Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3, 223-235
2024
Publisher: Learning Gate
DOI: 10.55214/25768484.v8i3.930

Organized leader election consensus protocol and a supportive blockchain model for ambient assisted living

Basem Assiri
Computer Science Department, Jazan University, Saudi Arabia; babumussmar@jazanu.edu.sa (B.A.).

Abstract: Blockchain enhances the development of other technologies and systems by providing more transparency, sharing, decentralization, security, and privacy. Blockchain has many applications that enable integration and application in many areas, such as the field of ambient assisted living (AAL). However, blockchain includes many processes for data proposing, validating, and approving, which result in high latency. Such latency negatively influences AAL systems, which require real-time responses in many cases. In addition, blockchain processes are processed based on consensus. This challenges specialized decisions that should be taken only by specialized members within the blockchain network. Therefore, this work introduces an organized leader election consensus protocol with a blockchain model that is applicable for AAL. The proposed protocol and model are able to solve the issue of latency as well as consider specialized decisions. Solving the issue of latency enables AAL to perform real-time processes in the needed cases. While considering the matter of specialization gives more credibility to the blockchain's decisions, which is necessary for AAL. Indeed, it classifies the blocks into special-sensitive, time-sensitive, and non-sensitive classes, where each class has a suitable procedure. In addition, to manage the organized leader election consensus protocol, we manage the blockchain feature and rewarding strategy. This enhances the miners' participation in a way that supports blockchain and AAL simultaneously. The experimental results show that our model reduces the execution time by about 51% in comparison to the original blockchain model.

Keywords: *Ambient assisted living, Blockchain, Consensus protocol, Internet of things, Organized leader election protocol, Data sensitivity.*

1. Introduction

Blockchain is a promising technology that supports other technologies and systems. The ability to integrate blockchain with other systems reflects on the development of other fields such as finance, healthcare, education, national security, quality of life, and others. In the area of quality of life, governments and organizations work to measure and achieve people's happiness in a standardized manner [1]. This includes many factors, such as people's financial level, the job's environment, family satisfaction, health situation, and safety. Nowadays, technology facilitates achieving such targets [2-4]. For example, ambient assisted living (AAL) supports and enables peoples with special needs and elderly people to be independent, so they will be able to live alone at home. AAL systems use electronic devices and technologies that are integrated into the living environment to provide independence, assistance, monitoring, safety, and enhance the overall quality of life [5, 6].

On the other hand, blockchain technology is proposed to be integrated with AAL to provide data security since AAL processes a huge amount of personal and sensitive data [7, 8]. In addition, blockchain provides many advantageous values and properties, such as decentralization, transparency, immunity, and credibility [9]. Indeed, a blockchain consists of nodes that are connected over a network. Each node has a copy of a distributed ledger that securely stores a chain of blocks; where each block contains a group of approved transactions. At the beginning of blockchain procedures, nodes compete to verify transactions

History: Received: 1 February 2024; Revised: 15 March 2024; Accepted: 4 April 2024; Published: 24 April 2024
Correspondence: babumussmar@jazanu.edu.sa

and store them in one block. The nodes have to satisfy a consensus protocol to propose their blocks to the others for validation. Indeed, according to the consensus protocol, one node proposes its block. Then, the other nodes validate the proposed block to approve it and connect it to the blocks' chain (ledger) or to disapprove it [10].

However, blockchain includes the processes of transactions' verification, block creation, consensus protocols' satisfaction, casting the proposed block to the others, validating the proposed block, and voting on the approval of the proposed block. All of those processes result in high latency. Such latency negatively influences AAL systems, which require real-time responses in many cases. Furthermore, blockchain processes operate through consensus. This challenges specialized decisions that should be taken only by specialized members within the blockchain network.

Another issue is that many traditional consensus protocols and rewarding systems depend on processing capabilities and wealth, such as in Proof of Work (PoW) and Proof of Stake (PoS) [11]. This disappoints nodes with low capabilities, as well as new joining nodes that do not have enough capabilities or cryptocurrencies to stake, which challenges the system's fairness. Other protocols satisfy fairness regardless of the node's capabilities or trustworthiness, such as in Proof of Queue (PoQ). This emphasizes the concerns related to how to use a rewarding system in a way that encourages node participation and satisfies fairness and trustworthiness, as well as maintaining AAL time and specialization requirements.

Therefore, this work introduces the organized leader election (OLE) consensus protocol with a supportive blockchain model to be applied to AAL. It is able to solve the issue of latency as well as consider the specialized decisions. Solving the issue of latency enables AAL to perform real-time processes in the needed cases. While considering the matter of specialization gives more credibility to the blockchain's decisions, which is necessary for AAL. Indeed, it classifies the blocks into special-sensitive, time-sensitive, and non-sensitive classes, where each class has a suitable procedure. In addition, to manage the OLE consensus protocol, we manage blockchain features and rewarding strategies. This enhances the miners' participation in a way that supports blockchain and AAL simultaneously. Therefore, the OLE protocol is efficient as it considers miner capabilities, trustworthiness, specialization and decentralization. Moreover, the experimental results show that the OLE reduces the execution time by about 51% in comparison to the original blockchain model.

The rest of the paper is organized as follows: The work investigates AAL characteristics in Section 2. Blockchain technology and consensus protocols are deeply analyzed and investigated in sections 3 and 4. The related work is illustrated in Section 5. Section 6 shows the proposed methodology, model architecture, and algorithms. Section 7 analyzes the features and reward management of the OLE protocol. The experimental results are shown in Section 8, while Section 9 concludes the paper.

