AN INCENTIVE PAYMENT MODEL TO FUTURE COMMUNICATION NETWORKS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

FATIH KIHTIR

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
COMPUTER ENGINEERING

SEPTEMBER 2018

Approval of the thesis:

AN INCENTIVE PAYMENT MODEL TO FUTURE COMMUNICATION NETWORKS

Submitted by **FATIH KIHTIR** in partial fulfillment of the requirements for the degree of **Master of Science in Computer Engineering Department, Middle East Technical University** by,

Prof. Dr. Halil Kalıpçılar
Dean, Graduate School of **Natural and Applied Sciences** ____________________

Prof. Dr. Halit Oğuztüzün
Head of Department, **Computer Engineering** ____________________

Prof. Dr. Ferda Nur Alpaslan
Supervisor, **Computer Engineering Dept., METU** ____________________

Dr. Kasım Öztoprak
Co-Supervisor, **Computer Eng. Dept., KTO Karatay University** ____________________

Examining Committee Members:

Prof. Dr. Mehmet Reşit Tolun
Computer Engineering Dept., Başkent University ____________________

Prof. Dr. Pınar Karagöz
Computer Engineering Dept., METU ____________________

Prof. Dr. Ferda Nur Alpaslan
Computer Engineering Dept., METU ____________________

Date: ____________________

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name : Fatih, Kıhtır

Signature :

ABSTRACT

AN INCENTIVE PAYMENT MODEL TO FUTURE COMMUNICATION NETWORKS

Kıhtır, Fatih
MSc., Department of Computer Engineering
Supervisor : Prof. Dr. Ferda Nur Alpaslan
Co-Supervisor: Dr. Kasım Öztoprak

September 2018, 55 pages

The developments in telecommunication world have allowed customers share the storage and processing capabilities of their devices by providing services through fast and reliable connections. This evolution, however, requires building an incentive system to encourage the information exchange in the future telecommunication networks. In this thesis, we propose a mechanism to share bandwidth and processing resources among subscribers by using smart contracts and a blockchain based incentive mechanism, which is used to encourage the subscribers to share their resources. We demonstrate the applicability of the proposed method through three use cases; i) pub/sub systems, ii) exchanging multimedia data, and iii) cpu sharing. We propose a universal payment system named TelCash between the users and between the users and operators, which puts forward a solution for current roaming problem and establishes trust in x2x communications. TelCash has a great potential in solving the charges of roaming problem in telecommunication sector.

Keywords: Blockchain, Device-to-Device Communication, Video Streaming, Reputation Management, Data exchange

ÖZ

GELECEĞİN HABERLEŞME DÜNYASI İÇİN BİR ÖDEME SİSTEMİ MODEL ÖNERİSİ

Kıhtır, Fatih
Yüksek Lisans Bilgisayar Mühendisliği
Tez Yöneticisi : Prof. Dr. Ferda Nur Alpaslan
Ortak Tez Yôneticisi: Dr. Kasım Öztoprak

Eylül 2018, 55 sayfa

Telekomünikasyon dünyasındaki gelişmeler, müşterilerin hızlı ve güvenilir bağlantı hizmeti sunarak, cihazlarının depolama ve işleme yeteneklerini paylaşmalarına olanak sağlamıştır. Ancak bu evrim, gelecekteki telekomünikasyon ağlarındaki bilgi alışverişini teşvik etmek için bir teşvik sistemi oluşturulmasını gerektirmektedir. Bu tez çalışmasında, abonelerin kaynaklarını paylaşmaya teşvik etmek için kullanılan akıllı sözleşmeler ve blok zincirine dayalı bir teşvik mekanizması kullanılarak aboneler arasında bant genişliği ve işlem kaynakları paylaşılması için bir mekanizma öneriyoruz. Önerilen yöntemin üç kullanım durumu aracılığıyla uygulanabilirliğini gösteriyoruz; i) pub/sub sistemler, ii) multimedya verileri değişimi ve iii) cpu paylaşımı. Kullanıcılar arasında, ve kullanıcılar ve operatörler arasında TelCash adında bir evrensel ödeme sistemi öneriyoruz. Bu, mevcut dolaşım sorununa bir çözüm getiriyor ve x2x iletişiminde güven oluşturuyor. Önerilen yöntem telekomünikasyon sektöründeki roaming sorununu çözme konusunda büyük bir potansiyele sahiptir.

Anahtar Kelimeler: Blockchain, Cihazlar Arası Haberleşme, Video Yayını, Güvenilirlik Yönetimi, Veri Paylaşımı

To My Family

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to my supervisor Prof. Dr. Ferda Nur Alpaslan and co-supervisor Dr. Kasım Öztoprak for their guidance, advice, criticism, encouragements and insight throughout the research.

I would also like to thank Prof. Dr. Mehmet Reşit Tolun for his suggestions and comments.

The technical assistance of Ms. Sultan Arslan was unbelievable and I do not want to miss her kind support during my studentship.

Nobody has been more important to me in the pursuit of this thesis than my awesome wife, Serpil. Thank you so much, my love. I wish to thank my three wonderful children, Kaan, Melisa and Aylin, who provide unending inspiration.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Recent decade has witnessed a huge and sharp increase in the transmission of multimedia data. Although this development was a direct consequence of developments in communication technologies, the increase in the need for larger bandwidth, higher data rates and larger processing power have surpassed the improvements in the underlying technologies. The rapid increase in the need for higher data rates and better processing power have lead researchers to consider the unused resources at the edge of the networks (internet) to improve the performance of end user devices. Through utilizing the idle processing power of the devices in its proximity, a device can accelerate the execution of its tasks. Internet Service Providers can utilize the device-to-device (D2D) data transmission to reduce the data traffic load on its servers and access points [36]. Device-to-device data delivery can be used to deliver data from an access point to a single device and relay it to other requesting devices in the same network. Making use of these idle resources however, comes with its difficulties [19]. Utilizing the unused bandwidth and idle processing power of other devices pose challenges in terms of coordination and housekeeping, privacy, and willingness of the nodes to share their resources. This research proposes a device-to-device data delivery model when encompasses a crypto-money based payment system to provide incentives for sharing the unused bandwidth between devices.

1.1 Application Model

The network environment will consist of an access point (or a base station) which will take over the responsibility of the coordinator, and a group of nodes, which can communicate with it. Each node can be in either one (or both) of the two categories of Providers, and Requesters dynamically. The node can decide to avoid sharing its resources and hence in none of the above categories.

A provider is sharing some public data through a D2D connection with requesting nodes within its direct link reachability range. We assume the providers may relocate to a new place. However, the supervising nodes (base stations/access points) keep track of the instantaneous locations of providers and requesters.

A requester can request data in one of the two possible ways:

1. Requester sends a request to the super node providing the identifying information of the requested data/data segment.
2. A requester may subscribe to one or some data topics. In this case, all data items from its subscribed topics are sent to this requester as they are received from a provider.

Providers provide data to requesters through direct communication channels. The data transmission starts after the super node establishes the communication. The super node after receiving a request for a specific data item identifies the providers of the data in its network. If no provider is found (or the provider(s) are busy), supervisor node tries to provide data through its own resources. If more than one provider are found, the super node makes a fair selection and instructs the provider to send the data to the requester.

The requester acknowledges the reception of data by sending a message to the super node. The super node writes a transaction record to the transaction pool.

1.2 Publishing Topics on Dynamic Networks

Topic based pub/sub networks have been designed and developed for optimizing message delivery to the interested subscribers. The message delivery optimization in these networks is based on using overlay networks. Overlay networks are virtual networks, which are used for modeling message broadcasting from publishers to subscribers of a topic. These networks try to minimize the number of transmitted data, minimize the maximum distance between the nodes in an overlay network (called overlay diameter), and minimize the number of connections from a node in an overlay to other interested nodes (node degree). In order to optimize the overlay networks, special node named brokers are added to the network. These nodes are neither subscribers nor publishers and are responsible to relay the messages. The overlay network design parameters such as overlay network diameter, maximum node degree, etc. are used by overlay design algorithms. However, these parameters do not include the physical distance in overlay computation. This means that the nodes interested in a topic are assumed to be connected and can exchange packets through the Internet. In D2D data exchange applications however, the reachability assumption between nodes may not be valid. This situation requires specialized overlay design algorithms for publishing on D2D networks. The proposed method can be considered as a dynamic overlay network where the super node instructs the nodes to behave as a broker whenever the connectivity requirements are met.

1.3 Streaming Data

Data streaming, specifically bulky multimedia such as high definition videos requires vast bandwidth. Device-to-device data transmission facilitates implementing this type of applications. The requesting device sends its request to the access point, which maintains a list of current users of the stream. If a device downloading the stream is interested in providing it to the devices in its signal range, the access point informs both devices to establish the connection.

1.4 Edge Computing

An important hinder in using the Internet of Things (IoT) in time-restricted applications, or applications running on networks with limited bandwidth connections is the latency of sending data to cloud servers and process them there. In fact some applications may include data from thousands of sensors which report the current status of the systems under control and their transmission to the cloud is not necessary. As a solution to this problem, processing at local servers has been proposed. Later on, this solution evolved to entail utilization of micro-processing power available at end-user devices in a distributed form. This solution encourages the end-users to share the processing power of their devices in a local network, where the initial processing of data can be carried out, and the need to forward the data to cloud will be eliminated largely. The solution which is referred to as Edge Computing [11] involves assigning a task to a device, processing the task, and sending back the results to the requester. In a similar manner to the data sharing, edge processing requires scheduling, solving security and privacy problems, and more importantly providing incentives for the owners of the devices to share their computing resources. Edge computing incentive system is one of the use-cases that we consider for our proposed crypto-money system.

1.4 Challenges

Locating the files that each device wants to share should be carried out through a directory system. Access points can maintain the directories. These directories should be updated when a device relocates to a new network.

Authorization to receive data should not be handled by the device sharing the data. The authentication should be performed by the owner of the data and managed by the access point. This type of authentication is more relevant when a device relays stream data.

Security is another concern and challenge in sharing data. The application requires establishing a trust mechanism between the devices before the communication can take place.

The success of the application is directly influenced by the motivation of the devices to allocate their processing and bandwidth resources. An incentive mechanism where the service provider receives a special form of crypto-money in return for the provided resources is necessary. The incentive mechanism should be beneficial enough for the network users to encourage them to use it to their advantage. This incentive should be easy to earn and spend.

