future internet

MDPI

Article

Low Power Blockchained E-Vote Platform for University Environment

Faten Chaabane [1], Jalel Ktari [2], Tarek Frikha [2,*] and Habib Hamam [3,4,5,6]

[1] Computer Sciences Department, ENIS, University of Sfax, Sfax 3029, Tunisia
[2] CES Lab, ENIS, University of Sfax, Sfax 3029, Tunisia
[3] Faculty of Engineering, Uni de Moncton, Moncton, NB E1A3E9, Canada
[4] Spectrum of Knowledge Production & Skills Development, Sfax 3027, Tunisia
[5] International Institute of Technology and Management, Libreville BP1989, Gabon
[6] Department of Electrical and Electronic Engineering Science, School of Electrical Engineering, University of Johannesburg, Johannesburg 2006, South Africa
* Correspondence: tarek.frikha@enis.tn

Abstract: With the onset of the COVID-19 pandemic and the succession of its waves, the transmission of this disease and the number of deaths caused by it have been increasing. Despite the various vaccines, the COVID-19 virus is still contagious and dangerous for affected people. One of the remedies to this is precaution, and particularly social distancing. In the same vein, this paper proposes a remote voting system, which has to be secure, anonymous, irreversible, accessible, and simple to use. It therefore allows voters to have the possibility to vote for their candidate without having to perform the operation on site. This system will be used for university elections and particularly for student elections. We propose a platform based on a decentralized system. This system will use two blockchains communicating with each other: the public Ethereum blockchain and the private Quorum blockchain. The private blockchain will be institution-specific. All these blockchains send the necessary data to the public blockchain which manages different data related to the universities and the ministry. This system enables using encrypted data with the SHA-256 algorithm to have both security and information security. Motivated by the high energy consumption of blockchain and by the performance improvements in low-power, a test is performed on a low-power embedded platform Raspberry PI4 showing the possibility to use the Blockchain with limited resources.

Keywords: E-vote platform; blockchain; Quorum; Ethereum; embedded system; Raspberry PI 4

Citation: Chaabane, F.; Ktari, J.; Frikha, T.; Hamam, H. Low Power Blockchained E-Vote Platform for University Environment. *Future Internet* **2022**, *14*, 269. https://doi.org/10.3390/fi14090269

Academic Editor: Massimo Cafaro

Received: 19 August 2022
Accepted: 16 September 2022
Published: 19 September 2022

1. Introduction

Blockchain technology has become secure, irreversible, anonymous and impossible to hack. Blockchain is based on decentralized registers. It allows encrypting data by transforming them into encrypted transactions and save them in blocks. After being mined, these blocks are added to the Blockchain and by then they become irreversible and impossible to modify by anyone. Blockchain is used for several types of applications in different fields such as e-health [1–3], industry [4–6], agriculture [7,8] as well as the academic field [9,10]. In this paper, blockchain will serve as an information backup system. In fact, the voting operation is a data-saving operation. Each voter chooses the person for whom they will cast their vote. Thus, each voting operation could be represented by a transaction recorded in the blockchain. This operation enables securing the vote and to maintain traceability while recording the attributed vote. Therefore, it could be said that the Blockchain is certainly a guarantor of the security of the system as well as a system of safeguarding information in our use case

The application straddles the social and academic domains. It is about implementing a system that enables remote voting. This voting operation will be performed in a university

setting. As a case study, the remote voting of the student representative within the university will be selected. This system is made to allow the security and the digitalization of the university operations in Tunisia. Indeed, among the national objectives we can cite the security of citizens in this period of the COVID-19 pandemic. This securitization requires the distancing and the valorization of remote work. To face this challenge, digitization turned out to be the best way to be implemented in the different ministries and particularly in the university education. The main elements of originality may be summarized as follows: A platform based on two Blockchains, namely a private Blockchain (Ethereum) and a public Blockchain (Quorum), is suggested.

− This system will allow students to vote remotely in order to elect their representative.
− It is a secure system by design (Blockchain) and by mobility (remote voting).
− The result which minimizes the risk of error or fraud is generated automatically.

Apart from the introduction, the remaining of this paper is structured as follows. In Section 2, we present a state of the art on the Blockchain part applied to different domains and particularly to e-voting in developing countries. Section 3 presents the proposed approach. It is the generic platform that has been chosen to link the ministry to different universities and by analogy the university to different institutions. In Section 4, we describe the implementation result of the application and its implementation on a Raspberry PI platform. Section 5 discusses the low power application. Finally, Section 6 presents the conclusions and future work.

2. Ease of Use

2.1. Blockchain Application

Blockchain technology is based on a principle similar to Peer to Peer (P2P) networks [11]. Indeed, each node trusts the blockchain constituted by the other nodes. Therefore, it is a medium of shared and reliable archiving of various operations (transactions, data, etc.). Each node in the network stores these encrypted data with the impossibility to delete them. On the Blockchain, adding information is possible but modifying what has previously been recorded is not. Thus, there is no way to corrupt the data.

The blockchain operates as a decentralized database including the exchanges/transactions made among the different nodes. This database is shared in a secure way by its different users, without intermediaries. Any node has the possibility to check the validity of the chain of transactions [12].

The various transactions are grouped into blocks to be validated by the miner nodes and then added to the blockchain. Once stored, the transaction will be visible by the various nodes of the network, guaranteeing thus traceability.

From an encryption point of view, asymmetric public key cryptography (PKI) [12] is used in transactions. This technique exploits a pair of keys (public/private) to encrypt and decrypt the stored data.

The advantages of blockchain are: [13]

− Reliability: one of the strengths of decentralization is the minimization of damage from attacks.
− Trustlessness: thanks to decentralization, the information exchange is realized without the need for a third party.
− Integrity: based on a control protocol, the execution of transactions is achieved. This ensures its integrity.
− Transparency: all transactions made to the chains are public, immutable and can be controlled and accessed by all nodes of the Blockchain.

Initially, Blockchain was dedicated to the financial sector. Nowadays, it has been generalized into several fields of use. In this section, we will try to highlight some of them:

− Exchange

Blockchain technology solves some problems related to fragmented market systems. We can present interoperability, trust and transparency as problems [14].

– Energy Industry

Blockchain is used in energy-related applications especially in microgrids. This latter is a localized collection of electrical energy sources and loads that are integrated and managed to improve the efficiency and reliability of energy production and consumption [15–17].

– Insurance

Blockchain is used in the negotiation, purchasing, recording of insurance findings, and processing of claims [18,19].

– Healthcare

The use of Blockchain in healthcare is becoming more prevalent in the literature [20–23]. While in [2,24] a summary of the use of eHealth was presented; in [16] the Blockchain was used to record electronic health data. In [3], Frikha et al. propose an embedded platform based on Raspberry PI and Xilinx FPGA. This platform demonstrates that limitless platform resources could be used to integrate PoW with this low consumption embedded system.

– Industry

The Blockchain is also used for different industrial supply chain applications. It allows the tracking of products from their raw state to the finished product. This minimizes the risk of theft [25,26]. Among the industrial applications, there are the certificates allocated to Halal meats in the Muslim countries. In [27], Almyash et al. use a Blockchain-Based traceability methodology to supervise the Halal supply chain ecosystem in Indonesia.

– Agriculture

The use of Blockchain has also touched the agricultural field [28,29]. Thus, the tracking of the product by the buyer from the field to the final product has been performed by using the Blockchain [30]. Another application of Blockchain appears in smart greenhouses. It allows taking into account data from different IoT sensors. These data are synthesized and stored in the Blockchain so that they can be saved and accessed by people with access to these products [31].

