National College of Ireland

Verification of participants in task offloading to volunteered mobile devices using a Blockchain-based incentive mechanism

MSc Research Project
Cloud Computing

Tamunobelema Miebaka-Ogan
Student ID: 20231890

School of Computing
National College of Ireland

Supervisor: Sean Heeney

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Tamunobelema Miebaka-Ogan
Student ID:	20231890
Programme:	Cloud Computing **Year:** 2022
Module:	MSc Research Project
Supervisor:	Sean Heeney
Submission Due Date:	15/08/2022
Project Title:	Verification of participants in task offloading to volunteered mobile devices using a Blockchain-based incentive mechanism
Word Count:	6881 **Page Count** 20

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: .....

Date: 13/08/2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Verification of participants in task offloading to volunteered mobile devices using a Blockchain-based incentive mechanism

Tamunobelema Miebaka-Ogan
20231890
MSc in Cloud Computing

15th August 2022

Abstract

Over the years, there has been an increase in the complexity of tasks that mobile application developers and mobile device users wish to perform on mobile devices. Sadly, this increase in the complexity of tasks has not been matched by the capabilities of most mobile devices. This is because mobile devices still suffer resource constraints in terms of memory, battery capacity, and computational capacity. Furthermore, in this era of machine learning and data mining, certain use cases like computational photography, optical character recognition, text and image labeling have made their way to mobile devices, but a high percentage of mobile devices are unable to perform these tasks. To address this issue, task offloading to volunteered mobile devices that are capable of performing these complex tasks has been identified as a possible solution. However, this comes with the challenge of incentivizing the owners of capable devices to volunteer their devices, and addressing concerns regarding security, trustworthiness, and privacy among both parties involved in the task offload process. This paper explored using a blockchain-based incentive mechanism to verify the participants in task offloading to volunteered mobile devices without compromising their privacy in order to address these concerns while enabling resource constrained devices to offload tasks. The evaluations conducted showed that the developed blockchain-based incentive mechanism enabled the verification of both parties involved in the task offloading without compromising their privacy based on pseudo-anonymity, and without adding any significant overhead to any of the stages involved in the task offloading process.

1 Introduction

Mobile devices have become an integral part of everyday activities for many people. They offer services like maps, photography, storage, and entertainment to mention a few. Furthermore, there has been an increase in the complexity of the tasks that application developers and owners of mobile devices intend to perform using their devices. Tasks like computational photography, optical character recognition, data mining and analysis, face detection, and analysis have use cases in applications running on mobile devices. However, most mobile devices struggle to execute these tasks because they are limited

by their constrained resources in terms of memory, battery capacity and computational capacity. To address this issue, task offloading has been identified as a solution.

Task offloading involves offloading a task from a resource-constrained device to a device capable of executing the offloaded task and returning the result to the constrained device. According to Buyya et al. (2018), the typical task offloading approach in the mobile cloud computing sector involves offloading tasks to cloud servers that execute these tasks and return the result to the mobile devices that own the task. Some of the problems with this approach are that it does not always guarantee the benefit of task offloading because it suffers from latency due to network bandwidth and connectivity challenges and it also comes at a cost to the application developers who have to pay to utilize servers provided by cloud platforms to execute these offloaded tasks. To address the latency and cost issues from task offloading to cloud servers, offloading tasks to a hybrid system that combines cloud resources and nearby volunteered mobile devices has been proposed because it solves both the cost and latency issues.

However, task offloading to volunteered mobile devices requires that the volunteers are incentivized to provide the redundant resources on their mobile devices to execute the offloaded task. It also requires that the concerns regarding the privacy and the verification of participants are addressed. Furthermore, various incentive mechanisms for task offloading to volunteered devices have been proposed by researchers, but a shortcoming of most of these suggested incentive mechanisms is that they do not address the verification of participants. A challenge that the verification of participants presents is how to verify their identities without compromising their privacy.

Blockchain technology provides the possibility of protecting personal user data by providing them a pseudo-identity that can be verified. Although initially proposed in Nakamoto (2008) for Bitcoin, the technology has grown beyond that with various applications of the technology now being explored. A major example of this is Ethereum, a blockchain-based decentralised computing platform that allows applications to run the blockchain using smart contracts. Zyskind et al. (2015), Malik et al. (2018), Zhao & Liu (2019), Gutiérrez-Agüero et al. (2021) and Ren et al. (2021), have explored using blockchain technology for identity management in order to avoid users sharing their private information to third party applications that can exploit them. Their research have shown that blockchain can be used to verify a user by assigning a pseudo-identity to the user and verifying their activity on the platform using the address associated with them on the blockchain.

Therefore, this paper explores using a blockchain-based incentive mechanism to verify participants in task offloading without compromising their privacy. It proposes a combination of cloud computing and volunteer computing. Cloud computing is used for storing the data related to the offloaded tasks as cloud service providers are regulated by data protection laws. And volunteered mobile devices that have been registered and verified using the blockchain-based incentive mechanism are used to execute the offloaded tasks.

1.1 Research Question

The aim of this paper is to answer the question;

> *Can a Blockchain-based incentive mechanism for offloading tasks to volunteered mobile devices in mobile cloud computing lead to the verification of involved participants without comprising privacy?*

To answer this question, the following objectives have been set for this paper;

- Research the state of the art in task offloading, volunteer computing and blockchain based identity management.
- Design and implement a task offloading application that uses a blockchain based incentive mechanism to verify participants without compromising their privacy.
- Evaluate the performance of the application and incentive mechanism developed.

The contributions of this research paper are;

- An android application that performs face detection and optical character recognition on the device.
- A hybrid cloud based mechanism that offloads face detection and optical character recognition tasks to volunteered mobile devices.
- A blockchain based incentive mechanism that allows the verification of the participants involved in task offloading without compromising their privacy.

The rest of this report is divided into the following sections. Section 2 discusses the related works, Section 3 explains the methodology used in the paper, Section 4 describes the design specifications, Section 5 discusses the implementation, Section 6 details the evaluation conducted and Section 7 concludes the paper discussing observations and future works.