1.5 Scope of the Thesis

In this thesis, a complete model is proposed to share the unused bandwidth between the devices in a network for reducing the total traffic load of the servers and access points. Although the proposed model considers all aspects of a fully functional system, the focus of the research is on developing an incentive mechanism based on a crypto-currency to motivate the nodes to share their unused resources, as well as proposing an inter-domain payment system to be used between users themselves, and users and telecommunication operators globally. This will enable operators to build a solution for the payment of roaming charges, and even will allow subscribers to use local rates from the operators by paying through proposed global payment system.

1.6 Organization of the Thesis

Chapter 2 provides the basic concepts in applying block chain technology in crypto-currency and establishes the fundamental technical details, which are used in this thesis to design and implement the payment system. In addition, a summary of the similar systems proposed by the researchers have been provided to establish the ground for a comparative analysis of the performance of the proposed method.

Chapter 3 has details of our proposed method. The proposed method is part of a complete system where incentives are used to motivate the nodes for sharing their unused resources. We not only describe the payment model, which is the main focus of this thesis, but also necessary communication messages for establishing data transfers in different situations.

Chapter 4 includes the experimental evaluation of our proposed method. We have considered performance comparisons with similar methods reported in the literature.

Finally, in Chapter 5 we discuss the results and draw our conclusions. Besides, Chapter 5 includes suggested possible extensions and improvements.

CHAPTER 2

LITERATURE REVIEW

The Internet is witnessing ever-increasing applications areas constantly, which brings about more dependency of our daily activities on its reliability. The Internet of Things was developed to extend the concept of interconnection between people to the interconnection between things. These "Things" are capable interacting with their environments, sharing data, and reacting to messages. As the next step in extending the concept of interconnectivity through the Internet, researchers introduce the new concept of the "Internet of Assets", where the interactions between "things" are replaced with financial transactions between "Assets" [14]. The most important technical development, which created the necessary reliability for transparent and safe financial transactions, is the introduction of the block-chain technology. In the years to come, block-chain technology will change many things from our habits of managing our assets in doing business, to the way we utilize tools and devices to cast our votes. These changes will change the structure of many institutes completely, as the main financial systems such as banking and insurance systems are going to develop in accordance.

Obviously, among these developments, the most important part belongs to the introduction of financial transactions and crypto-money. Crypto-money is digital money that can be used for payments and is transferred over the Internet in a completely simple manner. This simplicity however, does not come with the cost of sacrificing security of payments. In fact, safety, transparency, and simplicity of conducting transactions with crypto-money or crypto-currencies are the most promising features that led to the introduction of many different cryptocurrencies such as BitCoin, Ethereum, and LiteCoin.

Same as any newly introduced technology, the most important challenge is how trustworthy the crypto-currencies are. Clearly, we want to use secure channels in transferring our money. The question that arises immediately is: how can crypto-currencies reach the required security level? The present financial system is based on our trust on the banking systems, which are managed and handled by central authorities. This mechanism ensures the security by keeping the financial information in private locations and restricting access to them to only a limited authorized people. The block-chain technology on the other hand warrants the security by a distributed registry system, which is accessible by every computer on a network. The transactions must be approved by the members of the network, which provides a level of trust based of transparency of the information. In the following sections, a brief review of the block-chain technology is presented. Subsequently, the applications and challenges are discussed.

2.1 Block Chain Technology

The concept of block-chain is directly related to the introduction of BitCoin as a crypto-money capable of performing reliable payments in an electronic environment, which was publicized in “Bitcoin a point-to-point electronic cash system” [Nakamoto]. The main motivation in developing BitCoin was solving the inefficiency problem in financial transactions stemming from the need to have a third party guarantee. It removes the centralized guarantee by combining all transactions in a single decentralized structure called a public ledger, which is readable, by all members of the network. This decentralized structure consists of a sequence of data blocks, which are stored in a chronological order. The blocks are chained to each other using hash values. It can be assumed that a block-chain is a secure definition for a database where the records are stored in blocks, the security is provided through a public ledger, which cannot be tampered easily. The public ledger is managed through a peer-to-peer network of participants [4].

The Blockchain Technology with the capabilities of providing open and decentralized cryptographic ledger to be shared across all nodes participating in the network is becoming the de-facto standard of the future peer to peer transaction network. Every successfully performed transaction between two parties is recorded in the secured ledger in a permanent way without the need of third-party authentication. Starting from late 2012 [4], the researchers started using blockchain technology separate from bitcoin. It allowed researchers to build new distributed ledger platforms such as Ethereum, Hyperledger, Hedera Hasgraph etc. While some of them concentrates on running faster, the others concentrate on solving scalability problems. It is reported in [16] that, while Ethereum can handle 10-20 transactions per second (TPS), Hedera Hashgraph can perform up to 100.000 TPS. It is also noted that in peak time visa system has a value of 50.000 TPS. It is also known that Hyperledger can perform 10.000 TPS in a single cluster.

In the blockchain technology, the ledgers are programmable which allows us to take actions based on a transaction hitting the ledger. The technology establishes trust among parties by enabling;

- secure transactions,
- elimination of intermediaries,
- reduced transaction costs and errors,
- improved auditability.

By establishing the trust among the parties, it will be trivial to solve the following problems by using the blockchain technology. Utilizing blockchain technology allows us to;

- replace complex, slow and error-prone business processes,
- provide provenance, ownership, usage rights, or status of a record,
- proof of identity,
- automatic execution of smart contracts.

2.1.1 Blocks

Blocks are the basic building units of a blockchain. A block in fact is a set of transaction records verified by their hash values, and linked to the previous block through the hash value of the previous block [13].
Figure 2.1 depicts the structure of blocks.

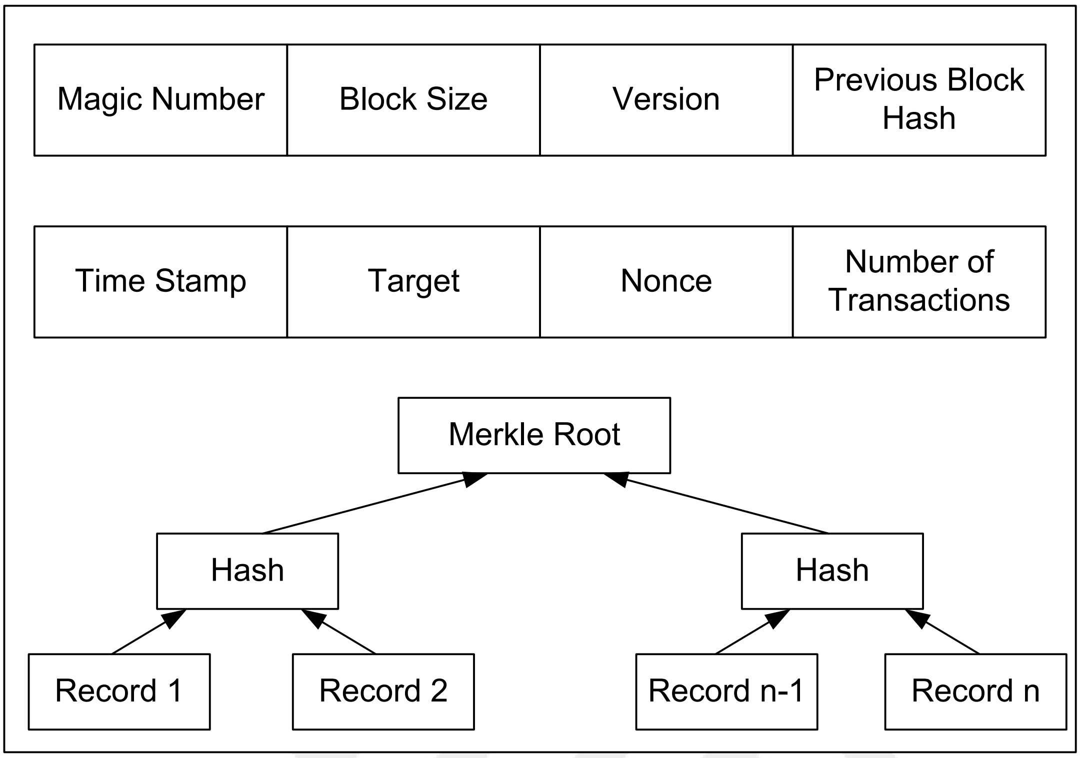

Figure 1 The Structure of Blocks in Block-Chain

As shown in Figure 1 each block consists of a header and a data part. The header part includes information about the block, the data records, and hash pointers to create a reliable chain from the blocks. Block header has the following fields:

- Magic number: Always has the value 0xD9B4BEF9
- Block size: Number of bytes in the block
- Version
- Hash of the previous block
- Merkle root hash
- Time stamp
- Target
- Nonce: initially zero
- Number of transactions

The hash values are pointers of the previous block in the chain of blocks, however, they also guarantee that any change in the previous block will be detected in the current block. These hash values make any tampering in the data infeasible. In fact, any change in a transaction record requires updating all following blocks in the chain [33].

2.1.2 Hashing

Hashing is defined based on function named hash function, which accepts as input a string of any length and returns a string of fixed length name hash value [9]. This concept can be shown as $h=H(x)$ where x is the input string of the arbitrary length, and h is the fixed length hash value. Hash function should have a reasonable time complexity such as O(n) to produce the hash value. Ideally, we expect a hash function to produce different hash values for different input strings. However, it can be proved that there exist cases where two different strings produce identical hash values. The problem of generating identical outputs for different input strings by a hash function is referred to as collision problem. The reliability of a hash function from security perspective is related to the difficulty of estimating the original value x, given the hash value h. Obviously the difficulty of estimating x depends on its probability distribution. If the probability distribution is not widely spread, an exhaustive search can determine the original string given its hash value. Hiding hash functions use a secrete string r to make estimating the original strings from the hash values when the distribution is not widely spread practically infeasible. These functions concatenate the secrete string (key) with the input string before applying the hash function. The operations of these functions can be defined as $hr = H(x,r)$, and $t/f=V(x,r,hr)$, where H is the hash function and V is Verifying function. V returns true if hr is generated by H given x and r as inputs and false otherwise.

2.1.3 Merkle Tree Structure

The transaction of a block is stored in a specific format named Merkle Tree [22]. A Merkle tree is a full binary tree where the data records are stored in the leaf nodes and the internal nodes store the hash values. Figure 2.2 depicts the structure of a sample Merkel tree.