– Education

Blockchain is also used in the academic setting. One of the best-known applications is the traceability of diplomas. In [32], a system for tracking the originality of architecture degrees is proposed.

In this work, an application based on e-vote is implemented. This data will be stored with a secure Blockchain-based application.

2.2. Applied Blockchain to E-Vote

In emerging democracies in North African countries, such as Tunisia, Egypt and Libya, elections are of paramount importance. Taking the example of Tunisia, since the revolution in 2011, it had to go through three presidential elections, three parliamentary elections and a referendum. As such, having a reliable, secure and efficient electoral system has become essential. With the spread of the COVID-19 pandemic, social distancing is increasingly becoming important. Several works have used Blockchain in the context of e-voting.

In [33], a voting platform with remote real-time ballot box auditing capability is proposed. This platform is based on the Blockchain. A mathematical approach is used to check if the results are correct and if no fraud occurred during the election.

In [34], a Blockchain-based system makes it possible to collect votes from mobile applications. For this application, the use of biometric data as a signature allows the validation of the vote that has been cast.

In [35], Polyas is a voting system used by industrialists in Germany. It is based on a private blockchain. In Sierra Leon, the voting system via Blockchain is used in the presidential elections; the reliability of this system is highlighted and shows that it is possible to have a reliable result using the Blockchain.

In [36,37], Ethereum was used to implement a voting system that allows between 50 and 60 voters.

Lai et al. [38] present an anonymous, decentralized and transparent electronic voting (DATE) which requires a minimal degree of trust between nodes.

Shahzad et al. [39] propose the BSJC completeness proof as a reliable e-voting method. They try to solve the problems of anonymity, privacy, and security of the voting.

Yi [40] proposed the blockchain-based for electronic voting system (BES), which provides methods to improve the security of electronic voting in developing countries.

In [41], the authors design a framework for electronic voting systems that use blockchain technology to address the flaws in current voting systems. A mixed approach is applied to explore the opportunities and challenges of the Hyperledger blockchain voting system.

In [42], the authors design and implement a Ethereum Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities. Each voter is given a secret key to be able to confirm that the vote has not been tampered. The advantage is the prevention against DoS attack, but the accuracy of the proposed solution is not evaluated using real-time data.

In [43], the authors propose an Electronic Voting system based on virtual ID of Aadhar using Blockchain Technology. It provides a secure evoting system based on biometric authentication using VID (Virtual ID) extracted from the Aadhar database. The advantage is authentication, availability, public, verifiable, integrity, SHA Algorithm but the overall system overhead increases such as the temporary ID, Virtual ID is to be generated to verify the authenticity of the user.

In [44], the authors propose a secured electronic voting system using the concepts of Blockchain. The proposed system is based on EVM (Electronic Vote Machine) is tamper-proof, and any effort to modify the registered votes can be recognized. Thus, it enables preventing double voting, but needs to use a strong, hybrid cryptographic techniques to enhance the security.

In [45], authors present a new SecEVS secure e-voting system. Designing the proposed system takes into consideration the network model and framework of the e-voting system. Regarding the network model, the authors applied it to a university campus. The issue of privacy has been considered. For voter confidentiality, it is also guaranteed as they are using the SHA-256 hash and encryption algorithm. For duplication and integrity, they have used a unique voter ID for each voter. For the storage, the single block used 84 bytes.

In [46], authors propose a secure voting protocol for score-based elections, where independent talliers perform the tallying procedure. The protocol offers perfect ballot secrecy: it outputs the identity of the winner (s) but keeps all other information secret, even from the talliers. However, authors do not use a decentralized blockchain.

In [47], authors present a novel electronic voting system (EVS) for political and social elections based on known cryptographic schemes. They use the El-Gamal algorithm to generate and encrypt random keys for the voters. This scheme is designed in a way that the communication channels are anonymous and at the same time privacy, eligibility and fairness are applied to the entire system. Nonetheless, authors do not use a decentralized blockchain.

In [48], the authors propose a layered architecture based on:

− Blockchain technology as a development platform and blockchain network. The Ethereum network provides a wide range of use cases, with the power of smart contracts. It is a platform where we can use tokens to build and run decentralized applications and create smart contracts.
− ML for automating the verification process of eligible voters using machine learning service of an AI-powered oracle platform for face authentication which helps enhance user experience.

In our system, an approach based on two Blockchains is proposed: a private Blockchain that will be used in institutions (faculty, institutions, schools) and a public Blockchain compatible with private Blockchains that will be used in universities and the ministry.

This choice makes it possible to solve the problem of the limited number of voters and to have an efficient, secure and low-cost solution. In this paper, an approach based on

Quorum as a private blockchain and Ethereum as a public blockchain is presented. Table 1 describes the essential of work on blockchain-based e-voting that compares our method with methods proposed in the literature.

Table 1. Compared approaches.

Author	Decentralised with Blockchain	Framework	Consensus	Hashing Algorithm	Counting Method	Anonymity	Audit	Integrity	Scalability
Lai [38]	Yes	Ethereum	PoW	SHA-3	Self-tally	Yes	No	No	Yes
Shahzad [39]	Yes	Bitcoin	PoW	SHA-256	3rd partie	Yes	Yes	Yes	No
Yi [40]	Yes	Bitcoin	PoW	SHA-256	N-A	Yes	Yes	No	No
Rathee [42]	Yes	Ethereum	PoW	Not specified	Self-tally	Yes	No	Yes	Yes
Roopak [43]	Yes	Not specified	Not specified	SHA-256	Self-tally	Yes	No	No	No
Krishna [44]	Yes	Not specified	PoW	AES-256	Self-tally	Yes	Yes	No	Yes
Singh [45]	Yes	Not specified	Not specified	SHA-256	Self-tally	Yes	No	Yes	No
Dery [46]	No	-	-	SSL	tallier module	Yes	No	Yes	Yes
El-Gburi [47]	No	-	-	El-Gamal algorithm	Self-tally	Yes	Yes	No	No
El Fezzazi [48]	Yes	Ethereum	Not specified	Not specified	Not specified	Yes	Yes	No	No
Gao [49]	Yes	Bitcoin	PBFT	Double SHA-256	Self-tally	Yes	Yes	Yes	No
McCorry [50]	Yes	Ethereum	2 Round-0 knowledge proof	Not specified	Self-tally	Yes	No	No	No
Our system	Yes	Ethereum & Quorum	PoW & PoS	SHA-256	Self-tally	Yes	Yes	Yes	Yes

2.3. Low Power Platform

An application can have various performances/consumption on a given target by varying the algorithmic or architectural target [51,52]. There is a lot of representative research in measure-based estimation techniques [53,54], which collect energy consumption data in a cycle-by-cycle. In the context of blockchain, the majority of work analyzes performance without any energy analysis [55,56].

Raspberry Pi and FPGA are popular platforms oriented to low power and low-cost computing applications [20] especially for developing countries [57–60].

Ktari et al. [20,58] analyze time and power consumption of an HW/SW hashing algorithm: Keccak in a Zedboard FPGA.

Sankaran et al. [61] use a Raspberry Pi to study the time and energy performance of miners in an Ethereum network.

For mobile devices with a limited storage, the Jupiter blockchain [62] aims at solving the problem of storing account wallets. However, this blockchain does not support energy performance evaluation.

In a data-center environment based on ARM cores, the energy efficiency is studied by Tudor et al. [63]. They analyze the CPU and the memory access performance [57].

Some power consumption measures of the Raspberry Pi with an external power meter are presented in Figure 1.