2. AAL

AAL facilitates healthcare assistance and safety for all people. It is more important for people with special needs and elderly people to be independent and to be able to live alone at home. AAL uses technologies to maintain people's healthcare, social-care, and safety. Actually, healthcare includes maintaining physical and mental health [12, 13]. While social-care focuses on social health and functional health, social-care allows for the provision of physical assistance, learning assistance, communication with others, and the performance of daily tasks [14]. Moreover, AAL should satisfy all healthcare and social-care values, such as social justice, dignity, emotional consideration, and confidentiality.

AAL interleaves with a variety of systems and applications, which are as follows:

• Smart homes and Internet of things (IoT): AAL applies smart homes and IoT concepts. They enable various electronic devices, sensors, and applications such as smart appliances, wearable devices, and voice assistants. Those can interconnect with each other's, building an intelligent living environment [15].

• Security and safety: AAL enhances environmental security and safety using automated doors, window locking, alarm systems, smoke and gas detectors, and cameras [16, 17].

• Healthcare and social-care: AAL provides remote monitoring of health conditions and daily activities for special needs and elderly people. Such monitoring allows for real-time assistance, instructions, and recommendations [2, 12, 14].

• Machine Learning: AAL systems can be supported by machine learning and deep learning models, which allow for finding patterns. This helps to predict needed assistance and recommendations, as well as detect irregular signs and behaviors in an automated manner. For example, machine learning models and smart applications can automatically suggest a daily eating regimen (including the amount of calories, fat, salt, or sugar) according to health signs and daily activities [18, 19].

• Data: for data management and storage, AAl uses cloud computing and blockchain. This provides data accessibility, real-time processing, and more security [20, 21].

3. Blockchain

As mentioned earlier, blockchain consists of nodes that are connected over a network to process and store data in a modern, democratic way. This will enforce cultural change in many administrative and business systems [22]. The blockchain is a distributed system, where every node stores and maintains its own copy of a ledger to be up-to-date and consistent with others. Therefore, blockchain runs using a determined structure and procedure for data processing, as follows:

• Assets: the original data that has a specific field and type. The field of data can be financial, educational, healthcare, business, or others. The type of data can be digital data, such as in a database, or analog data, such as signals that come from sensors and other resources.

• Transaction: The blockchain processes all data in the form of transactions. The transaction consists of multiple read and update processes on the original data (assets). These operations run in a temporary buffer, after which they either commit (approval and all changes reflect in the main memory) or abort (disapproval and buffer release). For example, for a money withdrawal transaction, the user enters the security information and a security check is conducted; then the user enters the amount to be withdrawn, and if it is available, it performs the task and commits the transaction. Otherwise, if any single operation fails, then the whole transaction is aborted.

• Block: the block mainly contains a group of verified transactions. The block size varies according to the system specifications. The block is proposed through a mining process. In the mining process, nodes verify transactions and create a new block. Therefore, the block should have a unique identifier (timestamp). Then, the whole content of block is hashed, producing a hash number. The hash number has some specific characteristic, that must be satisfied; otherwise, the block cannot be proposed for validation. Indeed, blocks use a nonce, which is a random number that keeps changing until the hash number satisfies the specific characteristic. The block also has the hash number of the previous block. Finally, the block is encrypted, so it is securely sent to the other nodes for validation.

• Ledger: It consists of a chain of all approved blocks. In fact, after block validation processes, all validator nodes vote on the approval of the new block. In the case of approval, the new block is chained to the ledger in-light of the previous block hash number. Since every node has its own copy of the ledger, every node updates its own copy. Therefore, any individual or illegal change to the ledger will be easily detected by comparing it to the others.

4. Consensus Protocols

Moreover, the blockchain's nodes are rewarded for creating, proposing, and validating a new block. Thus, they compete according to consensus protocols such as PoW, PoS, Delegated Proof of Stake (DPoS), Proof-of-Space, PoQ, Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoA), and leader election consensus protocols [11, 23-27].

- PoW is the consensus protocol used for Bitcoin and Ethereum cryptocurrency. In PoW, nodes compete in solving a mathematical computation, producing the hash number of the new block that satisfies specific lengths and characteristics. Then, the validator nodes validate the block's hash number as well as the block's content. Obviously, PoW requires high computational power; otherwise, nodes cannot compete.

- PoS and DPoS: in PoS, nodes should stake a specific amount of cryptocurrency, and then the node with the highest stake will propose the new block. In addition, DPoS enables the selection of a set of validator nodes instead of having all other nodes as validators. In DPoS, the validators' set includes the nodes with higher stakes. However, PoS and DPoS require that node have lots of cryptocurrency to stake; otherwise, node cannot compete.
- Proof-of-Space: it requires nodes to make their memory space available for the blockchain's data. However, it requires a maximum memory size. The nodes with the highest memory size will propose and validate the new block.
- PoQ: it requires nodes to be queued and get chances to propose and validate blocks according to their positions in the queue, which maintains fairness. However, it lacks practical efficiency, as it may assign certain complex or specialized tasks to a node with inadequate or inappropriate capabilities.
- PBFT: It focuses on the trustworthiness of the decision by considering the majority decision to determine its trustworthiness. It requires nodes to agree on voting and to consider the vote of the majority, which is the consensus of at least two-thirds of all nodes. However, the accuracy of votes is not maintained, as one-third of nodes could contradict the majority. Also, the majority of two-thirds is not enough in some sensitive cases, such as health or financial transactions.
- PoA: It is a consensus algorithm that gives the privileges of the block's proposing and validating to the trustworthy and the authorized nodes. The nodes build their trustworthiness through pre-programmed authority, history, and reputation. However, this strategy influences blockchain's decentralization.
- Leader Election Protocols: There are many leader election consensus protocols where an elected leader proposes the new block and coordinates blockchain decisions on data processing and updating. However, this strategy also influences blockchain's decentralization.