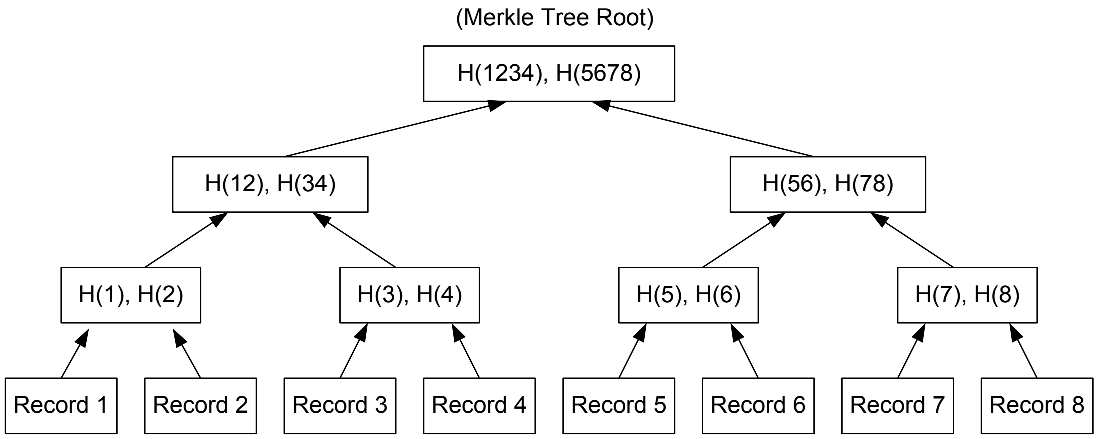

Figure 2 Merkle Tree Structure

As shown in Figure 2 the data records (which are transactions in a BitCoin implementation) are grouped in pairs and their hash values are computed. The hash values found in this way are stored in an internal node, which lies one level above them. In the next step, the hash values of the paired records are used to compute the hash values for their upper level. The hashing process continues until a single hash value pair is found and stored at the root of the Merkel tree.

Merkel trees can be used to verify the integrity of the transaction records. Any modification in a transaction will result in a different Merkel root hash that will not match with the originally computed one. In addition, Merkle trees can be used to verify if a transaction is included in a given Merkle tree. To perform this verification, it is simply needed to consider the blocks on the way form the transaction record to the tree root and compute the hash values as shown in Figure 3.

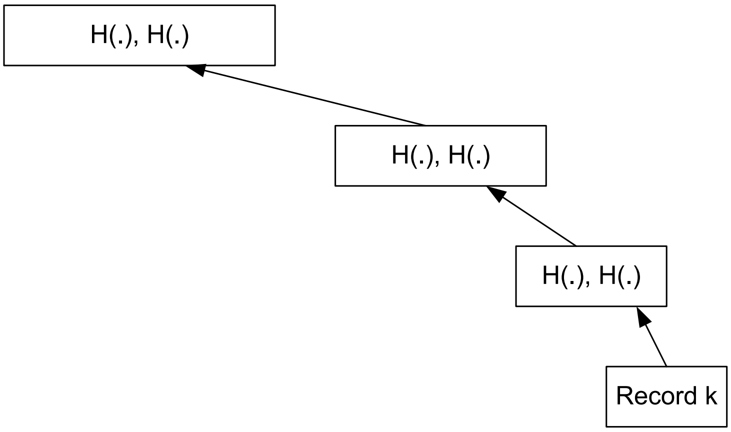

Figure 3 Inclusion Verification of a Record in a Merkel Tree

This property of the Merkle trees reduces the processing time complexity of an existence verification to log(n), where n is the number of transaction records in the tree.

Merkle trees are available in sorted formats as well. In the sorted Merkle trees, the transaction records are stored in their alphabetical or lexicographical order. The sorted Merkle trees simplify the non-inclusion verification of a record in the tree.

2.1.4 Proof of Work

Every block is added to the block-chain only when the last block of the chain is resolved by a miner. Each block contains a nonce field, which is initialized to zero. The miner should guess a number for nonce so that the hash value computed for the block is less than a threshold named Target. Target value adjust the difficulty level of computing a nonce value to resolve a block. The difficulty level is adjusted in a way that the average processing time to resolve a block is about 10 minutes. The Merkle tree includes a transaction named extraNonce. Each computation of the hash value involves changing extraNonce field, which requires re-computing the root hash value of the Merkle tree. This extra measurement guarantees that the processing will not finalize in less than the expected time.

As soon as a miner resolves a block, it creates a block from the transactions taken from the transaction pool, create the block and publish it by sending to the participants of the network. The block is added to the chain if it is confirmed by the majority of the participants.

2.1.5 Integrity and Security

As BitCoin and other applications of block-chain require integrity and security of the transactions, the algorithm considers some measurements. The first measurement inhibits storing more than one transaction from a single account in a block. This measurement helps resolving double spending problem, where a payment order is used multiple times in a repeated and falsified manner.

The need for the second measurement arises from the inherent distributed structure of the network. Since miners are rewarded for resolving blocks and adding transactions as new blocks to the chain, more than one miner may resolve a block and publish a new block. In this case, some participant may accept and add one of these blocks to their ledger and some the other. This situation results in generation of branches in the chain. The branches should be pruned to have a single chain and hence, a single ledger. The pruning rule is preserving the longer branch and pruning the shorter ones. The blocks pruned in this way are referred to as orphan blocks.

The third issue is the validity of the transactions. It is important to assure that the transactions are generated by authenticated nodes, and there has been no tampering of their values. In most of the distributed implementations of the block-chain algorithm this is carried out through running a consensus algorithm whenever a new block is created and published. Consensus algorithms however, suffer from many practical problems and imperfections such as lack of a global time, imperfect peer-to-peer communications [27], and unavailability of some of the nodes temporarily.

2.2 Examples of Blockchain Applications

Although blockchain was designed and implemented for monetary transfers through crypto-money, its powerful structure attracted researchers to adapt it to many other application areas [2]. In the following sections, some of these applications have been briefly introduced.

2.2.1 Crediting System

Smart contracts will change the traditional credit system. In the current system, the lenders often rely on incomplete, biased, and limited data which results in their underperforming rejecting the applications by clients who are already under high interest rates. In blockchain technology, one does not have to give anyone the manifest of his or her assets, their income documents and their identity. Hundreds of manual documents become unnecessary. The system can automatically reveal the creditworthiness of the person and how much credit he or she can borrow and can secure it within both parties [28].

2.2.2 Automobiles and Smartphones

Today's cars work with smart keys. Our mobile phones are only activated with the passwords we know. However, the password you use as your car key or to activate your smartphone is either stored in the key or on the sim card, and it is cumbersome and costly to prepare for their loss. The authority to exercise these entities on blockchain can be safely processed, tracked, renewed or revoked. In addition, the technology provides the facility of sharing car keys in a safe way [1].

2.2.3 Blockchain and Internet of Things (IoT)

Any thing is classified as a "thing" in IoT if it has a tranceiver capable of connecting to the internet and communicating with other things on the network [37]. When a thing like automobile joins the computer network, it is no longer a thing anymore and it allows communication between person and person. Analyzes made suggest that by 2020, 25 billion things will be tied together in the network. Thanks to this technology, your refrigerator can order milk, and the printer in your office can arrange the order according to how long the toner remains. On a larger scale, cities can become smarter and offer better living and working opportunities with a more green and sustainable management.

There are a few common problems in all of these cases. How will tons of data, coming from so many "things" connected to the Internet, be safely stored, displayed

and processed? How will companies protect their own data in this open environment?
Blockchain can answer all of these questions. The intelligent contracts written and implemented in a way that can never change the rules about who can view and process what information can easily resolve these problems [30].

2.2.4 Smart Instruments

Smart instruments are devices that connect to the Internet and give you more information about their applications and the surroundings. With this idea, even if you are next to your device, you can follow the work done by it, intervene and exchange information. This ensures that the devices operate more efficiently and more economically. Encrypted transfer of these devices to the blockchain ensures that the device is safe and can be used safely by someone else when necessary [5].

2.2.5 Supply Chain

Today, companies are replacing the human workforce within their supply chains with digital sensors. Until 2030, the number of digital sensors used in the supply chain sector is expected to reach a figure of 10 trillion. Blockchain technology can process, and store data from these sensors in a safe way that no technology can do [18].

2.2.6 Smart Contracts

Smart contracts are programs that can work on their own with this coding principle (if this then IFTTT). In real life, brokerage firms control whether the contractual parties fulfill their obligations. Blockchain technology allows these contracts to be automated and can be used for situations such as verifying not fulfilling or fulfilling the obligations of the contracting parties, where everybody is openly accommodated.
The application areas of smart contracts can range from financial derivatives to real estate law, insurance premiums to community funding [26].

2.2.7 Health Services on Blockchain

Records of personal health history can be transferred to the blockchain so that only authorized and relevant persons can view and process them. The same strategy can ensure that documents related to actual operations are delivered to the necessary institutions in a timely and error-free manner. The insurance companies will make the damage assessments easier, and patients' drug purchases and uses can be tracked without error [23].

2.2.8 Digital Right Management (Music) on Blockchain

The main problems in the music industry are shaped around property rights and copyright distribution. Property rights are often overlooked when the digital music industry makes the product a money-focused product. Blockchain and intelligent contract technology can create a music rights database in a comprehensive and error-free way and distribute the copyright of the artists in an honest and error-free manner [5].

2.2.9 Blockchain in Management

In today's elections held in almost every country, there are certainly complaints. In 2016, the three states in the US elections were requested to recount votes. After each election in Turkey same debates arise among the parties. Hackers consider election systems as very easy to maneuver even in the United States. However, a choice to be made with intelligent contracts on the blockchain will be completely safe and infeasible to intervene. The results can be displayed even instantly from the beginning of the election as the human power will not be needed for the counting of the votes. Elections can be completed in a much shorter time and with much less cost thanks to the blockchain. Moreover, the candidate will be bounded by their pre-election commitments as they are committed to the intelligent contract and are expected to fulfill their commitments after the election [24].