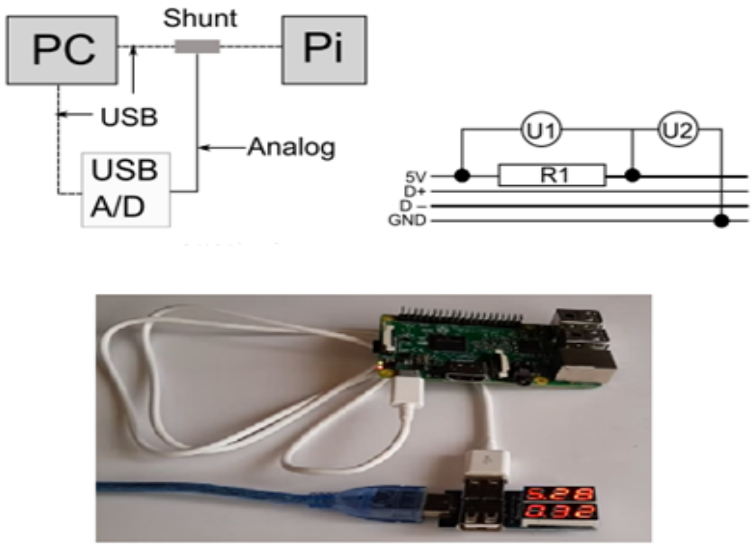

Figure 1. Raspberry power consumption measures.

Based on the literature [53,57,64], the power consumption of the quad core raspberry 3 depends on two factors: the power consumption in the idle state and the power consumption relative to CPU utilization "u" in the range 0 to 1. So, the consumption (W) can be written in this mathematical form:

$$Consumption = a * u + b \quad (1)$$

For example, the consumption of the board in the idle state will only consume approximately 1.5 W. According to [53,64], using the quad core board in Keccak algorithm will consume approximately 2.4 W

$$\text{Power (W)} = \text{Idle\_power} + \text{Running\_power} = 1.57\ \text{W} + 0.181 * \text{CPU\_utilization\%} \quad (2)$$

$$\text{Power\_ Keccak256} = 2.4\ \text{W}. \quad (3)$$

Thus, Raspberry achieves a reasonable performance with significant low energy especially for non-real time applications.

3. Proposed Approach

The high-power consumption of the blockchain system is a consequence of the use of high-performance platforms for mining. The ASICs or GPUs used for Bitcoin or Ethereum mining are very energy intensive. On the other hand, low-power ARM architectures have proven to be more energy efficient than traditional x86/64 architecture [53]. In this context, the paper introduces a low power Blockchain-based e-voting system. The proposed platform aims at providing a new voting system based on the private Blockchain (Quorum). This blockchain ensures the monitoring, security, and traceability of the online voting operation. The result of the elections will be then transformed into a transaction to be saved by another permissioned Blockchain that is shared among several institutions. Figure 2 illustrates the proposed system. The goal of this work is to show that it is possible to use low power platforms with limited resources during the realization of a voting system. The validation of the prototype has been realized using Raspberry PI.

Figure 2. Proposed approach.

3.1. General System

As shown in Figure 2, taking the Tunisian university system as an example, we consider that the Ministry of Higher Education and Scientific Research is linked to the different universities (Sfax, Tunis, Gabes etc.). In this figure, we represent four universities that are connected to the ministry by a public Blockchain. The connection is carried out via internet (Wifi, 4G, etc.).

Each university relates to its different faculties, institutions and schools. They are named (H.S 1, H.S 2, etc.). These institutions relate to the same public blockchain. However, each H.S uses a private blockchain. This is called the Quorum Blockchain.

Thus, let us take the case of an institution with seven departments. Each department has three levels, each with four groups. The total will be 84 groups, each with about 30 students. Each group represents a node of our Blockchain. So, the students who are part of this group will be able to vote for their representative. This vote will be counted, and the person voting will not be able to change or re-vote as soon as the vote is counted. In order to know if the student is part of this Blockchain node, the identification is realized using the barcode of their student card.

A mobile application will be created to allow the identification of the student and then to make it possible for them to choose the candidate they want and then cast their vote.

3.2. Particular University System

The University of Sfax will have Ethereum as Blockchain. It is connected to the 23 institutions (Institute, faculty, school). Each institution has its own private blockchain.

The Blockchain chosen is Quorum, which is a private blockchain. This choice is related to the fact that the number of students is known and the only people who can access our voting platform are the students at this institute, which is possible with a private Blockchain. The result of the vote of the different students is recorded as a transaction. This transaction will then be transferred and recorded as a new transaction in the Ethereum blockchain of the university.

In the framework of the work carried out in this paper, this approach will be tested in the context of our institution and particularly with the elections of the student representatives within the school as a case study.

The use of this method solves two problems:

- Facilitate the implementation of a secure election system.
- Create an efficient system respecting the social distancing in this period of COVID-19.

Figure 3 illustrates the described system. Thus, the university, which is the organization that groups all the faculties, institutions or schools, has its own public Blockchain (Ethereum). The institutions that belong to this organization each has its own private blockchain (Quorum).

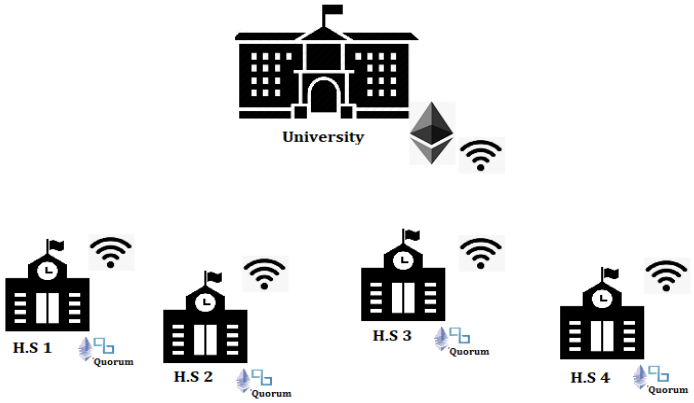

Figure 3. Specific system for e-vote application.

In this part, the proposed system is described. As far as the results revealed, the technologies used and the findings obtained will be described.

3.3. E-Vote Methodology

Figure 4 represents the methodology used algorithm. Every authorized user registers for the first time and then the data are saved on a server. In this work, we used the Node JS server. As soon as the user logs in to vote, they are not allowed to vote again. Once they have entered their login, we check if the data are correct. Then the user goes through the voting interface and votes. As soon as the vote is finalized, the data are sent to the Blockchain. This data will be encrypted and then added as a transaction in the current block of the blockchain.

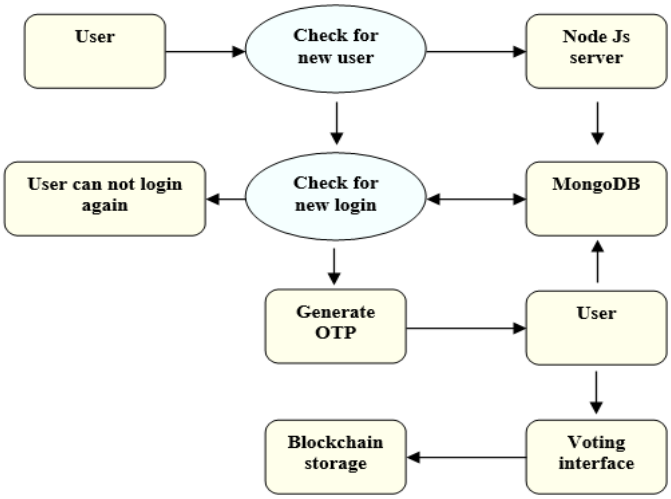

Figure 4. E-vote methodology.