In short, the existing consensus protocols have some issues, as some of them require huge capabilities and resources, while others satisfy fairness among miners but do not consider capabilities and efficiency. In addition, some consensus protocols influence the blockchain's decentralization. Actually, all consensus protocols mentioned do not support applying blockchain to AAL systems. Therefore, we propose the OLE protocol to consider miner capabilities, trustworthiness, specialization and decentralization.

5. Related Work

Blockchain applications appear for the first time in the cryptocurrency field. The first cryptocurrency is Bitcoin, and after that, many other cryptocurrencies have been introduced [28, 29]. Then, blockchain applications have expanded and been integrated into many other fields [30]. One of the important fields is AAL, where remote and electronic assistants are applied. Many works combine blockchain and AAL for IoT and sensors, as well as data management, security, and privacy [7, 8, 31].

However, the original algorithms and architecture of blockchain do not satisfy the major characteristics of AAL. Therefore, many researchers consider the modification of systems' architectures to solve data sensitivity issues, as well as procedures' fairness and trustworthiness [25, 26, 32, 33].

Moreover, numerous leader election algorithms serve as consensus protocols to meet these requirements. Indeed, Right-of-Stake (RoS), Resource Aggregation for Fault Tolerance (RAFT) and Single Secret Leader Election (SSLE) are efficient leader election consensus protocols. In RoS, nodes stake some amount of cryptocurrency; and the leader is one of those nodes that exceeds a specific threshold of stake [34]. In RAFT, a leader is elected and takes decisions, while every action is stored as a log. All other nodes are called followers, and they execute the same actions in the logs [35]. However, leader election algorithms suffer from denial-of-service attacks where the leader is targeted. Therefore, many algorithms modify previous protocols to hide the identity of the leader, such as SSLE [36]. However, leader election consensus protocols still suffer from some issues, such as single points of failure and time complexity, which are solved using the proposed OLE consensus protocol.

Actually, OLE consensus protocols use the idea of leader election in an organized way that reduces the time complexity of the election process and solves the issue of a single point of failure. OLE proposes a hybrid model to get the advantage of leader election and decentralization simultaneously.

6. Methodology and Model

As mentioned earlier, AAL's data and services have five categories, and integrating them into the blockchain requires considering their sensitivity to time and specialization. Thus, AAL transactions are classified into three classes: special-sensitivity, time- sensitivity, and non-sensitivity. The special-sensitivity transactions need fast and specialized approval; the time-sensitive transactions need fast approval; and the non-sensitivity transactions can follow the regular blockchain procedure, as explained in Table 1.

Table 1.
AAL's transactions classification.

Class of transaction	AAL categories
Special-sensitive	Transactions in the services of healthcare and social-care
Time-sensitive	Transactions for the services of smart homes, security, and safety
Non-sensitive	Transactions on the services of IoT and machine learning

On the other hand, blockchain has two main features, as follows:

- Decentralized Actions: transactions are first verified by individuals. Next, they form a block and submit their proposal to the others. Afterwards, the majority's votes validate and approve the block .

- Decentralized storage: Each node in the blockchain maintains a copy of the storage (ledger).

We introduce the idea of a two digits vector to represent the blockchain features that are mentioned above. For example, (1, 1) represents a blockchain procedure that completely satisfies both features; (0.5, 0, 5) represents a blockchain procedure that partially satisfies both features; and (0, 0) represents a blockchain procedure that does not satisfy both features.

According to AAL's classes and blockchain features, the OLE protocol has three procedures based on the transactions' classes. At the beginning, sensors, applications, and data resources should produce transactions in three pools.

Firstly, the first pool is for special-sensitive transactions, and it is processed using the (0, 1) blockchain procedure, where the transactions are committed directly and take effect on the main memory (assets) without votes. Therefore, the service is delivered, and it is added to the proposed block. Afterwards, we hash the proposed block and link it to the ledger without requiring additional validation. This relaxes blockchain procedures for the efficiency of AAL. Indeed, the feature of decentralized action is not satisfied (the first digit of the vector is 0), while the feature of decentralized storage is satisfied (the second digit of the vector is 1).

In fact, as shown in Figure 1, the first pool has five sub-pools for medical, dental, psychological, social, and pharmaceutical transactions. Consequently, there are five queues of specialized miners: doctor queue DQ, dentist queue DnQ, psychologist queue PQ, socialist queue SQ, and pharmacist queue PhQ. The doctors are enqueued in DQ, and the head of the DQ, denoted as DQHead, is directly elected as a leader. This allows the leader to approve and commit the transaction without any competition or voting. In addition, the leader is able to transfer the transaction to any other specialist if needed. Moreover, for each queue, we use a linked-list queue, and every time cycle, or in case the leader fails, the head pointer moves to the next spot in the queue, and previous head data is deleted. This makes the leader election process fast, and the time complexity = 1.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 223-235, 2024
DOI: 10.55214/25768484.v8i3.930