2.2.10 Identity Security on Blockchain

Especially the social media platforms know much more about us than we do. These platforms sell personal information to advertisers for money. Through blockchain technology it is possible to change this situation entirely, allowing only the necessary parts of the personal information to be viewed by the requesting people. For example, when you go to a bar, security at the door does not have to require you an identity document that has information about your birth place and your mother's name. Blockchain encrypts your credentials to protect you from advertisers and fraudsters [15]. Documents such as birth, marriage and death certificates have an important place in our lives. Through these documents, we are able to demand many rights, such as voting and citizenship. However, there is no fully reliable system that protects these documents from risks such as fraud, loss or damage. According to UNICEF, one out of every three children under the age of five has no birth certificate. Blockchain will be the biggest help in securing these documents and ensuring security [38].

2.3 BitCoin vis-à-vis Other Crypto-Currencies

As mentioned in the previous sections, the blockchain technology was first introduced to support an electronic payment system with a distributed structure named BitCoin. BitCoin despite its successful implementations suffers from a few drawbacks. These drawbacks motivated researchers to introduce similar crypto-currencies, which could achieve the same functionality, and do not suffer the same or similar drawbacks. In this section, a review of the most important crypto-currencies is presented.

2.3.1 Issues with BitCoin

As mentioned earlier, Bitcoin does not have a relationship with a central bank or an official institution. BitCoins are produced by miners [29]. A miner after finding the nonce value for the last block of the public ledger, can add a new block and gain BitCoins in return, Determining nonce value is a long processing which is intended to prohibit Sybil attack [7]. Sybil attack is a serious threat to distributed systems in which the attacker uses different identities to affect the operation of the system. However, finding nonce entails spending a lot of energy. BitCoin mining requires on average 260KWh per transaction, which amounts to 27.28TWh yearly consumption [6].

The second major issue with BitCoin is the long latency before a transaction is confirmed. This latency is about 164 minutes on average.

The third issue is related to the limited size of the blocks. Since determining a nonce value requires a long processing, the upper limit on the number of transactions in a block negatively affects the performance of the crypto-currency.

Many alternative crypto-money systems have been proposed. However, except for a few, the remaining have attracted limited attention.

2.3.2 Ethereum

Ethereum is an open-source distributed platform which is based on blockchain technology [8]. Ethereum supports consensus method of BitCoin for validating blocks, however, it uses state transitions of transactions [35]. The crypto-money in Ethereum is Ether. However, an internal payment unit named Gas is also used for using network and processing resources. The payment for utilization of the resources prevents spam transactions from flooding the network. Similar to BitCoin, Ethereum uses blocks to create the public ledger which includes the transactions and hash pointers. However, Ethereum considers state values for accounts which indicate their balances. Though, the state values are not stored in the blocks, and Ethereum uses a separate Merkle tree to store them. The mining in Ethereum mitigates utilization of ASICS and encourages use of GPUs. An important improvement over BitCoin is the block processing time which is around 15 seconds compared to ten minute processing time of BitCoin. Ethereum does not have a any limiting policy for the total amount of Ethers while the amount of BitCoins that miners can acquire is halved every 4 year. Ethereum also solves the limits on the block size problem.

2.3.4 LiteCoin

LiteCoin is a modified form of its counterpart crypto-currency BitCoin, which tries to resolve its major drawbacks [3]. LiteCoin claims that the transaction confirmation time is almost zero (instant confirmation). This feature makes LiteCoin attracting for many real-time payment applications. The data structures used by LiteCoin are very similar to BitCoin, both being based on blockchain technology. Miners are responsible for creating blocks and adding them to the public ledger. Adding a block is rewarded by 25 fiteCoins. Similar to its counterpart, BitCoin, the total number of LiteCoins that miners can produce is reduce by half every four year [21].

2.3.5 Nano

Nano is another alternative for blockchain based crypto-currency implementations [20]. Similar to its counterparts, Nano uses consensus for verifying the validity of transactions, however, it uses a different protocol, which is based on Proof of Stake (PoS) instead of proof of work as is used by BitCoin [17]. The participants in a PoS system use weighted votes with weight values proportional to their wealth. This means that the wealthier members are given more power to maintain the validity of the system. PoS has the advantage of avoiding power consuming computations. Nano crypto-currency is among the first methods that are based on Directed Acyclic Graph (DAG) [34]. Nano defines blocks with single transaction capacities. Hence, blocks and transactions are closely related. Despite other crypto-currencies, Nano creates multiple block chains, where each account has its own blockchain. Each transaction consists of two messages. The sender creates a send transaction which is confirmed immediately and the balance is updated accordingly. The receiver should submit a receive message before his balance is updated.

2.3.6 TelCoin

Yet another blockchain technology based cryptocurrency is TelCoin [32]. The main goal in developing TelCoin is providing the facility for financial operations without having any banking system involved. The developers of TelCoin consider the subscribers of mobile operators as the potential users of their cryptocurrency. A subscriber of the member mobile operators becomes able to transfer or receive money to or from other members of the community. TelCoins can be obtained through transferring from another member, or they can be bought from the mobile operator, which is in contrast with other cryptocurrencies where crypto-money can be earned by providing services such as transaction mining.

2.4 Distributed Ledger Technologies

In a higher level, we may consider a ledger as a collection of data items, replicated and distributed over different locations. These data structures do not require any central administration; however, a consensus system is required to ensure that all replicas are exactly alike. In addition, a peer-to-peer network is used as the underlying infrastructure for accessing the data. The internal organization of the data is not necessarily the same in all implementations. For instance, a linear list is used in blockchain, which puts the data blocks in a chain (hence the name), while Iota is based on directed acyclic graphs. Many unifying technologies in implementing distributed ledgers have been introduced. In the following sections, we will introduce some of these technologies.

2.4.1 Hyperledger

Hyperledger foundation is based on open source project supported by Linux foundation, and shared ledger databases. The main idea is developing open source tools and libraries for distributed ledgers used in different applications such as finance, health care, and supply chain. Hyperledger defines its goals as follows [12]:

- Create enterprise grade, open source, distributed ledger frameworks & code bases to support business transactions
- Provide neutral, open, & community-driven infrastructures supported by technical and business governance

- Build technical communities to develop blockchain and shared ledger POCs, use cases, field trials and deployments
- Educate the public about the market opportunity for blockchain technology
- Promote our community of communities taking a toolkit approach with many platforms and frameworks

Hyperledger team developed necessary tools and framework to provide a unified approach in utilizing the distributed ledger data structures. For instance, Hyperledger Fabric is intended to provide the possibility of using consensus and membership functions in a plug-and-play manner.

An important feature of hyperledger project is Hyperledger Sawtooth which provides a novel consensus algorithm, and a method for Proof of Elapsed Time (PoET) which is energy efficient.

2.4.2 Hedera

Hedera project follows similar goals as Hyperledger but they put more emphasis on efficiency of processing data. Unlike blockchain which requires a minimum elapsed time before a new block is added to the chain, the instant approval of the transactions in Hedera provides the possibility of microtransactions with very low costs. Hedera is based on virtual voting consensus which is quite fast and can handle millions of transactions per second [10].

Hedera has the extra features of providing fair transactions meaning that no user can block a transaction from reaching the hashgraph, or influence the order of processing transactions to their benefit.

Hedera is more powerful than similar structures in terms of its resistance to security threats such as denial of service attacks. The developers claim that the hashgraph has proven asynchronous Byzantine fault tolerance [10]

CHAPTER 3

DEVICE-TO-DEVICE DATA TRANSMISSION

3.1 Overview

In this section, we provide a general overview of the system. The overview describes the sequence of actions taken in the two main parts of the system, namely establishing the data flow between the devices in a proximity, and the incentive system, which is based on a crypto-money payment. The crypto-money based incentive system has two-fold benefits. Firstly, it motivates the owners of the devices to share the capacity of their devices. This motivation is essential for the successful application of the proposed method. Secondly, the crypto-money based structure of the proposed incentive system has the necessary transparency to ensure a fair incentive system.

Our assumptions are that a network with a base station/access point and several stations is present. A controller software running at the base station supervises the communications and payments. Hereafter, the base station and the supervisor software will be referred to as super node. All other stations are referred to as nodes. We assume the nodes are capable of direct Wi-Fi or Bluetooth communications.

3.1.1 Establishing the Data Flow Connection

Although many different application scenarios can be imagined for the proposed system, we claim that these applications can be grouped into two main categories:

- On demand data flow
- Multicast data flow

In the case of on demand data flow, a device requests the data and the super node establishes the data flow connection between the requester and a provider nodes when they are at a reachable vicinity. In the second category, the data is provided by a center such as a publisher in a pub/sub system. A super node uses the device-to-device connections to facilitate delivery of these messages. In the following sections, the procedure used with each category is summarized.

3.1.2 Connectivity Model

The super node maintains a matrix named "connectivity matrix". The entry at row i column j of the connectivity matrix indicates whether device i is close enough to device j to establish a direct link connection (indicated by one) or not (indicated by zero). Besides, the super-node computes a connectivity probability value for each pair of devices based on their connected periods in the past. This probability is computed using Markov Chain Model and is described in details in Section 3.2.

3.1.3 Data Availability and Volunteer Model

The super node maintains a table indicating the willingness of a device to share its direct link bandwidth capacity. The super node assumes a volunteer device is available for sharing its bandwidth/data as long as it is connected to the network. The device however, may change its status to unavailable if desires. In addition, the super node has the list of multimedia data that each device is willing to share. The device may update the list by adding or removing an item from its corresponding list.

3.1.4 Solicited Data Flow

In Solicited mode, a device sends a request for a specific data. The super node consults its data table to determine which device(s) have the data in their repositories. If the data is found available at some devices, the super node filters out those devices, which are not currently available. Next, the super node selects the node with the highest connectivity probability value with the requested device. The super node sends messages containing necessary details to establish direct link connection and data transfer to both devices. When a volunteer device is transferring data through direct link to a device in its vicinity, the super node changes its status to unavailable to avoid assigning new transmission request to it. We assume, a device can have a single direct link at any given time. At the end of the transmission, both devices confirm the completion of the transmission by sending acknowledgement messages to the super node. The acknowledgement includes the amount of data delivered. The super node updates the status of the devices and creates a transaction that is inserted into the transaction pool. The transactions are worked on and a new block is added to the block chain by super nodes. The details of these steps have been given in Sections 3.5.

3.1.5 Unsolicited Multicast Data Flow

Multicast messages cause problems originating from their definitions and implementations. For instance, multicast messages are not acknowledged. Hence, multicast transmissions are not suitable for reliable applications which are sensitive to packet losses. Besides, to maximize the number of nodes receiving the data correctly, access points maximize the energy and reduce the data rates. Higher energy utilized for multicast transmissions also contributes to the higher rate of interferences. These problems justifies a solution where the multicast messages are transmitted as unicast messages from access points to one of the nodes, and relayed from that node to the remaining recipients.