As already mentioned, the blockchain technology used here is Quorum. The choice of Quorum for the institution is justified by the fact that the internal data of the institutions must be private. For Ethereum, the data are public because university elections affect a limited number of people including only tenured faculty. These people are known and have been already elected in their own institutions. Thus, the data are already reliable and secure.

The power of smart contracts offers a variety of use cases. Quorum has a large open-source community with a wide range of software that can be used together to build a secure distributed application. Considering the underlying security from digital signature to hash provided by Quorum, it is difficult to modify the source code of the corresponding software.

4. Obtained Results

The platform that is set up in our article was proposed in the previous section. In this part, we will present the platforms used.

4.1. E-Vote Proposed Hardware

In this work, the feasibility of our system using an embedded system with limited resources is demonstrated. In this context, we will set up a prototype using the Raspberry PI 4 platform, a quad processor platform with 2 GB of Ram [65].

Motivated by the performance improvements in low-power and the high energy consumption of blockchain, this platform has been made to demonstrate that it is possible to use a low-resource, low-power platform to build an efficient and secure blockchain-based system that supports an implementation of the Ethereum blockchain [64,66].

The implementation of the Quorum Blockchain on the same platform has been tested [67].

Thus the Ethereum on RPI 4 will be linked to the other Quorum blockchain which corresponds to the private blockchain implemented within the institute (High Schoolii∈{1,2, . . . ,23}).

4.2. E-Vote Steps

Figure 5 represents the voting steps that will be performed by each student before selecting their candidate.

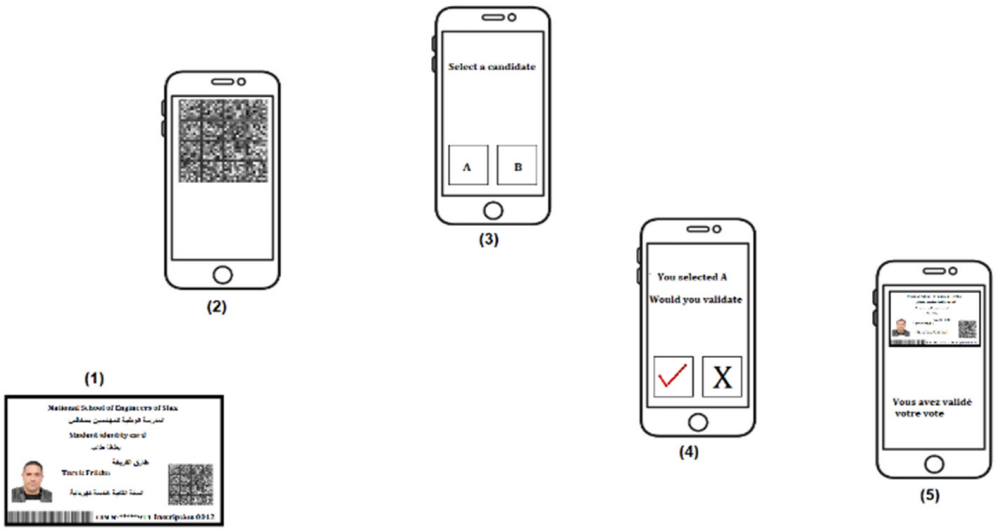

Figure 5. E-vote steps.

In the context of this work, Flatter, which makes it possible to have a multi-platform application, is chosen. Flatter allows us to have a system that can work on both Android platforms and IOS.

Thus, each voter will use their smartphone to choose their candidate.

The voting operation goes through five steps:

1. The voter must have their student card at their disposal.
2. Thanks to our application, the candidate scans the QR code present on their student card.
3. If the candidate has already voted, he/she will not be able to access the platform; otherwise, he/she will have the choice between the candidates (in our application we have chosen two candidates.)
4. After choosing, a validation request of the candidate is sent to the voter.
5. Following this validation, an image of the student's card and a confirmation of their vote are displayed on the application.

As soon as the operation is finalized, a transaction will be recorded in the Blockchain.

After the end of the votes, the result is immediately sent and displayed. This avoids the step of counting the votes manually. Thus, the risk of election rigging no longer exists.

After finalizing the voting operation within the institutions, the results obtained are sent directly to the university which must have access to all this information.

Thus, the Quorum administrator sends the information encrypted by public/private key as explained. The encryption system is based on the same principle as in the Quorum case. This data are then collected and put in a block in the Ethereum blockchain.

The university's blockchain will also be used for the elections of the university president. These elections include those of the university council members as well as the president. It is the same principle of elections for all institutions but using the Ethereum Blockchain.

4.3. Quorum on Raspberry PI

We have chosen a Raspberry PI with a minimal capacity and low energy consumption to show the possibility of creating a Blockchain system with low power consumption. Since blockchain is energy intensive, the migration to low power and cost architectures such as Raspberry or FPGA allows a significant gain in electricity, in addition to a reduction in the footprint. Besides being able to access and control the Raspberry Pi remotely as a headless computing unit, Raspberry can also be programmed in a variety of computer languages to run autonomously. It is a low-cost micro-computer that can support a wide range of coding functions and has high processing power.

After each voting operation, depending on the choice, the selected candidate will have their number of votes incremented and a transaction will be added to our block.

This encrypted transaction includes the choice and the student card number. These encrypted data remain inaccessible, but they make it possible to verify if the person has made the vote or not. Only the voter can verify their vote. Any other person will not have access to this information.

The protection is made thanks to the encryption system based on the public/private key. Each transaction is encrypted using the user's private key and the public key corresponding to the administration node. Decryption requires the user's public key and the administration's private key. This decryption is performed only for verification purposes.

While testing our blockchain, we noticed that it is impossible to insert more than four nodes per Raspberry PI. Beyond four nodes, the system will flatten. Each node cannot support more than 30 transactions.

To set up our system, three Raspberry Pi are used for departments with a large number of students (360 students). For the departments with half or less students, we were satisfied with one to two platforms per department.

The administration of the institute will have its own platform that will allow the collection of the information and the mining of the blocks including the results of each department. This platform will also include the graphic server part of our application.

It will then be connected to the Ethereum platform connected to the university.

4.4. Ethereum Implementation PI

The voting data stored on the Ethereum blockchain are decentralized, secure and immutable. In this work, a decentralized application via the smart contract protocol is used to develop the code. The latter runs on the Ethereum virtual machine, as shown in Figure 6.

Ethereum Virtual Machine smart contracts allow writing code and modifying reads and writes. The data are converted into value and any business logic is executed, which represents the program of the smart contract as a kind of micro service placed on the network.

To build decentralized applications (DAPPs), Node Package Manager, Ganache, Truffle Framework and MetaMask are required.