2 Related Work

This section discusses the work that has been done so far in key concepts that make up the topic of this research. It reviews papers on task offloading, explaining and comparing various mechanisms that have been employed. Then it discusses the incentive mechanisms that have been suggested and implemented for volunteered mobile devices by various researchers. This is followed by a discussion on the reviewed literature related to blockchain based identity management and then it concludes highlighting the need for the research done in this paper.

2.1 Task Offloading to Volunteered Devices

With the introduction and success of cloud computing, task offloading from resource constrained devices to cloud servers has been identified as a solution to the challenge of performing resource intensive tasks on resource constrained mobile devices. This was highlighted by Buyya et al. (2018), where they discussed some of the applications of mobile cloud in relation to empowering resource constrained devices. They also mentioned some of the challenges faced by researchers which are, developing the right offloading approach, identifying methods that are resource-intensive so they can be offloaded and designing code offloading mechanisms that consider the context of both the device and the cloud. Liu et al. (2016), Zhou et al. (2017), Alonso-Monsalve et al. (2018), Shi et al. (2018) and Sulaiman & Barker (2019) have identified that task offloading to the cloud is not always beneficial to the offloading device because it suffers from latency caused by

limited network bandwidth and unstable network connections. This latency issues results in battery drainage on the device offloading the task and prolong the execution time of the task thereby defeating the purpose of task offloading.

To solve the problem mentioned above, researchers have looked into offloading code to volunteered nearby devices. There are various approaches such as offloading tasks to cloudlets. Offloading tasks to mobile devices using the Internet, Bluetooth or WiFi-Direct. And offloading tasks to a hybrid cloud that makes use of nearby volunteered devices. Shi et al. (2018) proposed a mechanism for code offloading that evaluated the reliability of nearby cloudlets based on the prediction of the user's mobility before deciding which cloudlets to offload task to. The aim of their research was to reduce the failure of task offloading caused by the users mobility. Lu et al. (2020) proposed a framework for code offloading that made use of cloudlets to offload task to nearby mobile devices through Bluetooth and WiFi-Direct considering energy consumption. Sulaiman & Barker (2019) designed a code offloading mechanism that made the decision on the destination for offloaded code based on the evaluation of offloading scores of the mobile device and previous execution of offloaded tasks. It considered various cloud service providers, cloudlets and nearby mobile devices as possible destinations. The aim of their approach was to reduce battery consumption and the task execution time. Liu et al. (2016) and Zhou et al. (2017) proposed a context-aware framework for computation offloading. They both designed code offloading mechanisms that considered offloading code to nearby devices as an alternative to the typical approach of offloading task to a remote server. However, Liu et al. (2016) only considered offloading tasks to cloudlets as an alternative while Zhou et al. (2017) proposed code offloading to heterogeneous mobile cloud. A key benefit of offloading code to nearby volunteer mobile devices is that it can be done using offline wireless technology like WiFi-direct and Bluetooth which address the issue of latency suffered when offloading to the cloud. However, this suffers when there are no available nearby devices and is affected by the mobility of the device. It also offers limitation in regards to the tasks that can be executed.

Furthermore, with the resource constraints of mobile devices, offloading tasks to a hybrid system that combines cloud resources and volunteered mobile devices offers the best of both worlds. It provides more capability to execute the offloaded task while reducing the cost spent on cloud resources as some of the services are provided by the volunteered device. Alonso-Monsalve et al. (2018), proposed a heterogeneous mobile cloud computing model for hybrid clouds that suggested that part of the cloud resources be provided by volunteered devices. Their evaluation showed that the approach would be beneficial for cloud services with a substantial amount of mobile users. The addition of volunteered devices as stated by Alonso-Monsalve et al. (2018) reduces the cost spent on cloud resources which will be very appealing to application developers. They also argued that code offloading to volunteered mobile devices is the cheaper option when compared to code offloading to cloudlets because of the cost of the infrastructure required to setup cloudlets.

In conclusion, the research conducted in this paper builds on the work done by Alonso-Monsalve et al. (2018), using volunteered mobile devices to perform the processing service for offloaded tasks while the storage service is performed by the cloud. However, it differs from their approach by using blockchain technology to provide an incentive that allows the verification of participants without compromising their privacy.

2.2 Incentives for Task Offloading to Volunteered Devices

Task offloading to volunteered mobile devices require that the owners of the devices are offered an incentive. This is to encourage the owners of these devices to volunteer their devices to execute tasks offloaded by others as stated in Alonso-Monsalve et al. (2018). Zhou et al. (2019) also highlight privacy as a concern for volunteers that affects task offloading to volunteer devices. This sections reviews some of the incentive mechanisms proposed in existing literature.

Various authors have looked into developing different incentive mechanisms for different task offloading systems. Zhou et al. (2019) proposed an auction based incentive mechanism for task offloading to heterogeneous mobile cloud. Their approach used a central controller to handle the auction of services by volunteer devices in a reverse auction market. Wang et al. (2017) also used a centralised auction mechanism to assign both heterogeneous tasks and homogeneous tasks to volunteer devices and determine their payment. An alternative approach was taken by Wang et al. (2021), where a distributed auction mechanism was used to handle the assigning of offloaded task. The benefit of their approach is that it reduces the overhead of updating a central controller of the status of the devices available on the platform however it limits the number of volunteered device to only those connected with offline wireless technologies like WiFi-Direct and Bluetooth. A distributed auction mechanism also limits the mobility of the devices. This challenge was addressed by Khaledi et al. (2016) with an incentive mechanism that offloaded tasks to a group of nearby volunteer devices that worked together to execute the offloaded tasks that had been broken into smaller parts. In their approach, the volunteer devices were rewarded based on the size of the task done. And to address the mobility issue, their auction mechanism performed auctions at intervals to replace the lost devices with new ones that entered the network. However, this came with an overhead introduced by the repeated auctions and the disconnection of devices due to the range restriction of the connection used. They also highlighted privacy as a concern for volunteers.

Furthermore, Anderson (2019) proposed a credit system as an incentive for volunteers that executed offloaded tasks. The credit were calculated based on the estimated FLOPs used to execute the offloaded tasks. The targets set for this credit system were;

- It should be device neutral. This means that devices with less or more computation capability should be rewarded the same for executing the same task.
- It should be task neutral. This means that the reward for the different tasks executed should be the same.
- It should resist credit cheat. This means that it should avoid rewarding devices for task not done.