In our proposed model, the super node groups the recipients into sub groups based on their connectivity status. This grouping is carried out considering the network as a graph where the links are defined using the connectivity values maintained by the super node. The super node selects a node with the maximum connectivity value (as defined in Section 3.2) from each group and forwards the message as a unicast message to these representatives. The selected nodes are responsible for forwarding the message to the corresponding recipients in the group. The representative nodes of each group sends a confirmation message to the super node when the transmission of the messages is concluded. The confirmation message is an aggregate message containing ACK messages from the recipients. In addition, the confirmation message includes the list of the nodes, which received the message. If the message has not been delivered to a node (probably due to connectivity problems arising from the mobility of the nodes), the super node will send the message directly to that node.

The super node at this stage, adds the corresponding transactions to the transactions pool. The transaction amount is computed based on the number of recipients acknowledged the message, and the size of the message.

3.2 Connectivity Model

A major challenge in D2D data delivery is the mobility of the nodes, which negatively influences the performance of the delivery system. This mobility may occur in two different ways. A mobile node may leave the network and join a different (adjacent) network. The second case happens when the mobile node is displaced inside the network however, its direct signal reachability changes. The second problem can also occur when the signal power falls below a threshold level due to moving obstacles arriving between the nodes. The super node hence should prefer the connections with the lowest probability of connectivity problem if more than one choice are available. This selection requires modeling the connectivity between the nodes. We consider the connectivity pattern of the nodes in the past to predict their future behavior. The connectivity model is based on continuous time Markov chain. We assuming the random variables ξ_{ij} and ς_{ij} indicate that nodes i and j are in connected or disconnected state at a given time respectively. Besides, the state transitions from connected to disconnected or vice versa are independent and continuous time events. Hence, the random variables ξ_{ij} and ς_{ij} follow exponential distributions with CDFs as given in Equation 3.1 and 3.2.

$$\Pr(\xi_{ij} < \tau) = 1 - e^{\mu_{ij}\tau} \qquad 3.1$$

$$\Pr(\zeta_{ij} < \tau) = 1 - e^{\lambda_{ij}\tau} \qquad 3.2$$

where μ_{ij} and λ_{ij} are the distribution parameters. Assuming that *m* transitions have happened during the bounded past period, a maximum likelihood estimation can be used for determining the values of μ_{ij} and λ_{ij} from a limited number of transitions as given in Equations 3.3 and 3.4.

$$\hat{\mu}_{ij} = \frac{m-1}{2\sum_{z=1}^{(m-1)/2}(t_{ij}^{2z+1} - t_{ij}^{2z})} \qquad 3.3$$

$$\hat{\lambda}_{ij} = \frac{m-1}{2\sum_{z=1}^{(m-1)/2}(t_{ij}^{2z} - t_{ij}^{2z-1})} \qquad 3.4$$

where $\hat{\mu}_{ij}$ and $\hat{\lambda}_{ij}$ are the maximum likelihood approximations for μ_{ij} and λ_{ij}. Besides, we have assumed that the nodes are initially disconnected. t^{k}_{ij} is the time of k^{th} transition occurring between nodes i and j. We define the connectivity rate as given by Equation 3.5.

$$\psi_{ij} = \frac{\mu_{ij}}{\mu_{ij}+\lambda_{ij}} \qquad 3.5$$

where the connectivity rate ψ_{ij} changes between 0 and 1, and is maximized when the two nodes have been in connected state during the past period. Here, it is assumed that the nodes report changes in their connectivity status with every other node to the super node. The super node updates its connectivity table values using Equations 3.3, 3.4, and 3.5.

3.3 Data Delivery

In this section, we provide the details of data delivery by the proposed method.

Before any D2D data delivery, a sequence of steps should be taken to establish the connection and start the transmission. In the following subsections, the details of these steps are given. The data delivery is performed in two different mode of solicited and unsolicited. The sequence of steps in each of these data delivery modes is explained below:

3.3.1 Data Structures used by Super Nodes

Super nodes should maintain the list of the nodes in their network and their status, the connectivity and connectivity probability between the nodes, and the media files that each nodes has in its repository and is willing to share. These data is stored in the following data structures.

Nodes: is a list of nodes, their current *Connectivity Status* that indicates whether they can communicate with the super node or not, *D2D Status* indicates if the node is available for D2D data delivery, busy with another D2D transmission, or not available for some other reason, and finally the average *Availability* time which is used for credit computations as explained in Sections 3.4.2 and 3.4.3. Figure 4 depicts the data structure.

Node Id	Connectivity Status	D2D Status	Availability

Figure 4 Node Status Data Structure

Connectivity Table: includes the current connectivity between each pair of nodes, and the rate at which the two nodes have been connected. This rate is found as explained in Section 3.2. Figure 5 depicts the data structure where a box at row *i* and column *j* has the connectivity status of nodes with ids given at row and column *i* and *j* respectively. It should be noted that the node ids are not stored in the table in any order for optimization. This optimization is based of on the assumption that the network is volatile and the rows/columns that becomes vacant when a node leaves the network should be readily available to be used by new nodes.

	Node Id 1	Node Id 2		Node Id j
Node Id 1				
Node Id 2				
Node Id i				Connectivity Connectivity Rate

Figure 5 Connectivity Table

Media List: includes the list of media files that can be transmitted by a D2D connection. The data structure includes the node id, which stores the media file. The data structure is depicted in Figure 6.

Node Id	Media Data Id

Figure 6 Media Data File and Corresponding Nodes

Media Identifiers: includes ids assigned to each media data file and the keywords, which can be used in looking for it. For each media file a maximum of 10 keywords have been considered. Each row in this data structure stores only one of the keywords. In addition, the media file format is stored in the record. Figure 7 shows the media identifier data structure.

Media Data Id	Format	Keyword

Figure 7 Media Identifiers and Keywords

3.3.2 Solicited Data Delivery

Solicited data delivery starts with a request from a member node. The super node evaluates the request and if it can be satisfied through a D2D data delivery a connection is established.

3.3.2.1 Request

A request is started by a node sending a message to the super node. The message may include up to 10 keywords or the identifier of a media data file. The request process is performed in three steps. In steps one, the requesting node sends message 1 (Figure 8). This message includes either one or some keywords describing the media file or its identifier.

Message Type	Sender Node Id	Media File Id	Requested Format	Number of Keywords	Delimiter Separated List of Keywords

Figure 8 Message 1: Request

The super node replies by sending message 2 (Figure 9) which includes the list of media files matching the provided keywords. The list includes only one item if the initial request from the node has been made using media identifier instead of keywords. Besides, the list may be empty if the media is not found in the media list maintained by the super node.

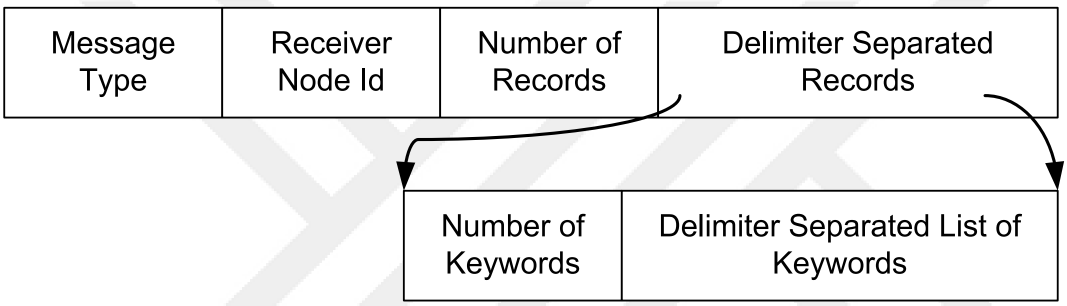

Figure 9 Message 2: List of Media Files matching the Request Criteria

In reply to message 2 the requesting node either chooses one of the items listed in message 2, or rejects them all. This reply is sent from the node to the super node using message 3 (Figure 10). The super node will proceed to the next steps according to the information given in message 3.

Message Type	Sender Node Id	Requested Media File Id	Starting Byte

Figure 10 Message 3: Selecting form the Media List

3.3.2.2 Establishing the Connection

If the node replies with the identifier of one of the media files, the super node decides to establish a D2D data delivery connection. The requested media file might be shared by more than one nodes. The super node decides which node should be used in establishing the D2D data delivery. Two different criteria are used for selecting node for delivering the requested media file. The first criterion considers the likelihood of a connection problem during transmission. The super node uses connectivity rate, which indicates the probability of having connection problems due to node displacements, noise, interference, or other problems. This metric, which is described in Section 3.2, tries to maximize the probability of a seamless transmission. The second criterion assures fair opportunities provided for all volunteer nodes. This requirement is necessary to ensure that the incentives given for direct data delivery will be effectively utilized. The super node keeps record of the number of times each node takes part in a D2D data delivery and in case that the same connectivity values are returned for volunteer nodes having the requested media in their repository, the node with smallest number of previous deliveries is selected. Any node currently engaged in a D2D transmission is not considered for a new D2D connection.

The super node uses the messages shown in Figures 11 and 12 to invite the requester and provider nodes to establish the connection. Both nodes should confirm the establishment of the connection to the super node.

Message Type	Time Stamp	Send To	Media File ID	Format	Starting Byte

Figure 11 Super Node Instruction Message to the Sender to Start D2D Transmission

Message Type	Time Stamp	Receive From	Media File ID	Starting Byte

Figure 12 Super Node Instruction Message to the Receiver to Start D2D Transmission

3.3.2.3 Closing the Connection

When the transmission is over, the sender and the receiver confirm the completion of the transmission by sending a message to the super node. The message includes the starting time, duration, and the transmission parameter values which are used for computing the credits as described in Sections 3.4.2 and 3.4.3. The super node changes the status of both nodes from busy to available. The super node initiates the transaction creation process at this stage.

3.3.3 Unsolicited Data

In unsolicited data delivery, the super node should deliver a multicast message to a subset of the network nodes. For instance, the message can be data from a publisher/subscriber (pub/sub) server. The goal in this case is minimizing the number of messages sent by the super node, and converting broadcast message into unicast messages as unicast messages are less prone to interferences due to their lower energy. In the following subsections the details of the proposed method are presented.