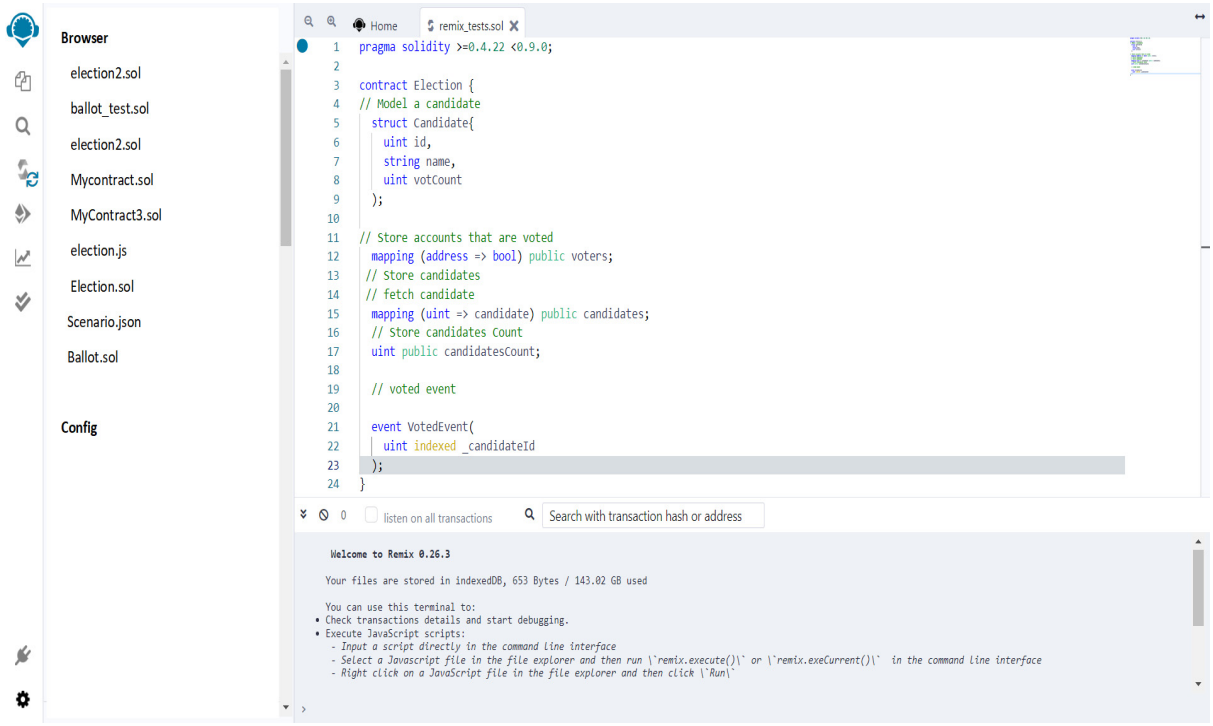

Figure 6. Ethereum Blockchain.

4.4.1. Node Package Manager

The Node Package Manager (NPM) tool was invented for Node.js. However, today, NPM has become the package manager for the whole JavaScript ecosystem, including outside Node.js. It permits to install libraries and frameworks considering the different dependencies. Figure 7 illustrates the commands allowing the installation of the environment needed.

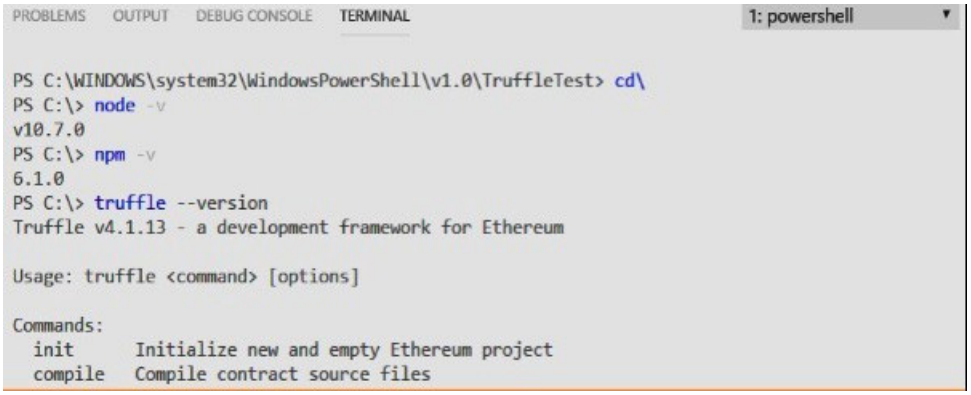

Figure 7. Node.js command prompt.

4.4.2. Truffle Framework

Truffle structure (framework) allows building decentralized applications on the Ethereum network.

Truffle provides a set of tools in order to create smart contracts using the programming language Solidity. It also provides structures for testing Smart Contracts and provides the tools needed to execute transactions (deploy) Smart Contracts. Figure 8 illustrates truffle framework.

```
   > balance:              99.99472518
   > gas used:             263741
   > gas price:            20 gwei
   > value sent:           0 ETH
   > total cost:           0.00527482 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:           0.00527482 ETH


2_deploy_[illegible].js
=======================

   Deploying 'HelloWorld'
   ----------------------
   > transaction hash:    0x5e6a26174d12474b53ec9b86d235d6b362ab9d8cfe39e5244dd4f5c080b79413
   > Blocks: 0            Seconds: 0
   > contract address:    0xCD461e4B556eF1Aa11DB570809c0D70B7DfF0a09
   > block number:        3
   > block timestamp:     1562399055
   > account:             0xe582029380bCa44B924F9E1ca19bFE613aba538D
   > balance:             99.98794752
   > gas used:            296860
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.0059372 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:           0.0059372 ETH


Summary
=======
> Total deployments:   2
> Final cost:          0.01121202 ETH

➜ [illegible]-solidity-truffle
```

Figure 8. Truffle framework.

4.4.3. Ganache

Ganache is used for distributed application development based on Ethereum and Corda [68]. In this work, Ganache is used as local storage for decentralized electronic voting development. Figure 9 illustrates the Ganache framework.

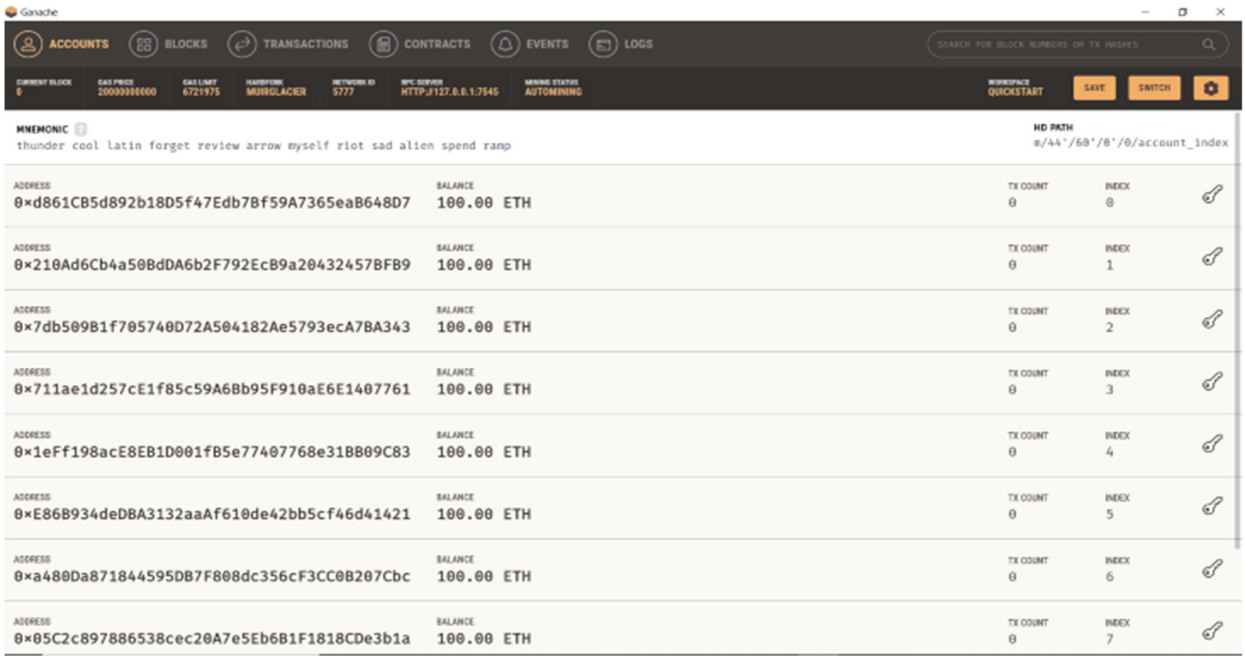

Figure 9. Ganache framework.