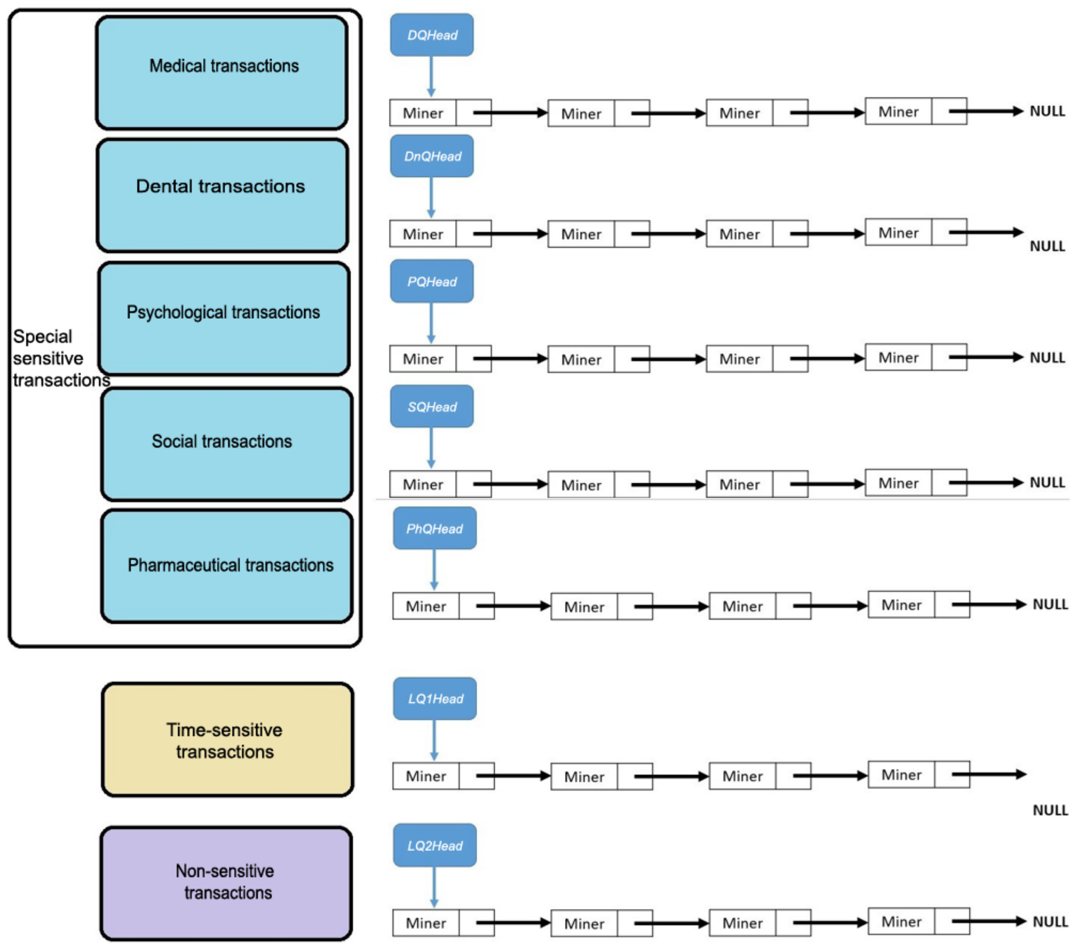

Figure 1.
Transactions' pools and the corresponding queues.

Secondly, the second pool is for time-sensitive transactions. It is processed using the (0.5, 1) blockchain procedure, where the transactions are committed based on the votes of three miners. Later on, those approved transactions are grouped in one block, hashed, and linked to the ledger without extra validation. Indeed, the feature of decentralized action is partially satisfied (the first digit of the vector is 0.5), where three miners vote on the transactions' committing, but they do not vote on the block validation. On the other hand, the feature of decentralized storage is satisfied (the second digit of the vector is 1). In fact, Figure 1 shows time-sensitive transactions, where a group of trustworthy miners are enqueued in the leader's queue LQ1, and they cooperate in proposing a new block by verifying transactions together. When at least three miners verify a transaction, it becomes committed and affects the main memory (assets). Therefore, the service is delivered, and it is added to the proposed block. As the block fills up, we hash it and link it to the ledger, eliminating the need for further validation. This enables decentralization of transactions' verification but relaxes the block validation process, which partially influences the blockchain decentralized action for AAL considerations.

Thirdly, the third pool is for non-sensitive transactions, as shown in Figure 1. It is processed using the (1, 1) blockchain procedure. A group of trustworthy miners are enqueued in the leader's queue LQ2, and each cycle the head of the queue (the leader) proposes a new block. Then, the other miners in the queue validate the proposed block to commit or abort it. If it is committed, the transactions' processes take effect on the main memory, the services are delivered, and the block is linked to the ledger.

6.1. Model Architecture

As shown in Figure 2, our model combines three layers of AAL and two layers of blockchain, for a total of five layers. The first layer is the perception layer, which has sensors, IoT, mobiles, PCs, and software applications. The second layer is the network layer, which can be public or private according to the data sensitivity. The third layer is the transactions layer, where transactions are grouped into three pools, as mentioned earlier. The fourth layer handles the verification and committing of transactions, delivering the services. The fifth layer is the storage layer, where the validated blocks are chained to all copies of the ledger.

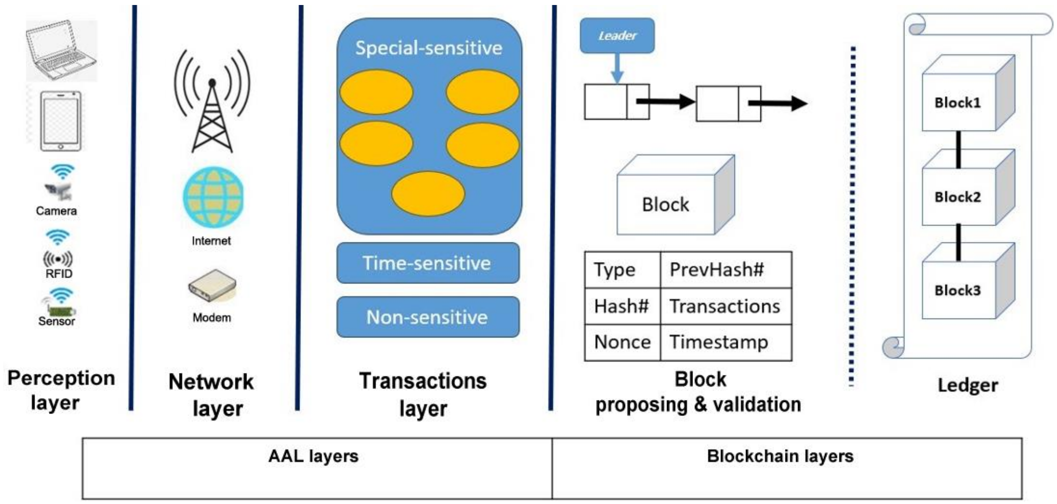

Figure 2.
Model architecture.

