and incentivize customers to use the service. Finally, the performance of the proposed model was evaluated based on end-to-end latency and throughput. It demonstrated minimal latency and high throughput compared to the existing model [47]. Further work would incorporate a gamification framework that offers an irreversible and impartial ledger with a standard format in which contributions may be certified, a reward system based on quantifiable successes, and a worldwide and verifiable assessment of these achievements for approval by the organization's stakeholders.

Author Contributions: Conceptualization, A.P.; Methodology, P.P. and A.P.; Software, Y.B. and A.S.; Validation, A.D.J.W.; Formal analysis, A.D.J.W.; Investigation, S.R.; Resources, S.R.; Data curation, S.R. and J.G.; Writing—original draft, P.P., Y.B. and A.S.; Visualization, J.G.; Supervision, A.D.J.W.; Project administration, A.P.; Funding acquisition, A.P. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by BK21 Four Project, AI-Driven Convergence Software Education Research Program 4199990214394 2. And also supported by National Research Foundation of Korea 2020R1A2C101 2196.

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

References

1. Bistarelli, S.; Mazzante, G.; Micheletti, M.; Mostarda, L.; Tiezzi, F. Analysis of Ethereum Smart Contracts and Opcodes. In *Advanced Information Networking and Applications*; Barolli, L., Takizawa, M., Xhafa, F., Enokido, T., Eds.; Advances in Intelligent Systems and Computing; AINA 2019; Springer: Cham, Germany, 2019; Volume 926. [\[CrossRef\]](#)
2. Huh, S.; Cho, S.; Kim, S. Managing IoT Devices using Blockchain Platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Republic of Korea, 19–22 February 2017.
3. Hlaing, K.M.; Nyaung, D.E. Electricity Billing System using Ethereum and Firebase. In Proceedings of the 2019 International Conference on Advanced Information Technologies (ICAIT), Yangon, Myanmar, 6–7 November 2019; pp. 217–221. [\[CrossRef\]](#)
4. Wood, G. Ethereum: A secure decentralized generalized transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
5. Pee, S.J.; Nans, J.H.; Jans, J.W. A simple blockchain-based peer-to-peer water trading system leveraging smart contracts. In Proceedings of the International Conference on Internet Computing (ICOMP), Las Vegas, NV, USA, 26 April 2019; The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), pp. 63–68.
6. Gür, A.Ö.; Öksüzler, Ş.; Karaarslan, E. Blockchain Based Metering and Billing System Proposal with Privacy Protection for the Electric Network. In Proceedings of the 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), Istanbul, Turkey, 25–26 April 2019; pp. 204–208. [\[CrossRef\]](#)
7. Albrecht, S.; Reichert, S.; Schmid, J.; Strucker, J.; Neumann, D.; Fridgen, G. Dynamics of Blockchain Implementation—A Case Study from the Energy Sector. In Proceedings of the 51st Hawaii International Conference on System Sciences, Hilton Waikoloa Village, HI, USA, 3–6 January 2018.
8. Adeyemi, A.; Yan, M.; Shahidehpour, M.; Botero, C.; Guerra, A.V.; Gurung, N.; Paaso, A. Blockchain technology applications in power distribution systems. *Electr. J.* **2020**, *33*, 106817. [\[CrossRef\]](#)
9. Ma, Z.; Jiang, M.; Gao, H.; Wang, Z. Blockchain for digital rights management. *Future Gener. Comput. Syst.* **2018**, *89*, 746–764.