4.4.4. MetaMask

MetaMask is a Google Chrome extension. It is used to connect to the Ethereum blockchain. Figure 10 shows MetaMask after installation.

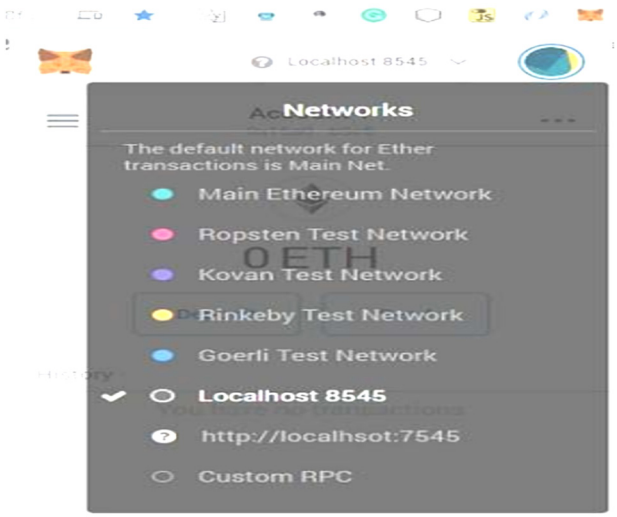

Figure 10. MetaMask framework.

MetaMask uses a personal account to establish a connection to the local Ethereum network and it is able to interact with the smart contract application.

4.5. Build Interaction with the Smart Contract

The application interacts with the smart contracts. This is an election results page with a table of candidates, each with an ID and name. The voting application platform supports the function of displaying voting results (Figure 11). Voters have realized that they voted for their correct candidates and applications based on blockchain protection. Voters can perform only one vote. If a voter wants to double vote, the system does not give them the possibility to connect twice in the same voting session.

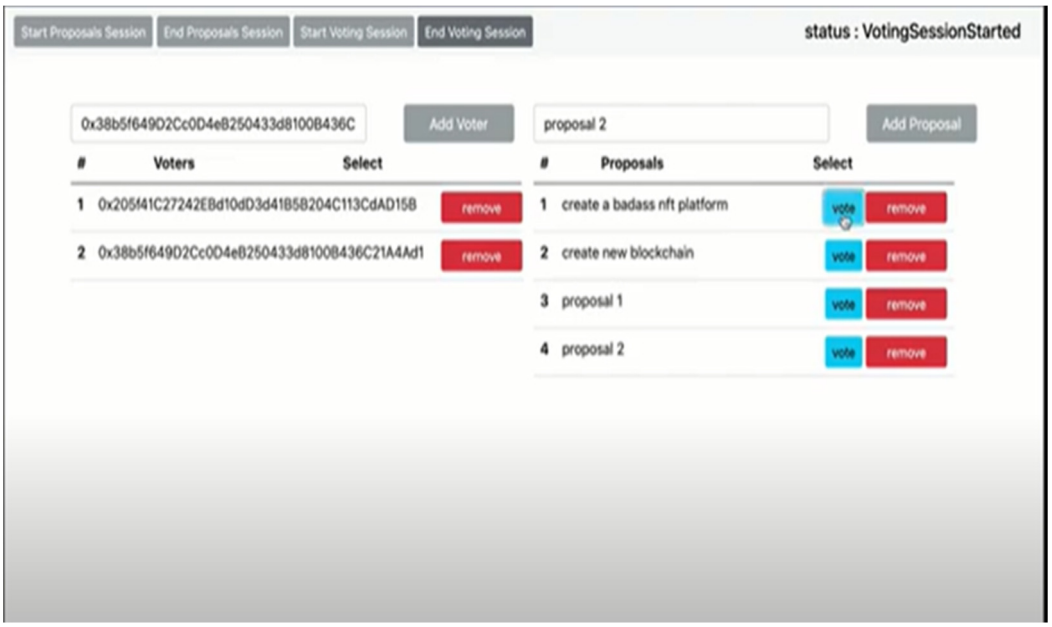

Figure 11. Voting interface.

5. Low Power Discussion

The low power factor has become an important issue, especially for blockchain which is energy intensive. The multi-core Raspberry platform can solve the power consumption problem even though its computing power is lower than a processor of the x86-64 family. This encourages the endorsement of a low power blockchain approach.

For voting applications, the real time aspect is not dominant especially for a private blockchain. In our case, if each university is related to its N different faculties, institutions and schools via a decentralized blockchain based on x86-64. This will generate high energy costs. The following table summarizes the performance (Instruction Per Second)/consumption of an Xeon processor and a Raspberry [53].

According to Table 2, we can also notice that despite the loss of performance with Raspberry (16 times) % Xeon, there is a very important energy gain (26 times) which largely compensates the loss of performance especially for applications without real time constraints. As such, the migration to raspberry allows a global energy gain of more than 61% and a greater gain compared to Radeon VII GPUs which consume more than 200 W.

Table 2. Compared performance/consumption.

	Xeon	**Raspberry Pi**
Characteristics	X86-64 3.5 GHz 6 cores	ARM 7-8 1.5 GHz 4 cores
Cost ($)	400	50
Performance (IPS)	185,000	11,000
Power (W)	128	4.9
Power cost Per Instrucion (mW/Instr)	0.70	0.44

However, in order to optimize more and more our system from an HW point of view, FPGA can be used. The goal is to have HW IPs which will be developed in VHDL and which will allow to accelerate the implementation of the consensus and particularly the PoW.

The addition of this consensus allows having a more secure system, which is, however, greedier in terms of resources and execution time.

Thus, thanks to FPGAs and IPs, we can create a more optimized, faster and less greedy architecture than Raspberry PI with generic HW architecture.

In this work, an optimized Blockchain for Raspberry PI is implemented using both the public Ethereum blockchain and the private Quorum blockchain. This implementation has resulted in a low power system compared to PC or GPU implementations.

Moreover, the proposed system is hybrid (two different blockchains), secure (SHA 256), self-tallied, anonymous, scalable, with high integrity, affordable and accessible. The application of barcode identification of voters permits to identify them and validates the voting operation. Thus, the feasibility, the implementation and the energetic study of the prototype have been realized in this work.

6. Conclusions

In this paper, a low power blockchain-based e-voting approach, which answers the requirements, has been proposed. This approach uses two blockchains: the public Ethereum blockchain and the private Quorum blockchain. An encrypted communication has been achieved between them. This paper attempts at solving the frauds and manual counting problems by saving the secured vote data in a decentralized blockchain network. The prototype of the proposed approach was developed for a Raspberry Pi which runs under the Raspbian Operating System. Energy calculations have shown the usefulness of platforms such as raspberry for energy intensive applications such as blockchain, allowing a gain in consumption of 61% compared to Xeon. As perspectives for this work, it is important

to study the behavior of our system after attacks and study the possibility to extend it to a larger scale. The application can be tested also on an FPGA in order to reach a low cost/resource solution.

Author Contributions: This paper is the result of a collaboration between different authors from different universities. Conceptualization, F.C. and J.K.; methodology, J.K.; software F.C.; validation, J.K., T.F. and H.H.; formal analysis, J.K. and F.C.; investigation, T.F. and F.C.; resources, F.C. and T.F.; data curation, T.F.; writing—original draft preparation, J.K.; writing—review and editing, T.F. and H.H.; visualization, J.K. and T.F.; supervision T.F.; project administration, T.F.; funding acquisition, H.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No data availability.

Conflicts of Interest: There is no conflict of interest.