6.2. Algorithm

Algorithm 1 illustrates blockchain procedure, focusing on the process of block proposing. According to the source of transaction T_j, it goes to a specific pool, which can be 1, 2 or 3. For pool = 1 there are five sub-pools donated as $pool_i$ and every sub-pool has a leader, donated as L_i. The first case represents special-sensitive transactions (in line 5), where the leader L_i approves T_j and adds it to $block_k$ for proposing. Otherwise, T_j is aborted.

The second case represents time-sensitive transactions (in line 13), where there are multiple leaders. When a leader approves T_j, it increases a counter. When T_j is approved by three leaders, it is added to $block_k$ for proposing. Otherwise, T_j is aborted.

The default case represents non-sensitive transactions (in line 23), where a leader L_i verifies T_j and add it to $block_k$ for proposing. Otherwise, T_j is aborted.

In addition, Algorithm 2 illustrates blockchain procedures for the processes of block validation and storage. Indeed, each type of transaction is stored in a specific block. The special-sensitive transactions grouped in blockType = 1 (in line 4), where $block_k$ is sent to all nodes, so they add it to their copies of the ledger.

The same thing is applicable for the $block_k$ of time-sensitive transactions. While the $block_k$ of non-sensitive transactions has to be sent to all nodes, and they validate it and vote 1 for valid or 0 for invalid. Next, the vote of the majority is calculated and if the majority approves the block, it is added to the ledger; otherwise, $block_k$ is aborted.

7. Features and Rewarding Management

In this section, we introduce the features and rewarding strategies of the OLE protocol. Firstly, the main features of our protocol are illustrated below:

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 223-235, 2024
DOI: 10.55214/25768484.v8i3.930

• Reward types: having different amounts and kinds of rewards gives more flexibility to the system.

• Trustworthiness and specialization: trustworthiness and specialization are very important to be considered for critical transactions, including processes and services.

• Efficiency: the rewarding strategies should be aligned with the efficiency of AAL (e.g., real-time processing and privacy) and blockchain (e.g., decentralization).

• Motivation: The rewarding strategies should motivate all nodes to participate.

• Fairness: the nodes with high capabilities should get credit for that, while the nodes with low capabilities should get fair chances to compete and to gain some rewards.

At the beginning, we have three types of rewards: cryptocurrency, social service credits, and the trustworthy credit trust that is maintained to participate again. Therefore, there are two amounts of rewards: A or B, where A is a specific positive amount that is greater than task's cost (A > cost) and B is a specific negative amount. Additionally, there are two amounts of credit, which are a or b, where a is a specific positive credit that is added to trust credit and b is a specific negative amount that is cut from trust credit.

Algorithm 1: Block proposal

```
//Initialization:
Input: i, j, k, pool; //Indexes of leader, transactions, block and pool
counter =0;
Switch (pool):
Case pool=1:
    L→pool_i (T_j); //A leader verifies a transaction from corresponding pool
    if (T_j)
        T_j →commit(); //If T_j is correct, it is committed
        T_j →blook_k; //The committed T_j is added to the proposed block
    else
        T_j →abort(); //If T_j is not correct, it is aborted
break;
Case pool=2:
    L→pool_i (T_j); //A leader verifies a transaction from corresponding pool
    if (T_j)
        T_j.counter++; //The T_j counter is increased
        if (T_j.counter==3)
            T_j →commit(); // If T_j is verified by three leaders, it is committed
            T_j →blook_k; //The committed T_j is added to the proposed block
        else
            T_j →abort(); //If T_j is not correct, it is aborted
break;
default:
    L→pool_i (T_j); //A leader verifies a transaction from corresponding pool
    if (T_j)
        T_j →blook_k; // T_j is added to the proposed block
    else
        T_j →abort(); //If T_j is not correct, it is aborted
```

Now for special-sensitive transactions, we investigate the rewarding strategies in-light of the above features. Firstly, we value the importance of trustworthiness and specialization, which are satisfied by enabling specialized members to only verify transactions, commit them, and store them in blocks and ledgers. Secondly, the efficiency of AAL is satisfied as the specialized member verifies transactions and commits them in a real-time manner. The blockchain is used as a decentralized storage, which provides security and privacy, but we compromise the blockchain's actions with decentralization over time. Thirdly, fairness is guaranteed for specialized members, and non-specialized members cannot participate. In fact, every participant is enqueued at the tail of the queue and moves on until it becomes the leader, and then it gets the chance. The leader is switched every specific cycle (predefined) or in case of failure. A new leader is elected by moving the head pointer to the next position in the queue, while the previous leader is dequeued and can be enqueued again at the tail. Fourthly, motivation is given to the specialized members, even if they have low capabilities. Actually, they are not supposed to have high capabilities as they do not compete in processing or staking, as in PoW or PoS. Fifthly, if the processing result is correct, the reward is A and trust = trust + a; and if the processing result is not correct, the reward is B. Any specialized member node gets B, cannot participate in this level again, and its trust becomes 0.