3.3.3.1 Grouping the Nodes

The optimum solution from the super node perspective is forwarding the message as a unicast message to one of the nodes to deliver it to all interested nodes. However, not in all cases the super node is able to find a node in connected state with all interested nodes. Hence, as a solution we consider the network as a graph and obtain its minimum spanning tree rooted at the super node. We use Kruskal's algorithm to obtain the minimum spanning tree [31]. Figure 13 depicts a sample minimum spanning tree obtained from a graph. The links belonging to the spanning tree are shown with thick lines.

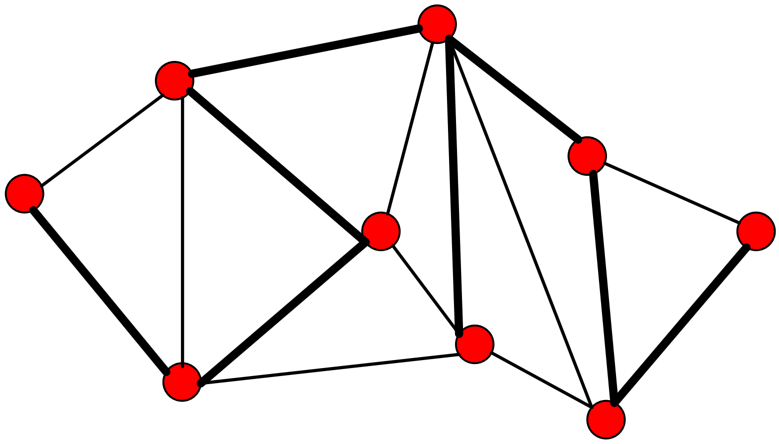

Figure 13 Minimum Spanning Tree Obtained from a Graph

The graph connecting the nodes is a weighted graph where the links are assumed to be bidirectional and their weights are given by the reciprocal of the connectivity rate values of the links, except the links connecting the nodes to the super node where the weight is always equal to ten. This weight assignment makes the algorithm prefer the links with higher connectivity rate. In addition, we prefer to minimize the number of messages sent by the super node. Therefore, the algorithm choose the minimum number of links between the super node and the other nodes due to the high values of these links. Hence, the minimum spanning tree will prefer paths through nodes to reach any destination rather than using direct links from the super node. Figure 14 depicts a sample case of minimum spanning tree created using the weights as assigned by the proposed algorithm.

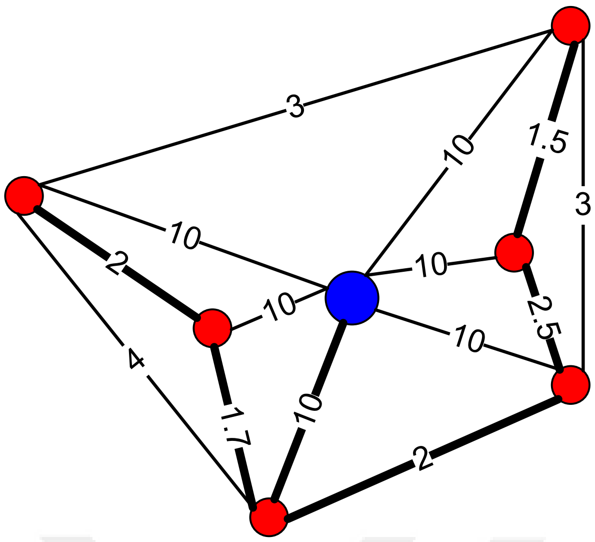

Figure 14 Minimum Spanning Tree Obtained using the Proposed Method

Since the messages sent in this way are multicast messages, not all nodes of the network should be included in the spanning tree. We consider a pruning algorithm to eliminate the branches without any recipient of the message.

3.3.3.2 Establishing the Connections

The super node sends the multicast data as unicast messages to its immediate neighbors on the minimum spanning tree. The message contains the next hop recipient list as shown in Figure 15. Each node will forward the message according to the information given in the message.

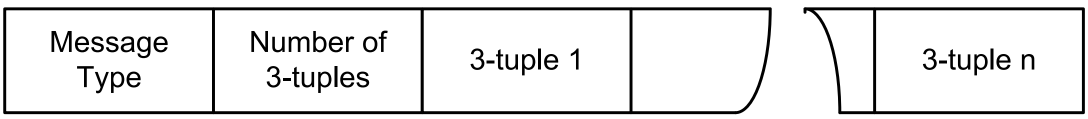

Figure 15 Unicast Message Layout Sent over Minimum Spanning Tree

Each message includes 3-tuples wherein the first part indicates whether the node is a recipient of the message or it should just relay the message, the second part is the node id of the sender and the third part is the node id of the receiver. For instance if node 500 is a relaying node on the spanning tree and nodes 600 and 650 are the next nodes on the path the list will include tuples <0, 500, 600>, <0, 500, 650>.

3.3.3.3 Closing the Connections

Each recipient of the multicast message sends back an acknowledgement message along the minimum spanning tree to the super node. The acknowledgement messages sent over the minimum spanning tree are aggregated before being forwarded by each node on the path. The super node finalizes the transmission by considering the average availability of each node, the size in bytes, and the number of messages sent by each node to create necessary transactions and adding them to the transaction pools

3.4 Incentive Model

The successful implementation of the proposed method is strictly dependent on the incentives that motivate the nodes to allocate their unused resources, and share data. These incentives should be fair, transparent, and proportional to the allocated resources. We propose a model for computing the credits that a node receives as incentive, which considers the amount, type, and quality of the allotted resources. Besides, we develop a blockchain based algorithm to keep track of the transferred incentive credits in a transparent and reliable way. In the following sections, we describe these methods in details.

3.4.1 Credit Computation

The incentive model considers rewarding resource sharing with a specific credit which from hereon will be referred to as *TelCash*. In order to compute the TelCash value of each resource sharing we have considered a set of criteria. However, since solicited and unsolicited data transmissions have different properties, we differentiate the credit computation criteria of these categories.

3.4.2 TelCash Computation for Solicited Data Transmission

The credit value embodies the extent to which a node provides data transmission services according to quality metrics of end users. Hence, a higher credit value indicates that the provided service is of a higher quality level. Obviously, for a trustworthy credit system, an objective evaluation metric based on clearly defined parameters is necessary. In the proposed method, the computed TelCash credit for each data transmission is determined through a weighted sum of the five different criteria. The final TelCash credit is defined as

$$\text{Credit Value (TelCash)} = \sum_{i=1}^{5} W_i P_i \qquad 3.6$$

where W_i is the weight value corresponding to the i^{th} parameter P_i. The weight values are assumed to be determined once and remain the same throughout the utilizations of the system. This assumption is in contrast with the Service Level Agreement (SLA) contracts available in cloud computing services. In our customized credit model we adopt the following criteria:

- *Availability*: As explained in Section 3.3.1 the super node maintains a list of the volunteer nodes, which includes their availability value. A node may change its availability value by sending a request to the super node. The super node determines the availability parameter of each node by finding the ratio of its *available* time to the sum of *available* and *unavailable* times as

$$P_{Avilability} = \frac{T_{Available}}{T_{Available} + T_{Unavailable}} \qquad 3.7$$

- *Quality of Service (QoS)*: QoS is especially relevant when the communicated multimedia data is streamed instead of being downloaded to the receiver device. In this case, the initial delay, jitters, and data rate are important factors. Jitters can be avoided by buffering media file initially if an estimation of the data rate between the two nodes is available. However, data rate fluctuations can result in jitters despite initial buffering. On the other hand, any transmission rate over the playback rate may not be desired as it entails larger buffer size. Hence, we compute QoS metric value as the ratio of the waiting times due to initial buffering or jitter, to the total playback time as

$$P_{QoS} = \frac{T_{initial\,buffering} + \sum T_{disuption(i)}}{T_{Total}} \qquad 3.8$$

  It should be noted that if streaming in not intended in receiving the media file, the value of this parameter will be zero.

- *Completion*: Mobility is an intrinsic characteristic of the nodes in wireless networks. As a result, the connectivity state of the nodes engaging in a D2D data transmission is subject to change at any time. This characteristic brings about incomplete transmissions. Therefore, the third parameter in our incentive metric is whether the data delivery task completed successfully or not. The completion parameter is a binary parameter, which takes a zero value if the data delivery did not complete, and one otherwise. It should be noted that even if the transmission is not completed, the transmitter receives credit for the partial transmission. This consideration has twofold reasons: first, it engages mobile nodes in D2D transmissions. Second, the proposed model considers segmented transmissions. Hence, a new node can take over the task from the disrupted point.

- *Data Size*: This parameter measure the amount of the data transferred in a D2D communication. Data size is measure independently from its type (multimedia, etc.), and transmission speed. We consider the parameter as the number of Kbytes of data.
- *Data Rate*: A faster transmission is a desired feature and should be awarded by extra credits. However, we do not consider any time restriction here and do not punish slow transmissions with frequent disruptions. This parameter is in contrast with QoS in which the disruptions and their durations are of significance. Hence, we consider this parameter when the transmission does not have time restriction requirement (non-streaming data). The parameter is measured in terms of average Kbytes/sec
- *Transcoding*: The requested format of the media file and the available format can be different. In this case, the sender is required to convert the media file into the requested format. This process requires allocating parts of the processing resource of the device and hence should be awarded by TelCash.

3.4.3 TelCash Computation for Unsolicited Data Transmission

The main differences between solicited and unsolicited data transmission modes in terms of data type are that the data in unsolicited mode is not bulky and without strict transmission time requirements. Hence, parameters such as QoS are not relevant here. This implies that data rate does not have any significance is unsolicited mode as well. We consider three parameters for defining the credit, and a weighted sum of these parameters will determine the final credit value as

$$\text{Credit Value (TelCash)} = \sum_{i=1}^{3} W_i P_i \qquad 3.9$$

The parameters considered for credit computation are as follows:

- *Availability*: This parameter is evaluated in the same way as we described in Section 3.4.2 for solicited data transmission. The availability measures the fraction of time that a node is interested to share its communication resources.
- *Data Size*: This parameter measures the size of the multicast message in Kbytes. The description of the parameter is the same as its description for solicited data transmission given in Section 3.4.2.
- *Number of Messages*: The main difference between the transmission type in solicited and unsolicited modes is that is unsolicited mode the data is transmitted in multicast mode while in solicited mode it is unicast transmission. Therefore, the number of messages forwarded by a node over the minimum spanning tree should be considered as a parameter for credit computation. This parameter is an integer greater than or equal to zero. The zero value of this parameter indicates that the node was not able to forward the message.