References

1. Ben Fekih, R.; Lahami, M. Application of Blockchain Technology in Healthcare: A Comprehensive Study. In *International Conference on Smart Homes and Health Telematics*; Springer: Cham, Switzerland, 2020; pp. 268–276.
2. Frikha, T.; Chaari, A.; Chaabane, F.; Cheikhrouhou, O.; Zaguia, A. Healthcare and Fitness Data Management Using the IoT-Based Blockchain Platform. *J. Healthc. Eng.* **2021**, *2021*, 9978863. [CrossRef] [PubMed]
3. Frikha, T.; Chaabane, F.; Aouinti, N.; Cheikhrouhou, O.; Ben Amor, N.; Kerrouche, A. Implementation of Blockchain Consensus Algorithm on Embedded Architecture. *Secur. Commun. Netw.* **2021**, *2021*, 9918697. [CrossRef]
4. Erol, I.; Neuhofer, I.O.; Dogru, T.; Oztel, A.; Searcy, C.; Yorulmaz, A.C. Improving sustainability in the tourism industry through blockchain technology: Challenges and opportunities. *Tour. Manag.* **2022**, *93*, 104628. [CrossRef]
5. Ktari, J.; Frikha, T.; Hamdi, M.; Elmannai, H.; Hmam, H. Lightweight AI Framework for Industry 4.0 Case Study: Water Meter Recognition. *Big Data Cogn. Comput.* **2022**, *6*, 72. [CrossRef]
6. Li, Z.; Zhong, R.Y.; Tian, Z.; Dai, H.-N.; Barenji, A.V.; Huang, G.Q. Industrial Blockchain: A state-of-the-art Survey. *Robot. Comput. Manuf.* **2021**, *70*, 102124. [CrossRef]
7. Demestichas, K.; Peppes, N.; Alexakis, T.; Adamopoulou, E. Blockchain in Agriculture Traceability Systems: A Review. *Appl. Sci.* **2020**, *10*, 4113. [CrossRef]
8. Harshitha, M.S.; Shashidhar, R.; Roopa, M. Block chain based agricultural supply chain-A review. *Glob. Transit. Proc.* **2021**, *2*, 220–226. [CrossRef]
9. Xue, L.; Fu, R.; Lin, D.; Kuok, K.; Huang, C.; Su, J.; Hong, W. Exploring the Innovative Blockchain-Based Application of Online Learning System in University. In *International Conference on Web-Based Learning*; Springer: Cham, Switzerland, 2021; pp. 90–101. [CrossRef]
10. Allouche, M.; Frikha, T.; Mitrea, M.; Memmi, G.; Chaabane, F. Lightweight Blockchain Processing. Case Study: Scanned Document Tracking on Tezos Blockchain. *Appl. Sci.* **2021**, *11*, 7169. [CrossRef]
11. Schollmeier, R. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In Proceedings of the First International Conference on Peer-to-Peer Computing, Linkoping, Sweden, 27–29 August 2001; pp. 101–102. [CrossRef]
12. Bradbury, D. Blockchain's. *Eng. Technol.* **2016**, *11*, 44–47. [CrossRef]
13. Acharjamayum, I.; Patgiri, R.; Devi, D. Blockchain: A Tale of Peer to Peer Security. In Proceedings of the 2018 IEEE Symposium Series on Compu-tational Intelligence (SSCI), Bangalore, India, 18–21 November 2018; pp. 609–617. [CrossRef]
14. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2018**, *36*, 55–81. [CrossRef]
15. Yang, J.; Paudel, A.; Gooi, H.B. Compensation for Power Loss by a Proof-of-Stake Consortium Blockchain Microgrid. *IEEE Trans. Ind. Inform.* **2020**, *17*, 3253–3262. [CrossRef]
16. Wu, Y.; Wu, Y.; Cimen, H.; Vasquez, J.C.; Guerrero, J.M. Towards collective energy Community: Potential roles of microgrid and blockchain to go beyond P2P energy trading. *Appl. Energy* **2022**, *314*, 119003. [CrossRef]
17. Wang, X.; Yao, F.; Wen, F. Applications of Blockchain Technology in Modern Power Systems: A Brief Survey. *Energies* **2022**, *15*, 4516. [CrossRef]
18. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaría, V. Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? *Futur. Internet* **2018**, *10*, 20. [CrossRef]
19. Chondrogiannis, E.; Andronikou, V.; Karanastasis, E.; Litke, A.; Varvarigou, T. Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations. *Blockchain Res. Appl.* **2022**, *3*, 100049. [CrossRef]
20. Ktari, J.; Frikha, T.; Ben Amor, N.; Louraidh, L.; Elmannai, H.; Hamdi, M. IoMT-Based Platform for E-Health Monitoring Based on the Blockchain. *Electronics* **2022**, *11*, 2314. [CrossRef]