However, the various incentive mechanisms proposed in the reviewed literature for offloading task to volunteered devices did not provide a way to verify the participants without compromising their privacy which was highlighted as a concern. Hence, the reason for the proposed blockchain-based incentive mechanism for rewarding and verifying participants in task offloading to volunteered mobile devices in this paper. Furthermore, the application of blockchain-based incentive mechanisms have been researched in crowdsensing which shares some similarity with task offloading to volunteer devices in terms of volunteer devices performing sensing task using their sensors. However, it differs because these volunteer devices do not perform any computation and it is not task offloading due to

resource constraint but rather to get sensor data. These applications are discussed in the subsection below.

2.2.1 Blockchain-based Incentive Mechanism

The application of blockchain-based incentive mechanism has been researched in crowdsensing to reward participants and preserve privacy. In Wang et al. (2018), a blockchain-based incentive mechanism was used to preserve privacy in applications for crowdsensing. One of their reasons for selecting blockchain was because of the decentralised yet provable characteristic of its cryptocurrencies. This is due to it not having a central authority but instead multiple computers provide their resources to validate transactions. In their developed mechanism, a server publishes a sensing task with a reward and quality requirement. Smartphone users then perform the sensing task and provide the data to miners that verify the data based on the standard set by the server before rewarding the smartphone users. They used K-anonymity by splitting the verification task in order to protect the privacy of users in their system. Furthermore, in Xu et al. (2019), a blockchain smart contact was used to implement a reward-penalty module for a trustless crowd-intelligence ecosystem. Their implementation made use of edge servers to host and run the smart contract that stored performance history data of workers, the rules for managing the platform, and the standards for collaboration between stakeholders. Hu et al. (2020) also researched the use of blockchain as a reward mechanism for mobile crowdsensing. Their reason for proposing a blockchain-based incentive mechanism was to address privacy and security issues in mobile crowdsensing. They also highlighted the anonymity feature of blockchain technology to protect the privacy of participants and the use of smart contracts to automate the sensing process as benefits of blockchain in crowdsensing. These reviewed papers therefore show the viability of a blockchain-based incentive mechanism to protect the privacy of participants. Hence, the reason for the proposed blockchain-based incentive mechanism for rewarding and verifying participants in task offloading to volunteered mobile devices in this paper.

2.3 Blockchain-based Identity Management

The aim of this project is to develop a blockchain-based incentive mechanism that rewards and verifies participants in task offloading to volunteered mobile devices without compromising their privacy. To achieve this, a review of existing literature regarding the use of blockchain for identity management was conducted. This section discusses the approaches taken in some of the reviewed literature.

The benefit of using the blockchain technology for identity management is that it enables an identity to be created and managed for an entity without using third-parties. This identity is tied to an incentive scheme, usually a smart contract token to ensure that the entity does not behave maliciously on the system due to anonymity. In Zyskind et al. (2015), the authors explored using blockchain to protect personal data thereby decentralising privacy. They used the blockchain to generate a pseudo-identity for the users and stored it on the blockchain with their associated permissions on the system. They also used offsite storing of pointers to encrypted data on the blockchain to maintain the system and enable verification. Furthermore, Ren et al. (2021) used blockchain to enable batch verification of vehicles in vehicular networks without compromising their privacy. Their developed scheme, enabled the vehicles to create pseudo-identities for

themselves and used a two Merkle Tree structures to store and revoke the pseudo-identities of the vehicles. It also enabled traceability of identities in order to identify vehicles that performed maliciously on the system and revoke their access. A similar work was also done by Malik et al. (2018), using blockchain to perform the authentication of vehicle identity on vehicular networks and revoking access of vehicles that perform maliciously. Lastly, Gutiérrez-Agüero et al. (2021) and Zhao & Liu (2019) both used Ethereum technology for identity management. Gutiérrez-Agüero et al. (2021) looked at creating burnable pseudo-identities that allowed users to unlink their pseudo-identities. While Zhao & Liu (2019) developed a blockchain identity management that considered reputation. Therefore based on the reviewed literature, blockchain-based identity management provides a way to enable anonymity while also providing a means to identify entities that act maliciously. Furthermore, when implemented with an incentive mechanism, it can be used to reward and penalise these entities without compromising their privacy.

2.4 Research Niche

The aim of this paper is to develop a blockchain-based incentive mechanism for rewarding and verifying the participants in task offloading to volunteered mobile devices without compromising their privacy. The reviewed literature highlight the need for an incentive mechanism to encourage the owners of mobile devices to volunteer their device. They also show that there are concerns regarding the privacy of participants in the task offloading process. However, they fall short of providing a verification mechanism that verifies the identity of volunteers without compromising their privacy.

Based on the work done so far in using blockchain technology for identity management in order to protect privacy via pseudo-identities and as an incentive mechanism, this paper explores applying blockchain technology to provide an incentive and identity management for task offloading to volunteered mobile devices in a hybrid cloud solution.

3 Research Methodology

The aim of this project is to design a blockchain-based incentive mechanism for offloading tasks to volunteered mobile devices and verifying the participants without compromising their privacy. In this section, the methodology used to achieve this aim is explained.

3.1 Review existing literature

To achieve the aim of this paper, a review of existing literature on the state of the art in offloading tasks to volunteer mobile devices, providing an incentive for volunteer mobile devices and blockchain-based identity management was conducted.

3.2 Develop a prototype

Based on the reviewed literature, the following components were identified as requirements for the mechanism developed in this paper.

3.2.1 Cloud controller

As suggested in Alonso-Monsalve et al. (2018), this is a hybrid cloud system that provides the storage resource for offloaded tasks, while the volunteered devices provided the processing resource for the offloaded task. The hybrid cloud system is positioned between the blockchain-based incentive mechanism and the mobile application running on the volunteered device.

3.2.2 Mobile application

This is the application that runs on the volunteered device. The volunteers register on the system using this application. The application also collects information on the device registered in terms of the manufacturer, ram and device name. These information are sent to the cloud server that stores them. Based on some of the use cases highlighted by Alonso-Monsalve et al. (2018) and Zhou et al. (2017), for the processing service, the application executes Optical Character Recognition (OCR) tasks and face detection tasks on the device.