10. Gul, M.J.J.; Paul, A. IoT Geography Chain: Blockchain-Based Solution for Logistics Ecosystem. In *The Fifth International Conference on Safety and Security with IoT*; Springer: Cham, Germany, 2023; pp. 191–194.
11. Bhadoria, R.S.; Das, A.P.; Bashar, A.; Zikria, M. Implementing Blockchain-Based Traceable Certificates as Sustainable Technology in Democratic Elections. *Electronics* **2022**, *11*, 3359. [[CrossRef](#)]
12. Butt, G.Q.; Sayed, T.A.; Riaz, R.; Rizvi, S.S.; Paul, A. Secure Healthcare Record Sharing Mechanism with Blockchain. *Appl. Sci.* **2022**, *12*, 2307. [[CrossRef](#)]
13. Shrestha, A.K.; Vassileva, J. Blockchain-Based Research Data Sharing Framework for Incentivizing the Data Owners. In *International Conference on Blockchain*; Springer: Cham, Switzerland, 2018; pp. 259–266.
14. Wu, A.; Zhang, Y.; Zheng, X.; Guo, R.; Zhao, Q.; Zheng, D. Efficient and privacy-preserving traceable attribute-based encryption in blockchain. *Ann. Telecommun.* **2019**, *74*, 401–411. [[CrossRef](#)]
15. Zhang, Z.; Zhao, L. A Design of Digital Rights Management Mechanism Based on Blockchain Technology. In *International Conference on Blockchain*; Springer: Cham, Switzerland, 2018; pp. 32–46.
16. Zhu, L.; Wu, Y.; Gai, K.; Choo, K.K.R. Controllable and trustworthy blockchain-based cloud data management. *Future Gener. Comput. Syst.* **2019**, *91*, 527–535. [[CrossRef](#)]
17. Bisht, D.; Singh, R.; Gehlot, A.; Akram, S.V.; Singh, A.; Montero, E.C.; Priyadarshi, N.; Twala, B. Imperative Role of Integrating Digitalization in the Firms Finance: A Technological Perspective. *Electronics* **2022**, *11*, 3252. [[CrossRef](#)]
18. Li, J.; Wu, J.; Chen, L. Block-secure: Blockchain based scheme for secure P2P cloud storage. *Inf. Sci.* **2018**, *465*, 219–231. [[CrossRef](#)]
19. Li, J.; Wang, X.; Huang, Z.; Wang, L.; Xiang, Y. Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing. *J. Parallel Distrib. Comput.* **2019**, *130*, 91–97. [[CrossRef](#)]
20. Xia, Q.I.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [[CrossRef](#)]
21. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Comput. Secur.* **2018**, *78*, 126–142. [[CrossRef](#)]
22. Gao, X.; Zhang, W.; Zhao, B.; Zhang, J.; Wang, J.; Gao, Y. Product Authentication Technology Integrating Blockchain and Traceability Structure. *Electronics* **2022**, *11*, 3314. [[CrossRef](#)]
23. Chen, Y.; Li, H.; Li, K.; Zhang, J. An improved P2P file system scheme based on IPFS and Blockchain. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2017; pp. 2652–2657.
24. Liang, W.; Tang, M.; Long, J.; Peng, X.; Xu, J.; Li, K.C. A Secure Fabric Blockchain-based Data Transmission Technique for Industrial Internet-of-Things. *IEEE Trans. Ind. Inform.* **2019**, *15*, 358–3592. [[CrossRef](#)]
25. Steichen, M.; Fiz Pontiveros, B.; Norvill, R.; Shbair, W. Blockchain-Based, Decentralized Access Control for IPFS. In Proceedings of the 2018 IEEE International Conference on Blockchain (Blockchain-2018), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1499–1506.
26. Gaby, G.; Chandra, L.; Enderson, T. Towards Secure Interoperability between Heterogeneous Blockchains Using Smart Contracts. In Proceedings of the Future Technologies Conference (FTC), Vancouver, BC, Canada, 15–16 November 2017; pp. 73–81.
27. Novo, O. Blockchain meets iot: An architecture for scalable access management in iot. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. [[CrossRef](#)]
28. Zhang, Y.; Kasahara, S.; Shen, Y.; Jiang, X.; Wan, J. Smart contract-based access control for the internet of things. *IEEE Internet Things J.* **2019**, *6*, 1594–1605. [[CrossRef](#)]
29. Khan, N.; Aljoaey, H.; Tabassum, M.; Farzamnia, A.; Sharma, T.; Tung, Y.H. Proposed Model for Secured Data Storage in Decentralized Cloud by Blockchain Ethereum. *Electronics* **2022**, *11*, 3686. [[CrossRef](#)]
30. Park, A.; Li, H. The Effect of Blockchain Technology on Supply Chain Sustainability Performances. *Sustainability* **2021**, *13*, 1726. [[CrossRef](#)]
31. Kumar, A.; Abhishek, K.; Nerurkar, P.; Ghalib, M.R.; Shankar, A.; Cheng, X. Secure smart contracts for cloud-based manufacturing using Ethereum blockchain. *Trans. Emerg. Telecommun. Technol.* **2020**, *33*, e4129. [[CrossRef](#)]
32. Taha, A.; Zakaria, A.; Kim, D.; Suri, N. Decentralized Runtime Monitoring Approach Relying on the Ethereum Blockchain Infrastructure. In Proceedings of the 2020 IEEE International Conference on Cloud Engineering (IC2E), Sydney, Australia, 21–24 April 2020; pp. 134–143.
33. Awadallah, R.; Samsudin, A.; Teh, J.S.; Almazrooie, M. An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain. *IEEE Access* **2021**, *9*, 69513–69526. [[CrossRef](#)]
34. Xu, D.; Yang, Q. The Systems Approach and Design Path of Electronic Bidding Systems Based on Blockchain Technology. *Electronics* **2022**, *11*, 3501. [[CrossRef](#)]
35. Mahmood, Z.; Jusas, V. Blockchain-Enabled: Multi-Layered Security Federated Learning Platform for Preserving Data Privacy. *Electronics* **2022**, *11*, 1624. [[CrossRef](#)]
36. Batool, A.; Byun, Y. Reduction of Online Fraudulent Activities in Freelancing Sites Using Blockchain and Biometric. *Electronics* **2022**, *11*, 789. [[CrossRef](#)]
37. Oad, A.; Razaque, A.; Tolemyssov, A.; Alotaibi, M.; Alotaibi, B.; Zhao, C. Blockchain-Enabled Transaction Scanning Method for Money Laundering Detection. *Electronics* **2021**, *10*, 1766. [[CrossRef](#)]
38. Srinivasu, P.N.; Bhoi, A.K.; Nayak, S.R.; Bhutta, M.R.; Woźniak, M. Blockchain Technology for Secured Healthcare Data Communication among the Non-Terminal Nodes in IoT Architecture in 5G Network. *Electronics* **2021**, *10*, 1437. [[CrossRef](#)]