Algorithm 2: Block validation and approval

```
//Initialization:
Input: blockType; //Index of block type
Switch (pool):
Case blockType =1:
    Cast(block_k); // Send block_k to all other nodes
    block_k →Ledger; //Every node adds block_k to its copy of the Ledger
break;
Case blockType =2:
    Cast(block_k); // Send block_k to all other nodes
    block_k →Ledger; //Every node adds block_k to its copy of the Ledger
break;
default:
    Cast(block_k); // Send block_k to all other nodes
    if (block_k)
        vote(1);
    else
        Vote(0);
    WaitForOtherVotes();//it waits for other votes and returns the majority
    if (majority)
        block_k →Ledger; //Every node adds block_k to its copy of the Ledger
    else
        block_k →abort();
```

Moreover, for time-sensitive transactions, we also value the importance of trustworthiness, which is satisfied by enabling trustworthy members only to be in the queue while specialized members can also participate. Secondly, the efficiency of AAL is satisfied as the trustworthy members verify transactions and commit them in an almost real-time manner. The blockchain decentralization is partially satisfied since at least three trustworthy members have to verify a transaction to commit. Blockchain is also used as a decentralized storage, which provides security and privacy. Thirdly, fairness is guaranteed only for trustworthy members since they follow the queue order. All the nodes in the queue are considered leaders and fairly competitive. Any leader is dequeued every specific cycle (predefined) or, in case of failure, a new leader will join. Fourthly, motivation is given to the trustworthy members through the total credit of rewards, even if they have low capabilities. To build trustworthy credits, the member has to participate in the non-sensitive level first. Fifthly, if the processing result is correct, the reward is A and trust = trust

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 223-235, 2024
DOI: 10.55214/25768484.v8i3.930

+ a. If the processing result is not correct, the reward is B. Any node that gets B cannot participate in this level again, and its trust becomes 0.

Furthermore, for non-sensitive transactions, the application of the full blockchain procedure ensures greater transparency, thereby satisfying trustworthiness. In contrast, the specialization is not important at this level. Secondly, the efficiency of AAL is fully satisfied as any member verifies transactions, proposes them, and the others vote on them. This does not satisfy real-time processing, which is not important at this level. The blockchain decentralization is fully satisfied, and it is also used as a decentralized storage, which provides security and privacy. Thirdly, the fairness is guaranteed for all members since they follow the queue order. The head of the queue can propose a new block, and the other nodes in the queue can validate it. The leader is dequeued every specific cycle (predefined) or, in case of failure, a new leader is elected. Fourthly, motivation is given to all members by rewarding all nodes for proposing and validating, even if they have low capabilities. Fifthly, if the processing result is correct, the reward is A and trust = trust + a. If the processing result is not correct, the reward is B and trust = trust − b.

Clearly Table 2 summarizes the analysis of the features of the proposed protocol.

Table 2.
Rewarding strategies.

Features	Special-sensitive	Time-sensitive	Non-sensitive
Trustworthiness & specialization	Yes	Yes	Fully for trustworthiness but not for specialization
Efficiency	Fully for AAL and partially for blockchain	Fully for AAL and almost fully for blockchain	Fully for AAL and blockchain
Fairness	Only for specialized members	Only for trustworthy members	For all
Motivation	Only for specialized members	Only for trustworthy members	For all

8. Experimental Results

This part shows the experimental simulation of the proposed OLE protocol for blockchain and AAL. It compares the proposed procedure with the original blockchain procedure. The experiment runs on a machine with an Intel Core (TM) i7 CPU, 2.90 GHz, and 4 GB (RAM). We repeat each test ten times, and then we take the average.

As explained earlier, using the OLE of blockchain, there are three types of procedures that produce three types of blocks. Essentially, we generate 12,000 transactions and divide them into three pools, each containing 4000 transactions. The three pools have special-sensitive, time-sensitive, and non-sensitive transactions. We build a blockchain network of ten nodes. A queue comprises three nodes. The queues' leaders create blocks of size 100, validate, and add to the ledgers according to the proposed procedures.

Figure 3 illustrates the execution time of the OLE protocol for blockchain and AAL, in comparison with the original blockchain procedure (using PoQ as a consensus protocol). The OLE reduces the execution time by about 51% in comparison to the original blockchain model. In addition, Figure 4 shows the detailed execution time of the OLE protocol in comparison with the original blockchain. It shows the execution time of special-sensitive, time-sensitive, and non-sensitive blocks out of the total execution time. Indeed, the original blockchain procedure verifies transactions, groups them in a block, sends the block for validation, nodes validate and vote on the block's correctness, and finally stores the block in the ledger. However, OLE approves special-sensitive transactions, groups them in a block, and all nodes store the block in the ledger. OLE also approves time-sensitive transactions by at least three miners, groups them in a block, and all nodes store the block in the ledger.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 3: 223-235, 2024
DOI: 10.55214/25768484.v8i3.930

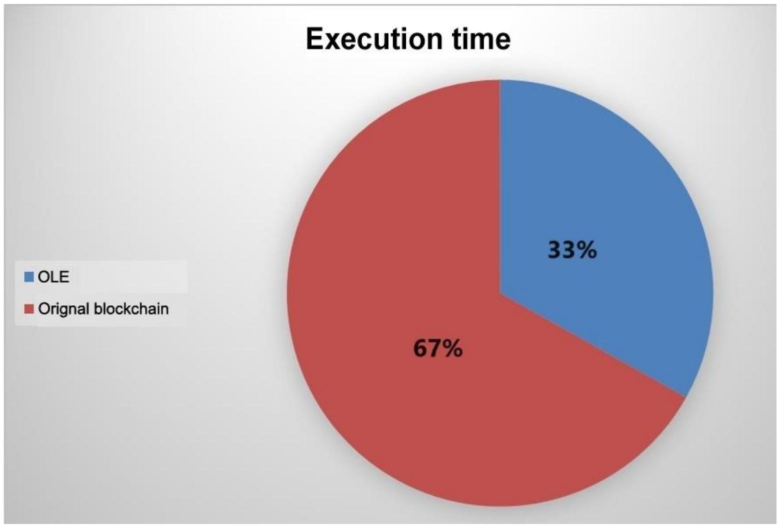

Figure 3.
Execution time of OLE in comparison with original blockchain.

These fast procedures reduce the execution time and satisfy AAL requirements. Note that OLE treats non-sensitive transactions just like the original blockchain procedure.