3.2.3 Blockchain-based incentive mechanism

This is responsible for generating a pseudo-identity for the volunteers and rewarding them with a blockchain token. The incentive mechanism is quite similar to the approach taken by Anderson (2019) where credits are used as an incentive for the volunteers to show how much work they have done thereby serving as an indication of reputation. However, it differs from their approach because the incentive used in this paper leverages blockchain technology to manage the identity of volunteers and reward them.

3.3 Evaluate prototype

To evaluate the developed prototype a test is done using the developed prototype to offload face detection and OCR tasks to registered volunteered android devices. The execution time and memory usage of the blockchain-based mechanism is then measured to determine the overhead it adds to the task offloading process. Furthermore, the reputation of the volunteered device is checked to confirm that the incentive mechanism behaves as expected.

4 Design Specification

This section discusses the design specification of the system. It contains the overall architecture of the system, the various modules in the individual components of the system and their functionalities.

4.1 System Architecture

The system is made up of a cloud controller, a mobile application running on volunteered devices and a blockchain-based incentive mechanism. The cloud controller sits in-between the the mobile application and the incentive mechanism running on the blockchain network. This architecture is shown in Figure 1. The offloading flow of the system involves client devices running the mobile application offloading their tasks to volunteered mobile

devices via the cloud controller. The selected volunteered devices then perform the tasks and send the results to the client devices via the cloud controller. This flow concludes with the cloud controller verifying and rewarding the volunteers by communicating with the incentive mechanism running on the blockchain network to transfer a fixed amount of token to the volunteers. The details of the architecture of the individual components that make up the system are discussed in the subsections below.

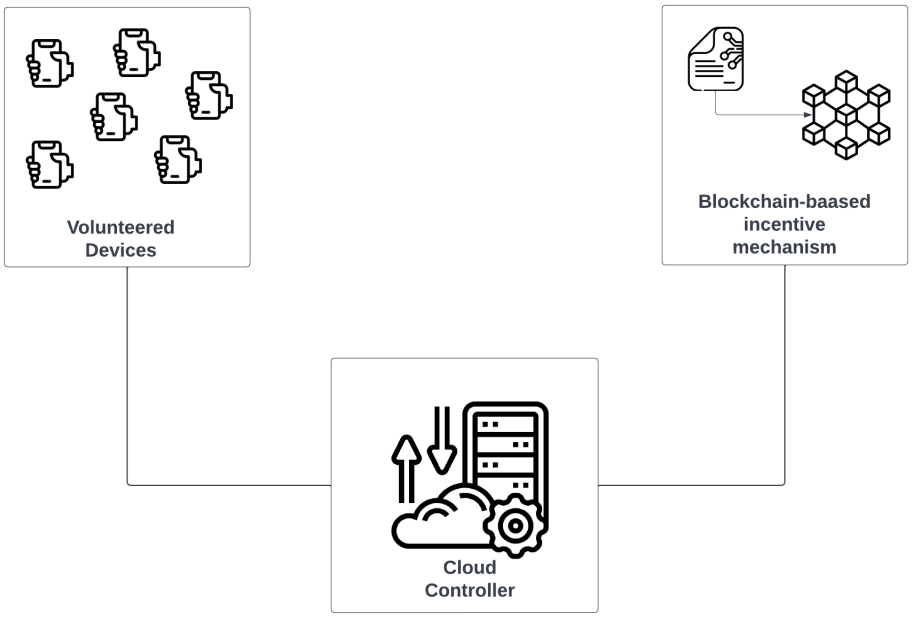

Figure 1: System Architecture

4.1.1 Cloud controller design

Figure 2 shows the cloud controller design. The cloud controller is a hybrid cloud system that has a volunteer module, task offloading module and reward module. The volunteer module handles the registration of volunteers on the platform by firstly, communicating with the mobile application running on the volunteered device to collect the volunteer's email, password and device information. Then communicating with the blockchain-based incentive mechanism to generate a pseudo-identity for the volunteered devices and storing the generated address alongside the information gotten from the task execution application on the system.

The task offloading module handles the offloading process and storage. The process involves the hybrid cloud system receiving the offloaded task from the client and offloading it to the selected volunteered mobile device. It then stores the result of the offloaded task received from the volunteered mobile device on a cloud server and delivers the result to the client device. When the result has been returned, it notifies the reward module.

The reward module communicates with the blockchain-based incentive mechanism to reward the volunteer with a token, storing the transaction hash with the result for the verification of the participants. It also updates the token balance of the volunteer on the system which serves as the reputation of the volunteer on the system. The updated token balance is gotten from the blockchain-based incentive mechanism.

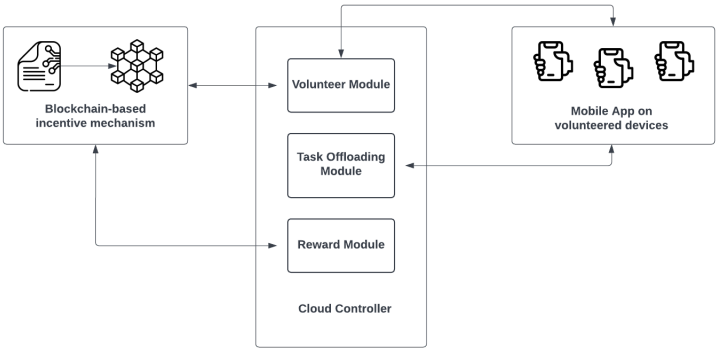

Figure 2: Cloud controller design

4.1.2 Mobile application design

This is the mobile application that runs on the volunteered devices. It is made up of four modules: the authentication module, the device profiler module, task offload module and task execution module. The authentication module and device profile module enable volunteers to register their devices. They both communicate with the cloud controller's volunteer module to achieve this. The task offload module also communicates with the cloud controller's volunteer module. However, it does this to provide the client with the volunteers so that it can offload the task provided by the client to the selected volunteered device. The task execution module enables the volunteered device to execute the task offloaded to it. It actively listens for tasks assigned to the volunteered device from the cloud controller's task offloading module. An illustration of the mobile application design is shown in Figure 3.