21. Elangovan, D.; Long, C.; Bakrin, F.S.; Tan, C.S.; Goh, K.; Ming, L.C. The Use of Blockchain Technology in the Health Care Sector: Systematic Review. *JMIR Med. Inform.* **2022**, *10*, e17278. [CrossRef]
22. Fatima, N.; Agarwal, P.; Sohail, S.S. Security and Privacy Issues of Blockchain Technology in Health Care—A Review. In *ICT Analysis and Applications*; Springer: Cham, Switzerland, 2022; pp. 193–201. [CrossRef]
23. Gambril, J.; Boyd, C.; Egbaria, J. Application of Nonfungible Tokens to Health Care. Comment on Blockchain Technology Projects to Provide Telemedical Services: Systematic Review. *J. Med. Internet Res.* **2022**, *24*, e34276. [CrossRef]
24. Frikha, T.; Abdennour, N.; Chaabane, F.; Ghorbel, O.; Ayedi, R.; Shahin, O.R.; Cheikhrouhou, O. Source Localization of EEG Brainwaves Activities via Mother Wavelets Families for SWT Decomposition. *J. Health Eng.* **2021**, *2021*, 9938646. [CrossRef]
25. Chen, Y.; Lu, Y.; Bulysheva, L.; Kataev, M.Y. Applications of Blockchain in Industry 4.0: A Review. *Inf. Syst. Front.* **2022**, 1–15. [CrossRef]
26. Wamba, S.F.; Queiroz, M.M. Industry 4.0 and the supply chain digitalisation: A blockchain diffusion perspective. *Prod. Plan. Control* **2020**, *33*, 193–210. [CrossRef]
27. Alamsyah, A.; Hakim, N.; Hendayani, R. Blockchain-Based Traceability System to Support the Indonesian Halal Supply Chain Ecosystem. *Economies* **2022**, *10*, 134. [CrossRef]
28. Vyas, S.; Shabaz, M.; Pandit, P.; Parvathy, L.R.; Ofori, I. Integration of Artificial Intelligence and Blockchain Technology in Healthcare and Agriculture. *J. Food Qual.* **2022**, *2022*, 4228448. [CrossRef]
29. Alobid, M.; Abujudeh, S.; Szűcs, I. The Role of Blockchain in Revolutionizing the Agricultural Sector. *Sustainability* **2022**, *14*, 4313. [CrossRef]
30. Praveen, P.; Shaik, M.A.; Kumar, T.S.; Choudhury, T. Smart Farming: Securing Farmers Using Block Chain Technology and IOT. In *Blockchain Applications in IoT Ecosystem*; Springer: Cham, Switzerland, 2021; pp. 225–238. [CrossRef]
31. Guo, C.; Zi, Y.; Ren, W. A Blockchain Based Framework for Smart Greenhouse Data Management. In *International Conference on Knowledge Science, Engineering and Management*; Springer: Cham, Switzerland, 2021; pp. 299–310. [CrossRef]
32. Khan, A.A.; Laghari, A.A.; Shaikh, A.A.; Bourouis, S.; Mamlouk, A.M.; Alshazly, H. Educational Blockchain: A Secure Degree Attestation and Verification Traceability Architecture for Higher Education Commission. *Appl. Sci.* **2021**, *11*, 10917. [CrossRef]
33. Vote, F.M. The Secure Mobile Voting Platform of The Future—Follow My Vote. 2020. Available online: https://followmyvote.com/ (accessed on 28 July 2020).
34. Voatz. Voatz—Voting Redefined®. 2020. Available online: https://voatz.com (accessed on 28 July 2020).
35. Polyas. Polyas. 2015. Available online: https://www.polyas.com (accessed on 28 July 2020).
36. Agora. Agora. 2020. Available online: https://www.agora.vote (accessed on 28 July 2020).
37. Zhang, S.; Wang, L.; Xiong, H. Chaintegrity: Blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *Int. J. Inf. Secur.* **2019**, *19*, 323–341. [CrossRef]
38. Lai, W.J.; Hsieh, Y.C.; Hsueh, C.W.; Wu, J.L. Date: A decentralized, anonymous and transparent e-voting system. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018.
39. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access* **2019**, *7*, 24477–24488. [CrossRef]
40. Yi, H. Securing e-voting based on blockchain in P2P network. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 137. [CrossRef]
41. AlAbri, R.; Shaikh, A.K.; Ali, S.; Al-Badi, A.H. Designing an E-Voting Framework Using Blockchain Technology: A Case Study of Oman. *Int. J. Electron. Gov. Res.* **2022**, *18*, 1–29. [CrossRef]
42. Rathee, G.; Iqbal, R.; Waqar, O.; Bashir, A.K. On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities. *IEEE Access* **2021**, *9*, 34165–34176. [CrossRef]
43. Roopak, T.; Sumathi, R. Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology. In Proceedings of the 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 5–7 March 2020; pp. 71–75. [CrossRef]
44. Krishna, S.B.; Arvindh, M.P.; Alagappan, M. Secured Electronic Voting System Using the Concepts of Blockchain. In Proceedings of the IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 17–19 October 2019; pp. 675–681. [CrossRef]
45. Singh, A.; Chatterjee, K. SecEVS: Secure Electronic Voting System Using Blockchain Technology. In Proceedings of the International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, India, 28–29 September 2018; pp. 863–867. [CrossRef]
46. Dery, L.; Tassa, T.; Yanai, A.; Zamarin, A. A secure voting system for score based elections. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (Virtual), Korea, 15–19 November 2021; pp. 2399–2401.
47. El-Gburi, J.; Srivastava, G.; Mohan, S. Secure voting system for elections. *Int. J. Comput. Aided Eng. Technol.* **2022**, *16*, 497–511. [CrossRef]
48. El Fezzazi, A.; Adadi, A.; Berrada, M. Towards a Blockchain based Intelligent and Secure Voting. In Proceedings of the 2021 Fifth International Conference on Intelligent Computing in Data Sciences (ICDS), Fez, Morocco, 20–22 October 2021; pp. 1–8.
49. Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C. An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function. *IEEE Access* **2019**, *7*, 115304–115316. [CrossRef]
50. McCorry, P.; Shahandashti, S.F.; Hao, F. A smart contract for boardroom voting with maximum voter privacy. In Proceedings of the International Conference on Financial Cryptography and Data Security, Sliema, Malta, 3–7 April 2017.
51. Ktari, J.; Abid, M. A Low Power Design Methodology Based on High Level Models. In Proceedings of the International Conference on Embedded Systems & Applications, Las Vegas, NV, USA, 14–17 July 2008; pp. 10–15.

52. Ktari, J.; Abid, M. System Level Power and Energy Modeling for Signal Processing Applications. In Proceedings of the 2nd IEEE International Design and Test Workshop, Cairo, Egypt, 16–18 December 2007; pp. 218–221. [CrossRef]
53. Loghin, D.; Chen, G.; Dinh, T.; Ooi, B.C.; Teo, Y.M. Blockchain Goes Green? An Analysis of Blockchain on Low-Power Nodes. *arXiv* **2019**, arXiv:1905.06520.
54. Ktari, J.; Abid, M. A Low Power Design Space Exploration Methodology Based on High Level Models and Confidence Intervals. *J. Low Power Electron.* **2009**, *5*, 17–30. [CrossRef]
55. Dammak, B.; Turki, M.; Cheikhrouhou, S.; Baklouti, M.; Mars, R.; Dhahbi, A. LoRaChainCare: An IoT Architecture Integrating Blockchain and LoRa Network for Personal Health Care Data Monitoring. *Sensors* **2022**, *22*, 1497. [CrossRef]
56. Islam, M.R.; Rashid, M.M.; Rahman, M.A.; Mohamad, M.H. A Comprehensive Analysis of Blockchain-based Cryptocurrency Mining Impact on Energy Consumption. *Int. J. Adv. Comput. Sci. Appl.* **2022**, *13*, 590–598. [CrossRef]
57. Kaup, F.; Gottschling, P.; Hausheer, D. PowerPi: Measuring and modeling the power consumption of the Raspberry Pi. In Proceedings of the 39th Annual IEEE Conference on Local Computer Networks, Edmonton, AB, Canada, 8–11 September 2014; pp. 236–243. [CrossRef]
58. Ktari, J.; Frikha, T.; Yousfi, M.A.; Belghith, M.K.; Sanei, N. Embedded Keccak implementation on FPGA. In Proceedings of the 2022 IEEE International Conference on Design & Test of Integrated Micro & Nano-Systems (DTS), Cairo, Egypt, 6–9 June 2022; pp. 1–5.
59. Loukil, K.; Khalfa, M.; Jmal, M.W.; Frikha, T.; Abid, M. Design and test of smart IP-camera within reconfigurable platform. In Proceedings of the 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, 26–27 March 2017; pp. 25–29.
60. Frikha, T.; Ben Amor, N.; Diguet, J.-P.; Abid, M. A novel Xilinx-based architecture for 3D-graphics. *Multimed. Tools Appl.* **2018**, *78*, 14947–14970. [CrossRef]
61. Sankaran, S.; Sanju, S.; Achuthan, K. Towards Realistic Energy Profiling of Blockchains for Securing Internet of Things. In Proceedings of the 38th IEEE International Conference on Distributed Computing Systems, Vienna, Austria, 2–6 July 2018; pp. 1454–1459. [CrossRef]
62. Han, S.; Xu, Z.; Chen, L. Jupiter: A Blockchain Platform for Mobile Devices. In Proceedings of the 34th IEEE International Conference on Data Engineering (ICDE), Paris, France, 16–19 April 2018; pp. 1649–1652.
63. Tudor, B.M.; Teo, Y.M. On understanding the energy consumption of ARM-based multicore servers. In Proceedings of the International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS), Pittsburgh, PA, USA, 17–21 June 2013; ACM Press: New York, NY, USA, 2013; p. 267.
64. Ge, Z.; Loghin, D.; Ooi, B.; Ruan, P.; Wang, T. Hybrid blockchain database systems: Design and performance. *Proc. VLDB Endow.* **2022**, *15*, 1092–1104. [CrossRef]
65. Raspberry Pi Tutorials. Available online: https://raspberrypi-tutorials.fr/ (accessed on 9 July 2022).
66. Ethereum. Available online: https://ethereum.org/en/ (accessed on 9 July 2022).
67. ConsenSys Quorum. Available online: https://consensys.net/quorum/ (accessed on 9 July 2022).
68. Ganache. Overview—Truffle Suite. Available online: https://trufflesuite.com/docs/ganache/ (accessed on 10 October 2021).