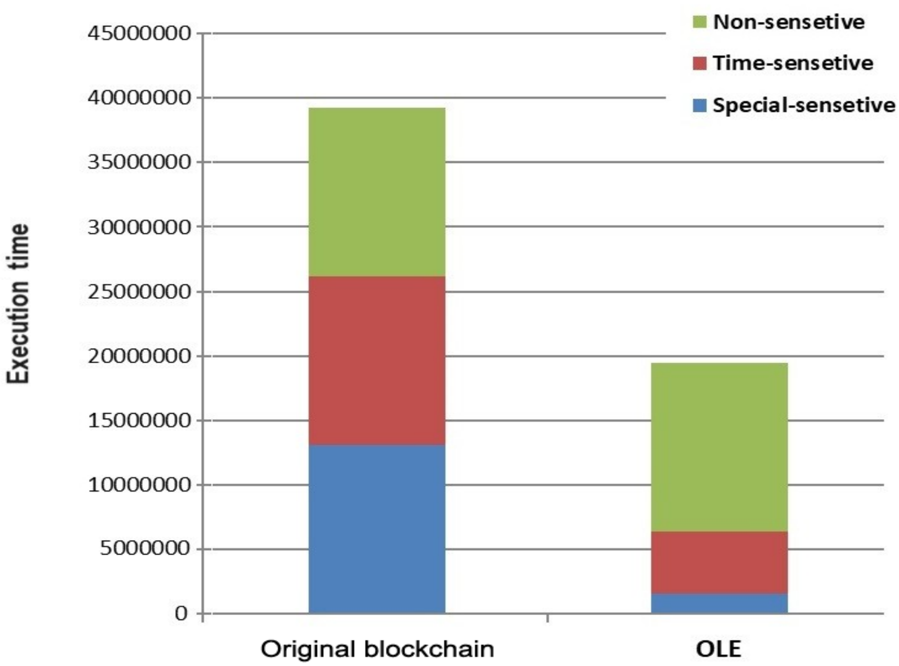

Figure 4.
Detailed execution time of OLE including the three kinds of transactions in comparison with original blockchain.

9. Conclusions

The paper introduces the OLE protocol, which is supported by a specific blockchain model and procedure to solve the issue of latency and to consider the specialized decisions that are required by AAL systems. It classifies the blocks into special-sensitive, time-sensitive, and non-sensitive classes, where each class has a suitable procedure. Each procedure is supported by a specific rewarding strategy. The use of OLE allows for a speed up in execution time of 51% in comparison to the original blockchain model. The future work has to consider smart transactions and block classification instead of being pre-programmed.

Funding:
This study received no specific financial support.

Institutional Review Board Statement:
Not applicable.

Transparency:
The author confirms that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Competing Interests:
The author declares that there are no conflicts of interests regarding the publication of this paper.

Copyright:

References

[1] A. Purwanto, J. T. Purba, R. Sijabat, and I. Bernarto, "The role of transformational leadership, organizational citizenship behaviour, innovative work behaviour, quality work life, digital transformation and leader member exchange on universities performance," *Linguistics Antverpiensia*, vol. 399, no.2, p. 2908 – 2932, 2021.

[2] K. Haraldstad *et al.*, "A systematic review of quality of life research in medicine and health sciences," *Quality of life Research*, vol. 28, pp. 2641-2650, 2019.

[3] M. Uysal, A. Berbekova, and H. Kim, "Designing for quality of life," *Annals of Tourism Research*, vol. 83, no. 1, p. 102944, 2020.

[4] J. C. F. De Guimarães, E. A. Severo, L. A. F. Júnior, W. P. L. B. Da Costa, and F. T. Salmoria, "Governance and quality of life in smart cities: Towards sustainable development goals," *Journal of Cleaner Production*, vol. 253, p. 119926, 2020. https://doi.org/10.1016/j.jclepro.2019.119926

[5] G. Cicirelli, R. Marani, A. Petitti, A. Milella, and T. D'Orazio, "Ambient assisted living: A review of technologies, methodologies and future perspectives for healthy aging of population," *Sensors*, vol. 21, no. 10, p. 3549, 2021. https://doi.org/10.3390/s21103549

[6] R. Maskeliūnas, R. Damaševičius, and S. Segal, "A review of internet of things technologies for ambient assisted living environments," *Future Internet*, vol. 11, no. 12, p. 259, 2019. https://doi.org/10.3390/fi11120259

[7] A.-I. Florea, I. Anghel, and T. Cioara, "A review of Blockchain technology applications in ambient assisted living," *Future Internet*, vol. 14, no. 5, p. 150, 2022.

[8] A. Mkpa, J. Chin, and A. Winckles, "Holistic blockchain approach to foster trust, privacy and security in IoT based ambient assisted living environment," in *Proceedings of the 2019 15th International Conference on Intelligent Environments (IE), IEEE*, 2019, Ed., 2019, vol. 414, pp. 52–55.

[9] B. Assiri and W. Z. Khan, "Enhanced and lock-free tendermint blockchain protocol," in *Proceedings of the 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), IEEE*, 2019, pp. 220–226.