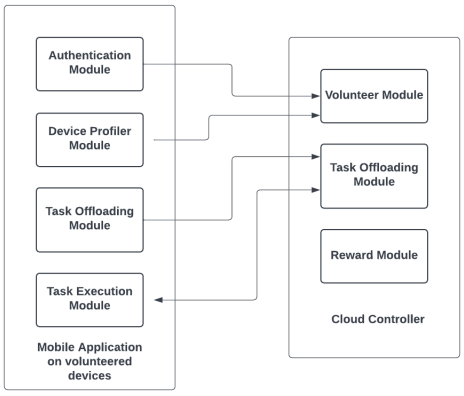

Figure 3: Mobile application design

4.1.3 Blockchain-based incentive mechanism design

This is made up of an identity management module, a reward module and a reputation module. The identity management module creates a pseudo-identity for a volunteer and provides the cloud controller's volunteer module with this identification to store. The reward module communicates with the cloud controller's reward module to get the volunteers to reward. And the reputation module provides the cloud controller's reward module with the reputation of the volunteers. This system design is shown in Figure 4.

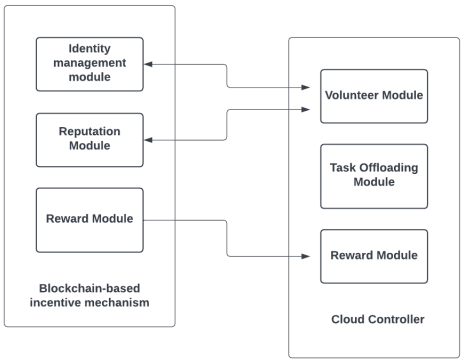

Figure 4: Blockchain-based incentive mechanism design

5 Implementation

This section discusses the implementation of the proposed mechanism in this paper. The aim of this paper is to develop a blockchain-based incentive mechanism for offloading tasks to volunteered mobile devices and verifying the participants without compromising their privacy. The system requires that volunteers register on the platform. The stages involved in this process are shown in Figure 5. In the first step, the volunteer sends their device specification and authentication details to the cloud controller. This is done using the mobile application component of this system. In the second step, the cloud controller instructs the blockchain-based incentive mechanism to generate a pseudo-identity for the volunteer which is a blockchain address. This is the address that will be used to identify and reward the volunteer by the blockchain-based incentive mechanism. In the last step, which is step 3, the blockchain-based incentive mechanism returns the generated pseudo-identity to the cloud controller which stores it with the other information of the registered volunteer.

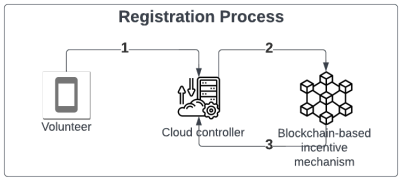

Figure 5: Volunteer registration process

Figure 6 shows the task offloading and reward process. In the first step, **Volunteer A** selects **Volunteer B** as the volunteer they want to offload their task to and sends this information and the task to the cloud controller through the mobile component of the system. In the second step, the cloud controller pushes the task to **Volunteer B** who is subscribed to the cloud controller to receive assigned tasks. **Volunteer B** then executes the offloaded task and returns the result to the cloud controller in step 3. In step 4, the cloud controller verifies the result and provides the blockchain-based incentive mechanism with the pseudo-identity for **Volunteer B** to reward them for executing the offloaded task. The blockchain-based incentive mechanism then performs this transaction and returns the updated reputation for **Volunteer B** to the cloud controller in step 5. In step 6, the result of the offloaded task is transferred by the cloud controller to **Volunteer**

A along with the transaction hash so that **Volunteer A** can confirm the source of the result if they want to.

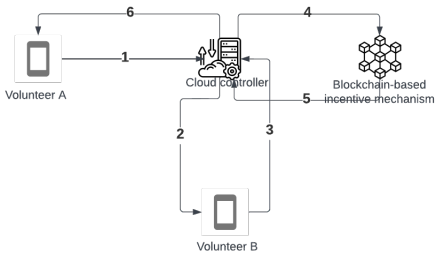

Figure 6: Task offloading and reward process

The implementation of the various components are discussed in more details below.

5.1 Cloud controller

The cloud controller is implemented with Firebase provided by Google Cloud Platform. It uses Firebase firestore as the storage resource for the system to store the volunteer's device information and blockchain address for the volunteer module. It also stores the results of the executed offloaded tasks for the task offloading module. The task offloading module in the cloud controller communicates with the volunteered devices using a Message Queuing Telemetry Transport (MQTT) implementation. A volunteered device subscribes to receive its assigned tasks while the offload module publishes the offloaded task to the subscribed volunteer selected by the client.

Furthermore, the volunteer module communicates with the blockchain based incentive mechanism to create a blockchain address for the volunteered device using a cloud function. This cloud function is triggered by the the registration action of the authentication module in the mobile application running on the volunteered device. Likewise, the reward module communicates with the blockchain-based incentive mechanism to reward a volunteer using a cloud function. This is triggered by the result event from the task execution module in the mobile application running on the volunteered devices. The result is then stored along with the transaction hash gotten from the blockchain-based incentive mechanism for verification.

Lastly, the cloud controller communicates with the reputation module in the blockchain-based incentive mechanism using cloud functions to get the reputation of the volunteer. This is the volunteer's token balance of the ERC20 smart contract token created for this paper called Code Offloading Reputation token (COR). This is triggered by a verification action from the cloud controller.

5.2 Mobile application

The mobile application is an android application built using Kotlin and Android Studio IDE. It makes use of the Firebase Android Software Development Kit (SDK) to implement the functions to communicate with the cloud controller. The authentication module collects the email and password of the volunteer. This is solely for authentication purpose so that the volunteers do not loose their account in the case of a forgotten password and to protect the account from unauthorised access. This information is never shared with

other users on the platform. Furthermore, the device profiler module collects the RAM size, phone manufacturer and the name of the device being volunteered and sends it to the cloud controller using the Firebase firestore SDK.

The task offloading module displays the volunteered devices with their device specification, blockchain address and reputation as gotten from the cloud controller's volunteer module. To offload the task, it communicates with the cloud controller's task offloading mechanism providing the selected volunteer and the task offloaded. Based on the use cases selected for the developed mechanism in this paper, the task offload module allows the client to upload an image from the file system of the android device for an OCR or Face detection task to be performed on the image.