39. Buccafurri, F.; De Angelis, V.; Lazzaro, S. A Blockchain-Based Framework to Enhance Anonymous Services with Accountability Guarantees. *Future Internet* **2022**, *14*, 243. [[CrossRef](#)]
40. Liang, X.; Shetty, S.; Tosh, D.K.; Kamhoua, C.A.; Kwiat, K.A.; Njilla, L. ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. In Proceedings of the 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Madrid, Spain, 14–17 May 2017; pp. 468–477.
41. Hong, H.; Sun, Z. A secure peer to peer multiparty transaction scheme based on blockchain. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 1106–1117. [[CrossRef](#)]
42. Hong, H.; Sun, Z. A flexible attribute-based data access management scheme for sensor-cloud system. *J. Syst. Archit.* **2021**, *119*, 102234. [[CrossRef](#)]
43. Suratkar, S.; Shirole, M.; Bhirud, S. Cryptocurrency Wallet: A Review. In Proceedings of the 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 22–23 April 2020; pp. 1–7. [[CrossRef](#)]
44. Thapliyal, H. Internet of Things-Based Consumer Electronics: Reviewing Existing Consumer Electronic Devices, Systems, and Platforms and Exploring New Research Paradigms. *IEEE Consum. Electron. Mag.* **2018**, *7*, 66–67. [[CrossRef](#)]
45. Caldarola, F.; d’Atri, G.; Zanardo, E. Neural Fairness Blockchain Protocol Using an Elliptic Curves Lottery. *Mathematics* **2022**, *10*, 3040. [[CrossRef](#)]
46. Hamledari, H.; Fischer, M. Role of blockchain-enabled smart contracts in automating construction progress payments. *J. Leg. Aff. Disput. Resolut. Eng. Constr.* **2021**, *13*, 04520038. [[CrossRef](#)]
47. Deny, J.; Narasimha, A.; Reddy, R.V.; Sathish, S. Electricity Monitoring and Auto Bill Generation Using IOT. In Proceedings of the 2021 3rd International Conference on Signal Processing and Communication (ICPSC), Coimbatore, India, 13–14 May 2021; pp. 695–698. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.