[10] B. Assiri and W. Z. Khan, "Fair and trustworthy: Lock-free enhanced tendermint blockchain algorithm," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 4, pp. 2224-2234, 2020. https://doi.org/10.12928/telkomnika.v18i4.15701

[11] L. Ismail and H. Materwala, "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions," *Symmetry*, vol. 11, no. 10, p. 1198, 2019. https://doi.org/10.20944/preprints201908.0311.v1

[12] A. C. Eldh, I. Ekman, and M. Ehnfors, "A comparison of the concept of patient participation and patients' descriptions as related to healthcare definitions," *International Journal of Nursing Terminologies and Classifications*, vol. 21, no. 1, pp. 21-32, 2010. https://doi.org/10.1111/j.1744-618x.2009.01141.x

[13] J. Hegarty *et al.*, "An international perspective on definitions and terminology used to describe serious reportable patient safety incidents: A systematic review," *Journal of Patient Safety*, vol. 17, no. 8, p. e1247, 2021. https://doi.org/10.1097/pts.0000000000000700
[14] Y. Kelly, N. O'Rourke, R. Flynn, J. Hegarty, and L. O'Connor, "Definitions of health and social care standards used internationally: A narrative review," *The International Journal of Health Planning and Management*, vol. 38, no. 1, pp. 40-52, 2023. https://doi.org/10.1002/hpm.3573
[15] G. Marques, "Ambient assisted living and internet of things," *Harnessing the Internet of Everything (IoE) for Accelerated Innovation Opportunities*, pp. 100-115, 2019.
[16] A. Vulpe *et al.*, "IoT security approaches in social robots for ambient assisted living scenarios," in *Proceedings of the 2019 22nd International Symposium on Wireless Personal Multimedia Communications (WPMC), IEEE*, 2019, vol. 432 pp. 1–6.
[17] M. A. Choukou, A. Polyvyana, Y. Sakamoto, and A. Osterreicher, "Ambient assisted living technologies to support older adults' health and wellness: A systematic mapping review," *European Review for Medical & Pharmacological Sciences*, vol. 25, no. 12, pp. 4289-4307, 2021.
[18] M. A. Qureshi, K. N. Qureshi, G. Jeon, and F. Piccialli, "Deep learning-based ambient assisted living for self-management of cardiovascular conditions," *Neural Computing and Applications*, pp. 1-19, 2021. https://doi.org/10.1007/s00521-020-05678-w
[19] A. Manocha, Y. Afaq, and M. Bhatia, "Digital Twin-assisted Blockchain-inspired irregular event analysis for eldercare," *Knowledge-Based Systems*, vol. 260, p. 110138, 2023. https://doi.org/10.1016/j.knosys.2022.110138
[20] J. Rodrigues and A. Cardoso, "Blockchain in smart cities: An inclusive tool for persons with disabilities," *Proceedings of the 2019 Smart City Symposium Prague (SCSP), IEEE*, pp. 1–6, 2019.
[21] S. Wazalwar and U. Shrawankar, "Community cloud service model for people with special needs," *Cloud Computing Technologies for Smart Agriculture and Healthcare*, pp. 47-55, 2021. https://doi.org/10.1201/9781003203926-4
[22] M. Poblet, D. W. Allen, O. Konashevych, A. M. Lane, and C. A. Diaz Valdivia, "From athens to the Blockchain: Oracles for digital democracy," *Frontiers in Blockchain*, vol. 3, p. 41, 2020. https://doi.org/10.3389/fbloc.2020.575662
[23] B. Cao *et al.*, "Performance analysis and comparison of PoW, PoS and DAG based blockchains," *Digital Communications and Networks*, vol. 6, no. 4, pp. 480-485, 2020. https://doi.org/10.1016/j.dcan.2019.12.001
[24] S. Fahim, S. Rahman, and S. Mahmood, "Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV," *International Journal of Mathematics and Mathematical Sciences Computer*, vol. 3, pp. 46-57, 2023. https://doi.org/10.5815/ijmsc.2023.03.04
[25] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432-1465, 2020. https://doi.org/10.1109/comst.2020.2969706
[26] S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," *Expert Systems with Applications*, vol. 168, p. 114384, 2021. https://doi.org/10.1016/j.eswa.2020.114384
[27] D. P. Oyinloye, J. S. Teh, N. Jamil, and M. Alawida, "Blockchain consensus: An overview of alternative protocols," *Symmetry*, vol. 13, no. 8, p. 1363, 2021.
[28] S. P. Yadav, K. K. Agrawal, B. S. Bhati, F. Al-Turjman, and L. Mostarda, "Blockchain-based cryptocurrency regulation: An overview," *Computational Economics*, vol. 59, no. 4, pp. 1659-1675, 2022. https://doi.org/10.1007/s10614-020-10050-0
[29] M. H. Ur Rehman, K. Salah, E. Damiani, and D. Svetinovic, "Trust in blockchain cryptocurrency ecosystem," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1196-1212, 2019. https://doi.org/10.1109/tem.2019.2948861
[30] S. Hakak *et al.*, "Recent advances in blockchain technology: A survey on applications and challenges," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 38, no. 1-3, pp. 82-100, 2021.
[31] V. Nehra, U. Rungta, and B. Choudhury, "Blockchain enabled ambient assisted living for critically ill patients," in *Proceedings of the 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), IEEE*, 2021, pp. 575–581.
[32] B. I. Mohideen and B. Assiri, "Internet of Things (IoT): Classification, secured architecture based on data sensitivity, security issues and their countermeasures," *Journal of Information & Knowledge Management*, vol. 20, p. 2140001, 2021.
[33] M. Numan, F. Subhan, W. Z. Khan, B. Assiri, and N. Armi, "Well-organized bully leader election algorithm for distributed system," in *Proceedings of the 2018 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), IEEE*, 2018, pp. 5–10.
[34] T. G. Tan, V. Sharma, and J. Zhou, "Right-of-Stake: deterministic and fair blockchain leader election with hidden leader," in *Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE*, 2020, pp. 1–9.
[35] W. Fu, X. Wei, and S. Tong, "An improved blockchain consensus algorithm based on raft," *Arabian Journal for Science and Engineering*, vol. 46, no. 9, pp. 8137-8149, 2021. https://doi.org/10.1007/s13369-021-05427-8
[36] D. Catalano, D. Fiore, and E. Giunta, "Adaptively secure single secret leader election from DDH," in *Proceedings of the Proceedings of the 2022 ACM Symposium on Principles of Distributed Computing*, 2022, pp. 430–439.