The task execution module subscribes to the task offload module in the cloud controller to monitor when a task is offloaded to the device in real-time. It makes use of the Firebase Machine Learning Kit (ML Kit) to perform the OCR and Face detection use case tasks on the volunteered device. The results of the executed tasks are then sent to the cloud controller using the Firebase firestore SDK.

5.3 Blockchain-based incentive mechanism

The blockchain-based incentive mechanism is made up of the identity management module, the reputation module and the reward module. The identity management module makes use of the ether.js library to create a wallet for a volunteer registering on the system. It then provides the the cloud controller with the generated blockchain address for the volunteer. The cloud controller stores this information and uses it as the identification for the volunteer in performing offloaded tasks assigned to them.

The incentive mechanism is powered by the reward module which is an ERC20 smart contract token called Code Offloading Reputation token (COR) running on the Ethereum blockchain. The smart contract was written with Solidity on Remix IDE and deployed to the Ropsten Testnet. It is a fixed supply token that rewards the volunteer with 5 COR tokens for executing tasks offloaded to them. Furthermore, the token amount for reward is fixed and is not affected by the device specification or the task performed. It only considers that the task was done by the volunteer. When a volunteer performs a task and returns the result, the smart contract is executed on the Ethereum blockchain to transfer 5 COR tokens to the blockchain address of the volunteer, the transaction hash is then attached to the result of task as a verification key.

The reputation module gets the amount of COR tokens a volunteer has using their blockchain address. The token amount a volunteer has serves as the reputation of the volunteer on the system. It is called each time a volunteer executes an offloaded task and returns the result to update the cloud controller's volunteer module.

6 Evaluation

The objective set for this paper is to design a blockchain-based incentive mechanism for task offloading to volunteered mobile devices and verifying participants without compromising their privacy. This is achieved by implementing a prototype that consists of a cloud controller, a mobile application and a blockchain-based incentive mechanism. To evaluate this developed prototype, an offload of OCR and Face detection tasks are performed. The evaluation checks that;

- The privacy of the volunteer is protected while being verified.
- The OCR and Face detection tasks can be offloaded to the volunteered devices.
- The offloaded OCR and Face detection tasks can be executed by the volunteered device.
- The volunteers are rewarded for executing tasks and verified.
- The overhead from the incentive mechanism is measured.

6.1 Verification & Privacy

An evaluation of the developed blockchain-based mechanism's ability to verify the participants in task offloading without compromising their privacy was performed. To perform this test, two volunteers are registered on the created mobile application for task offloading. They will be referred to as **Volunteer A** and **Volunteer B** in this report. **Volunteer A** is registered with an emulation of a Google Pixel 3a that has 1.29 GB RAM running on Android Studio. While **Volunteer B** is registered with a Google Pixel 3 XL that has 3.5 GB and is a physical device. Figure 7 and Figure 8 show how the volunteers are represented on the system highlighting the blockchain address being used as the identifier for the volunteers. While Figure 9 shows the result of an executed offloaded task and Figure 10 shows the verification of the reward associated with the executed task on Etherscan.

The evaluation performed showed that the blockchain-based incentive mechanism was able to verify the participants without compromising their identity by using the pseudo-identity created for the volunteers. With the transactions being recorded on the blockchain and the transaction hash being provided in the result, clients can verify that the source of the result they received is the volunteer they selected based on the blockchain address associated with the transaction. Furthermore, the pseudo-identity protects the privacy of the volunteers because it does not require a Know-Your-Customer(KYC) process or a Proof of Identity (POI). It also does not require third-party agencies or government-based agencies to verify the participants. Thereby providing a level of anonymity for the users. However, it still provides a way to trace the activities of the volunteers on the system as their actions are tied to the pseudo-identity created for them. This pseudo-identity is also used to associate the reward and reputation on the system to the volunteers.

Furthermore, the device information obtained in order to perform task offloading can be exploited by malicious actors if they are able to attach the private details (KYC and POI) to to the owner. However, with the blockchain-based incentive mechanism developed in this paper, the privacy of the participants are retained while ensuring they can still be identified and rewarded using their pseudo-identity.

6.2 Task Offloading

To evaluate the task offloading of the designed prototype, a simulation was performed to offload images for OCR and face detection tasks. The result from the evaluation of these tasks are discussed in the following subsections.

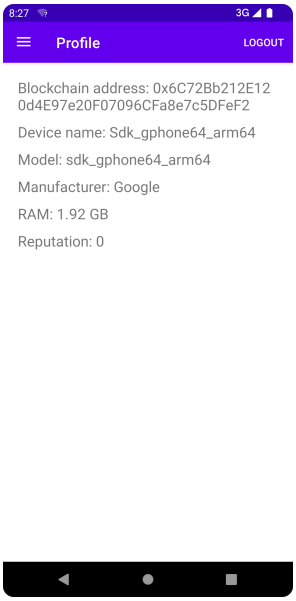

Figure 7: **Volunteer A**'s profile on the system

6.2.1 OCR Task

To evaluate the offloading and execution of OCR tasks, an image containing texts was offloaded from **Volunteer A** to **Volunteer B**. The simulation performed showed that the mobile application performed the OCR task accurately and returned the recognised text in the result being shared with the client device (**Volunteer A**) . However, this came at the cost of the image size being compressed by the cloud storage. This reduction in size however did not affect the generated result for the OCR task as it remained accurate.

6.2.2 Face Detection Task

To evaluate the offloading and execution of OCR tasks, an image of a person smiling was offloaded from **Volunteer A** to **Volunteer B**. The mobile application was able to perform the face detection task. It analysed the face detected in the image for the probability of the person smiling, their right eye closed and their left eye closed. The probability score for these various classifications were then provided in the result sent to the client device (**Volunteer A**).

6.3 Blockchain-based Incentive Mechanism

The different modules in the blockchain-based incentive mechanism are evaluated in terms of time taken and memory used to determine the overhead added by its integration in the offload process. To evaluate this, fourteen (14) volunteers were registered and offloading of tasks were performed to get the average execution time and memory used by each module in the blockchain-based incentive mechanism. The cloud functions that are executed by each module's functionality are evaluated using Firebase's monitoring tool.