3.4.4 Transferring Parameter Values to the Super Node

The super node has the responsibility of computing the credit value and creating the corresponding transaction. In solicited data transmission mode, the receiver acknowledges the end of transmission to the super node. The acknowledgment message include the values of metric parameters except for the availability, which is computed by the super node using the information from its own data structures. In unsolicited mode, the immediate neighbor nodes of the super node in the minimum spanning tree are responsible for aggregating the acknowledge messages into a single message and sending it to the super node. Similar to the solicited transmission mode the acknowledgment message in this mode does not include availability parameter.

3.5 Representing the Transactions

When the super node has computed the amount of TelCash for the transaction, it adds a record to the transactions pool, which is publicly readable. Similar to the block-chain structure used by Bitcoin or Ethereum, TelCash has an ordered list blocks containing the transaction details. The block structure used by TelCash and its maintenance however, have significant differences, which have been introduce to customize with our specific application. In the following sections, we describe our modified block-chain model, the customized block structure, and the processing details.

3.5.1 Customized Block-Chain Properties

The customized properties of the proposed model are follows:

- The customized model is designed to involve no mining process. Instead, the verification and registration of the transactions are carried out by the super node. Despite this restriction, the ledger and transaction pools are publicly accessible. The main reason for considering this feature is providing a safer system against malicious actions, faster processing of the transactions, and avoiding unnecessary energy consumption by the mobile nodes, which have limited energy resources.
- In similar crypto-money systems such as Bitcoin, the users can earn credit through mining. Since in our proposed model the nodes are not involved in mining process, we allow them buy credit from the super node, which in fact represents a communication service provider. This type of changes in the credit level of a node is shown as a transaction where the super node transfers a given amount of TelCash to the account of a node. The balance of the super node is not affected by transactions.
- Our proposed model allows the balance of the node accounts become negative. This flexibility is based on two features of the proposed model.

First, the amount to be transferred from the account of requester of data depends on some parameter values, which are not available before the completion of the data transfer. Hence, controlling the balance will be on approximations only. In addition, the node with a negative balance can buy credit as mentioned above.

3.5.2 Modified Block Structure

Each block in our proposed method consists of two segments namely Header, and Data. The data segment includes a set of transactions organized in a Merkle tree structure in the similar way as other cryptocurrencies such as Bitcoin. The header segment includes an identifier which at the same time represents the version value of the block-chain used, hash value of the header of the previous block, hash value of the data segment, number of transactions in the data segment, and a time stamp. The hash values are computed using SHA256. It is important to note that the modified block structure does not include nonce field as no challenge is considered to slow down the process. Figure 3.13 shows the block layout in the proposed method.

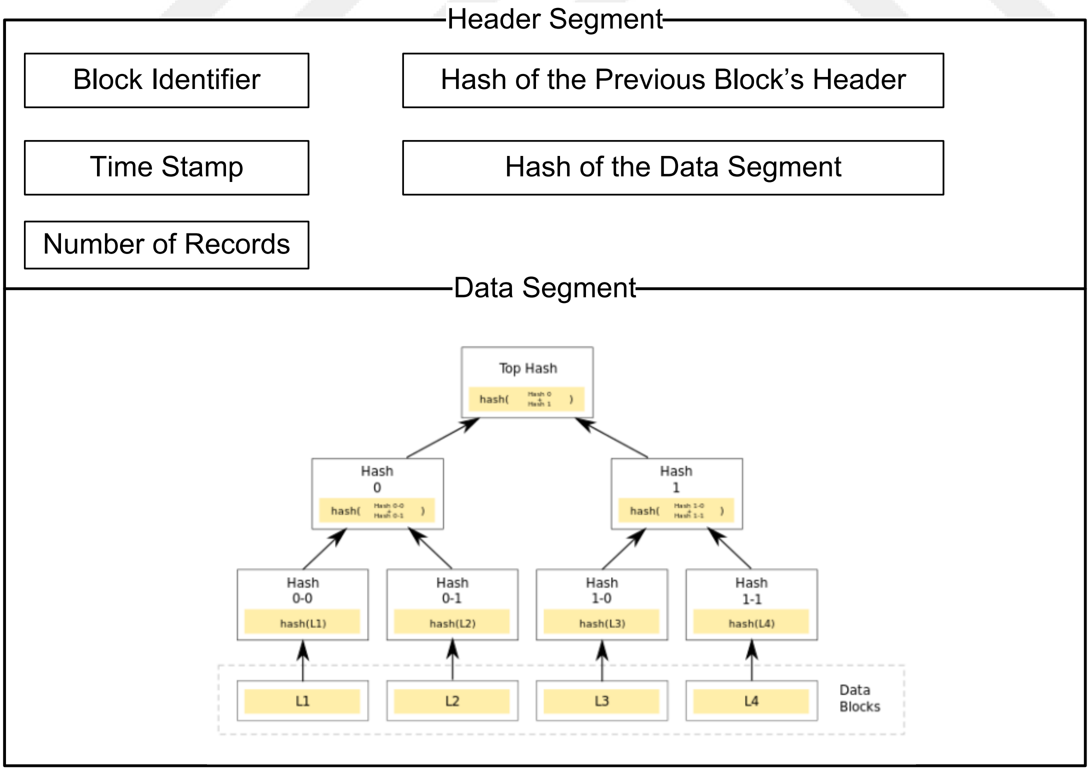

Figure 3.13 Layout of the Blocks

3.5.3 Processing Transactions

As explained in the previous sections, after the completion of each data transmission, both the sender and the receiver inform the super node by sending the values of the evaluation parameters. These messages include the node id of both devices involved in the transmission, the values of the parameters, time stamp, and the hash value created using the private key of the node sending the message. In addition, each transaction record has a status field, which is not included in computing its hash value. The status field indicates whether the record has been processed (included in a block) or not. The super node creates a transaction record and adds it to the transactions pool after receiving the messages from both nodes and verifying their validity. The transaction record includes a transaction id, the node ids of sender and receiver, transaction amount, a time stamp, super node id, and transaction hash. The hash value is computed using the concatenated fields of the record and the private key of the super node. Hence, the super node plays the role of the trusted node for transaction validity verification. The transaction pools and the block chain are visible to all nodes in all of the networks from the same service provider. Therefore, a mobile node will be able to spend its earned TelCash when it leaves the current network and joins another one. The transaction record is depicted in Figure 16.

Transaction ID	Sender Node ID	Receiver Node ID	Amount	Time Stamp	Hash	Status

Figure 16 Transaction Record

It should be noted that the transaction id is created by concatenating the node id of the super node, and the incremented sequence number of the transaction records added by this super node. A block is created by writing transactions in its data section. The hash value of the data section is computed and written in the header section of the block. The block also include the hash value of the header section from the previous block. These measurement guarantee that the transactions cannot be tampered by a malicious node.

3.5.4 Edge Computing Support

The media files are provided in different formats and encodings. The applications in end user devices may not be capable of handling the media data in all different formats. Hence, conversion from one format (resolution, frame rate, bit rate, or encoding standard) can be necessary before sharing media data. This process, which is referred to as transcoding, is generally very expensive in terms of processor time. In traditional implementation of centralized data centers, transcoding and reformatting data are handled by large scale processors. In the proposed distributed model, the transcoding is performed by the node who is sharing the file. This consideration is to provide the proof of applicability of the proposed crypto-money incentive method to edge computing as well. However, the edge computing in general, and transcoding in specific, can be performed independently from data sharing.

CHAPTER 4

EXPERIMENTAL RESULTS

The evolution in crypto-currency based payment systems enabled us to solve the reputation management problem experienced during the P2P era. The proposed model uses a centralized crypto-currency called *TelCash*, payment system for the resource sharing and utilization among the devices. In this study, *TelCash* is handled by a third party system who is responsible for managing the payment system to be used in D2D communication and resource sharing. The crypto-credit of each device is stored as its *TelCash*.

During the media data transmission an appropriate amount of credit through *TelCash* system is transferred. The simplicity to employ reputation management/payment system is due to the introduction of a blockchain based payment control system. In this section we evaluate the performance of the proposed system experimentally. Our evaluations are based on the following assumptions:

- The proposed D2D media data sharing system imposes some overhead to the network. An important criteria should be the amount of the overhead imposed in terms of the number of extra bytes sent, and the amount of energy used.
- As the direct connection between the devices is not always available, the devices with direct connectivity are grouped in a cluster. Therefore the communication can be either in the cluster, which requires less energy, or between clusters that spends more energy. It should be noted that between cluster communications are possible if a device is connected to both clusters and behaves as an intermediate node for inter-cluster communications.
- Media file can be shared through access points when the nodes are in different networks.

- And finally, the data can be provided from CDN, which imposes the highest cost on the network.

In addition, since the proposed method assumes that the super nodes process the transactions, the transaction processing will impose an extra load on the super node. We consider the analysis of the extra load as part of the evaluation of the proposed network.

Finally, an important consideration in resource sharing networks is the selfishness of the nodes. If the member nodes avoid sharing their resources, the system will fail. The proposed method considers two measurements to overcome this problem. The first measurement is providing incentives in terms of *TelCash* credits. The second measurement is a punishment mechanism which adds extra charges to media data downloading when the node has not been available during the past time. An analysis of these measurements is also considered in our experimental results. Table 1 shows the parameters used in our simulation.

Table 1 The Parameters used in the Simulations

Parameter	Parameter Value
LTE Radius	500 meters
Cluster Radius	50 meters
Number of Users	100
Average Number of Users in Clusters	100
E_T x + E_Rx	50 nj/bit
ε_{amp}	100 pj/bit/m^2
E_T ranscode	48 nj/bit

4.1 Cost of Accessing Media Files

In this part of experiment, the cost of accessing video is calculated. The credit to access smallest speed GoP (100 Kbps quality for 2 seconds) is assumed to be 1 credit if it is accessed within the same cluster. This amount is increased to 2 when accessing to another cluster, to 3 when the node having the file is within another network and is reached through the access point, and finally 5 to access a GoP within cache or CDN servers. Table 2 depicts the amount of credits paid for communication in different scenarios for both data transfer and transcoding (edge computing) usage. Those credits are calculated by considering the energy consumption of the devices when transferring the data in order to allow the nodes sharing data to earn money. Obviously, the less the energy consumption is, the cheaper the price is.