6.3.1 Identity Management Module

The identity management module had the lowest execution time and used the least memory when compared to other modules. This could be to it being called fewer times

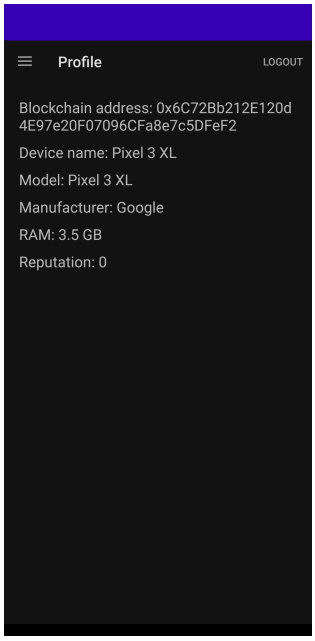

Figure 8: **Volunteer B**'s profile on the system

than the other modules as it only handles generation of pseudo-identity for a volunteer. In the test, it was invoked fourteen times to create pseudo-identities for the volunteers when they registered. Table 1 shows the evaluation result. The mean execution time is the average time it took to execute the module's operation and the mean memory is the average memory that was used by the module. The mean execution time is measured in seconds and the mean memory is measured in megabytes.

Execution count	Mean execution time(s)	Mean Memory used(mb)
14	0.01	73.14

Table 1: Identity module evaluation result

6.3.2 Reputation Module

The reputation module had the second lowest execution time. It is the module executed the most in the blockchain-based incentive mechanism. It was executed 280 times during the test. This module is executed to get the reputation of volunteers when they perform task offloading and when volunteers are trying to offload tasks. Table 2 shows the evaluation result.

Execution count	Mean execution time(s)	Mean Memory used(mb)
280	0.05	86.05

Table 2: Reputation module evaluation result

6.3.3 Reward Module

The reward module is the module that contributes the most to the task offloading time. It had the highest execution time when compared to other modules. It is called to reward

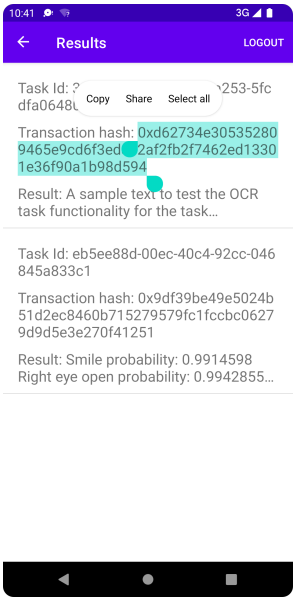

Figure 9: Result view in mobile application showing transaction on blockchain

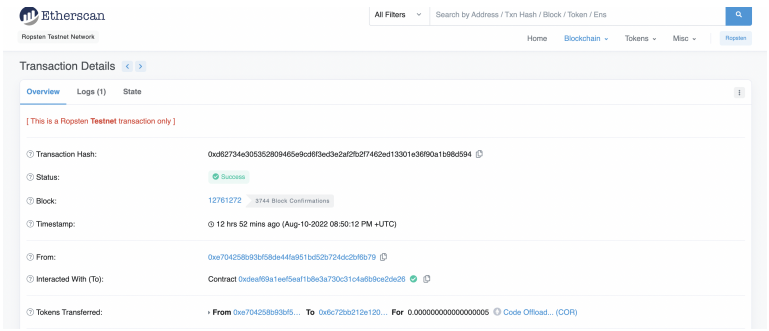

Figure 10: Verification of transaction on blockchain

the volunteer and verify the result and it was executed 35 times during the test. Table 3 shows the evaluation result for this module.

Execution count	Mean execution time(s)	Mean Memory used(mb)
35	9.63	82.28

Table 3: Reward module evaluation result

6.4 Discussion

The evaluation performed showed that the developed system works as expected and that it fulfills the objective of offloading OCR and Face detection tasks to volunteered mobile devices and rewards the volunteers for executing the tasks. It also shows that the privacy of the volunteers are protected by using pseudo-identities generated for them.

The execution time of the various modules and memory usage were also recorded to measure the overhead added by the blockchain-based incentive mechanism. The primary modules involved in the task offloading process are the reputation and reward modules. The evaluation shows that reward module has an average execution time of 0.05 seconds and the reward module has an average time of 9.63 seconds. This means together they

add 9.68 seconds to the execution time of the task offloading process. The execution time for the identity management module is not included in this calculation becomes it only executes once for each volunteer while the other modules are executed every time the task offload process is performed.

7 Conclusion and Future Work

This research paper investigated if a blockchain-based incentive mechanism can be applied in task offloading to volunteered devices in order to enable the rewarding and verification of participants without compromising their privacy. The designed mechanism comprised of an identity management module, reputation module and reward module. Furthermore, the simulation and evaluation performed showed that the developed blockchain mechanism enabled the reward and verification of participants without sharing personal data. It was able to achieve this without adding any significant overhead in terms of execution time to the task offloading process. The developed mechanism therefore shows that concerns regarding privacy and the absence of verification of participants in task offloading to volunteer mobile devices can be addressed with blockchain technology. Thereby improving trust With the verification participants.

A limitation in the developed system is that it did not implement a penalty module that penalised volunteers that performed malicious actions on the system. However, the developed system has the infrastructure that enable this module with the identities of the volunteers being attached to the incentive on the system. This can be implemented in a future work. Another limitation is that with the hybrid cloud system adopted for the task offloading and cloud controller system, it suffers from the latency issue highlighted as a problem with the restrictions of network bandwidth and network congestion. However, this is a trade-off decision to enable the availability of more volunteer devices in order to avoid limiting available devices to only those in a volunteer's location. Furthermore, to enable further anonymity on the system, an anonymous sign-in mechanism that relies solely on the pseudo-identity generated for the volunteers can be implemented.

Finally, with the developed mechanism, application developers can implement a hybrid system that offloads computation tasks to volunteered devices and rewards them with an incentive. Thereby reducing the amount spent on paying cloud service providers to perform these tasks on servers.

8 Resources

The video presentation and code artefact for this project are;

- Video presentation `https://youtu.be/AIRZtBWG9gU`.
- Artefact: `https://drive.google.com/file/d/1SfIlYlEjY2zDjJWAwlFeS_qhTuqFQd4Q/view?usp=sharing`.

References

Alonso-Monsalve, S., García-Carballeira, F. & Calderón, A. (2018), 'A heterogeneous mobile cloud computing model for hybrid clouds', *Future Generation Computer Systems*

87, 651–666. JCR Impact Factor 2021: 7.187.
URL: *https://www.sciencedirect.com/science/article/pii/S0167739X17313894*

Anderson, D. P. (2019), 'Boinc: A platform for volunteer computing'.
URL: *https://arxiv.org/abs/1903.01699*

Buyya, R., Srirama, S. N., Casale, G., Calheiros, R., Simmhan, Y., Varghese, B., Gelenbe, E., Javadi, B., Vaquero, L. M., Netto, M. A. S., Toosi, A. N., Rodriguez, M. A., Llorente, I. M., Vimercati, S. D. C. D., Samarati, P., Milojicic, D., Varela, C., Bahsoon, R., Assuncao, M. D. D., Rana, O., Zhou, W., Jin, H., Gentzsch, W., Zomaya, A. Y. & Shen, H. (2018), 'A manifesto for future generation cloud computing: Research directions for the next decade', *ACM Computing Surveys* **51**(5). JCR Impact Factor 2021: 10.282.
URL: *https://doi.org/10.1145/3241737*

Gutiérrez-Agüero, I., Anguita, S., Larrucea, X., Gomez-Goiri, A. & Urquizu, B. (2021), 'Burnable pseudo-identity: A non-binding anonymous identity method for ethereum', *IEEE Access* **9**, 108912–108923. JCR Impact Factor 2021: 3.476.

Hu, J., Yang, K., Wang, K. & Zhang, K. (2020), 'A blockchain-based reward mechanism for mobile crowdsensing', *IEEE Transactions on Computational Social Systems* **7**(1), 178–191. JCR Impact Factor 2021: Not Available.

Khaledi, M., Khaledi, M. & Kasera, S. K. (2016), Profitable task allocation in mobile cloud computing, *in* 'Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks', Q2SWinet '16, Association for Computing Machinery, Malta, Malta, p. 9–17. CORE2021 Rank=A.
URL: *https://doi.org/10.1145/2988272.2988281*

Liu, Z., Zeng, X., Huang, W., Lin, J., Chen, X. & Guo, W. (2016), Framework for context-aware computation offloading in mobile cloud computing, *in* '2016 15th International Symposium on Parallel and Distributed Computing (ISPDC)', Fuzhou, China, pp. 172–177. CORE2021 Rank=A.

Lu, F., Gu, L., Yang, L. T., Shao, L. & Jin, H. (2020), 'Mildip: An energy efficient code offloading framework in mobile cloudlets', *Information Sciences* **513**, 84–97. JCR Impact Factor 2021: 6.795.
URL: *https://www.sciencedirect.com/science/article/pii/S0020025519309636*

Malik, N., Nanda, P., Arora, A., He, X. & Puthal, D. (2018), Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks, *in* '2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)', New York, NY, USA, pp. 674–679. CORE2021 Rank= B.

Nakamoto, S. (2008), 'Bitcoin: A peer-to-peer electronic cash system', *Decentralized Business Review* p. 21260. JCR Impact Factor 2021: Not Available.

Ren, Y., Li, X., Sun, S.-F., Yuan, X. & Zhang, X. (2021), 'Privacy-preserving batch verification signature scheme based on blockchain for vehicular ad-hoc networks', *Journal*

of Information Security and Applications **58**, 102698. JCR Impact Factor 2021: 4.96.
URL: *https://www.sciencedirect.com/science/article/pii/S2214212620308450*

Shi, Y., Chen, S. & Xu, X. (2018), 'Maga: A mobility-aware computation offloading decision for distributed mobile cloud computing', *IEEE Internet of Things Journal* **5**(1), 164–174. JCR Impact Factor 2021: 9.471.

Sulaiman, D. & Barker, A. (2019), Mamoc-android: Multisite adaptive computation offloading for android applications, *in* '2019 7th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)', Newark, CA, USA, pp. 68–75.

Wang, J., Li, M., He, Y., Li, H., Xiao, K. & Wang, C. (2018), 'A blockchain based privacy-preserving incentive mechanism in crowdsensing applications', *IEEE Access* **6**, 17545–17556. JCR Impact Factor 2021: 3.476.

Wang, X., Chen, X. & Wu, W. (2017), Towards truthful auction mechanisms for task assignment in mobile device clouds, *in* 'IEEE INFOCOM 2017 - IEEE Conference on Computer Communications', Atlanta, GA, USA, pp. 1–9.

Wang, X., Sui, Y., Wang, J., Yuen, C. & Wu, W. (2021), 'A distributed truthful auction mechanism for task allocation in mobile cloud computing', *IEEE Transactions on Services Computing* **14**(3), 628–638. JCR Impact Factor 2021: 8.216.

Xu, J., Wang, S., Bhargava, B. K. & Yang, F. (2019), 'A blockchain-enabled trustless crowd-intelligence ecosystem on mobile edge computing', *IEEE Transactions on Industrial Informatics* **15**(6), 3538–3547. JCR Impact Factor 2021: 10.215.

Zhao, Z. & Liu, Y. (2019), A blockchain based identity management system considering reputation, *in* '2019 2nd International Conference on Information Systems and Computer Aided Education (ICISCAE)', Dalian, China, pp. 32–36.

Zhou, B., Dastjerdi, A. V., Calheiros, R. N., Srirama, S. N. & Buyya, R. (2017), 'mcloud: A context-aware offloading framework for heterogeneous mobile cloud', *IEEE Transactions on Services Computing* **10**(5), 797–810. JCR Impact Factor 2021: 8.216.

Zhou, B., Srirama, S. N. & Buyya, R. (2019), 'An auction-based incentive mechanism for heterogeneous mobile clouds', *Journal of Systems and Software* **152**, 151–164. JCR Impact Factor 2021: 2.829.
URL: *https://www.sciencedirect.com/science/article/pii/S0164121219300548*

Zyskind, G., Nathan, O. & Pentland, A. S. (2015), Decentralizing privacy: Using blockchain to protect personal data, *in* '2015 IEEE Security and Privacy Workshops', San Jose, CA, USA, pp. 180–184. CORE2021 Rank= A*.