The experiments are run 10 times and the average of the results are calculated and presented during this study otherwise stated. The first row of Tables 2, 3 and 4 contains the maximum credits to be paid for streaming the whole video.

Table 2 Total TelCash Credits Paid for in Different Data Rates and Scenarios.

Availability\Rate	100Kbps	200Kbps	400Kbps	800Kbps
Cache/CDN	500	1000	2000	4000
1%	360	784	1755	3807
2%	290	673	1564	3580
3%	252	593	1384	3418
4%	234	522	1256	3323

Table 3 TelCash Credits Paid for Transcoding in Different Data Rates and Scenarios.

Availability\Rate	100Kbps	200Kbps	400Kbps	800Kbps
Cache/CDN	300	400	400	0
1%	44	57	31	0
2%	57	89	55	0
3%	54	87	77	0
4%	59	87	82	0

Table 3 depicts the amount of TelCash credits paid for transcoding of the video chunks into lower layer qualities. It is obvious that there is no higher quality video than 800 Kbps hence the rightmost column presenting the values for transcoding from any higher value to 800 Kbps is all 0. The While TelCash credit usage is decreasing when the existence probability of a GoP increases, it increases in the transcoding credits since the number of total GoP used after transcoding increased.

Table 4 TelCash Credits Paid for Data Sharing in Different Rates and Scenarios.

Availability\Rate	100Kbps	200Kbps	400Kbps	800Kbps
Cache/CDN	500	1000	2000	4000
1%	316	727	1724	3807
2%	233	583	1510	3580
3%	198	506	1387	3418
4%	175	435	1174	3323

Table 4 depicts the amount of TelCash credits paid for transferring of the video chunks into to the player account. Since the probability of locating a GoP in a device nearby of the player device, the cost of streaming the whole video decreases clearly.

4.2 Energy Consumptions

Since the energy consumption in direct D2D media file sharing is dependent on the results of a search process to locate the files, we evaluate the proposed method by measuring the amount of energy spent in different case of search scenarios. The scenarios assume the search is in terms of media file segments (GoP). In these scenarios the probability of locating a GoP is varied from 1% to 4%. The requested video has a length of 200 seconds and is delivered with different connection rates. The results of this experiment have been shown in Table 5.

Table 5 Energy Consumption for a Video Request with Varying Data Rates, and Variable Probability of Availability

Availability\Rate	100Kbps	200Kbps	400Kbps	800Kbps
Cache/CDN	400 J	800 J	1600 J	3200 J
1%	214.87 J	527.23 J	1331.11 J	3034.05 J
2%	125.49 J	371.01 J	1105.99 J	2803.80 J
3%	85.87 J	290.61 J	887.27 J	2627.10 J

4%	63.33 J	210.93 J	743.63 J	2531.35 J

The transaction between devices and the system has been logged and the payment among the systems are allowed according to the proposed simulation scenario. Although, the *TelCash* management platform is designed centrally for this simulation, it should use distributed ledger platforms to enable multiple operators. It should be open for all Internet users and telecommuters in order to solve roaming and scalability problems. As it can be seen from the Table 5 the cost of play-out decreases when the success ratio of finding a chunk within device overlay increases. On the other hand, the decrease in the cost is not in the same magnitude with the power consumption decrease. Even more interestingly, the cost of playing higher bandwidth increases much faster than the rate of quality increase in bits per second. This can be attributed to the limited contribution of the devices in the overlay network when the demand for higher quality increases as well as the price of the delivery service through centralized systems. The savings in the cost can reach up to 40% cheaper when the system is utilized intensively.

4.3 Fairness and Selfishness Analysis

The credit computation considers the availability rate of the nodes as one of the parameters in determining the amount of payments. The availability of a node changes with two affecting factors: either the node is not reachable due to the displacement of the device from other nodes, or the node is unavailable as the result of such a preference by the users. Although the incentive changes due to availability change is a user-dependent parameter, an empirical evaluation reveals that increase in payment should be proportional to the inverse square of availability during the past hour as shown in Equation 4.1

$$P = \partial \frac{1}{T^2} \qquad 4.1$$

Equation 4.1 requires lower payment for utilizing the network resources from a node, which has been available for a period of T during past hour. P is included in payment computation together with other parameters.

4.4 Processing Overhead in Super Node

Processing overhead in the proposed model is quite negligible. This is due to the fact the telecommunication networks. which are connected and managed by a single base station include a limited number of nodes and the number of messages exchanged to establish a connection and process a transaction.

4.5 Tracking the Earnings of the Nodes

In order to analyze the credit earnings of the nodes, experiments with 100 nodes have been carried out. The experiments include 1% through 4% probability of finding a media file in a node, with 100Kbps and 400Kbps data rates. The results of the experiments have been given in Figures 17 and 18.

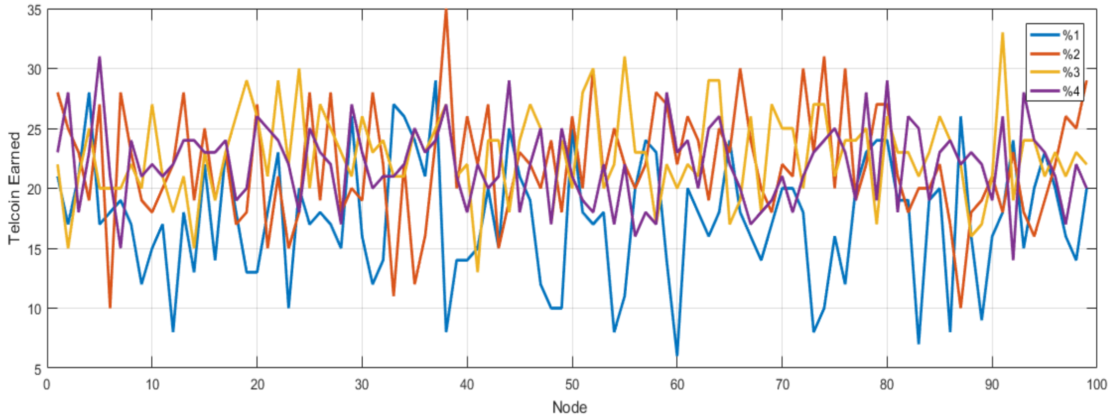

Figure 17 TelCash Earned by 100 Nodes with Different Data Availabilities

As it can be seen from Figures 17 and 18, with increased probability of having a media data file the distribution of the TelCash becomes more uniform. This indicates that the system has a relatively fair approach in giving incentive credits when the number of data files and their availability increases.

With increased data rates, the total time to transmit media files, and hence the resource allocation period decreases. This decrease results in earning less credits as shown in Figure 18.

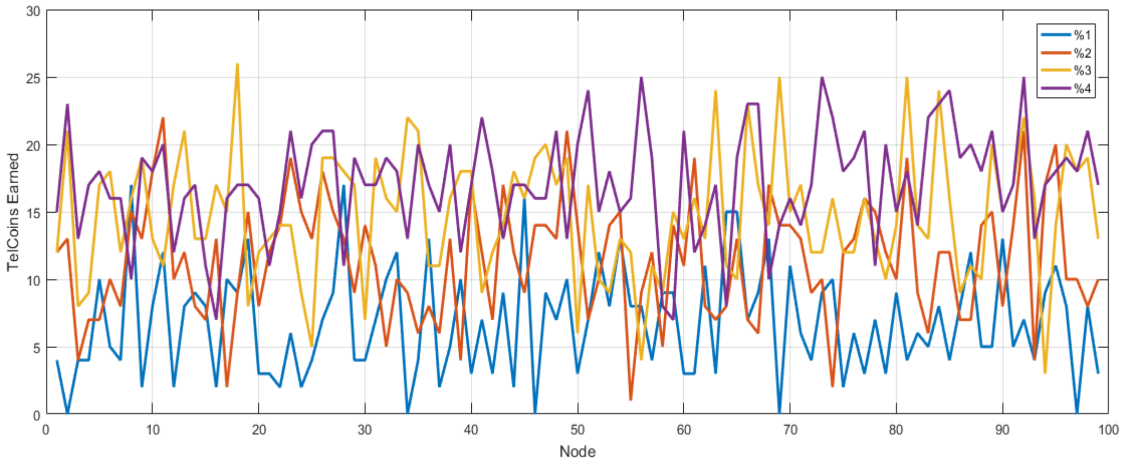

Figure 18 TelCash Earned by 100 Nodes with Different Data Availabilities

CHAPTER 5

CONCLUSIONS

In this thesis a blockchain incentive payment method has been proposed to encourage D2D resource sharing. The main goal of the proposed method is providing the possibility of media data sharing through direct communications between devices. The proposed system addressed several problems and provides potential solutions for them. The most important problem addressed is building a architecture with the capability of solving *Roaming* problem in telecommunication systems. The proposed *TelCash* credit can be used for payment to foreign operators when subscribers are roaming. This also needs a software based SIM cards for the mobile devices in order to bring the ability to configure the systems dynamically. Soft SIM cards are widely in use for IoT systems and migration to them have already started.

During the peer-to-peer (P2P) technology evolution over time [27], there was a need for a mechanism to manage the Trust Relationship during the second decade of P2P evolution where the systems became fully distributed without centralized control. At that point, it was almost impossible to build a trustful data exchange, and reputation management systems. The lack of such systems limited the rise of P2P networks. In contrast to past decade, Blockchain Technology enabled us to perform trustless transactions where no parties need to know nor trust each other for transactions, which completely solves the trust and reputation management problems.

Besides, our experimental results indicate that the proposed system has the capability of reducing network traffic load by replacing it to direct communications between nodes at the edge. These results prove the potential of the proposed method to be used in telecommunication systems.

Our proposed method has also the capability of sharing the processing load of edge level devices and providing cloud based applications the possibility of working in near real-time. Although we implemented the processing power sharing for transcoding the media files, the proposed model is readily applicable to any application requiring distributed processing.

For future studies, the details of the *TelCash* system should be presented with all architectural details as well as re-organizing the architecture in all mobile systems in order to achieve the best service available by the infrastructure.

The second proposal is a solution to motivate the content holder devices by allowing them to accumulate a specific block chain based crypto currency credits in order to use the resources owned by someone else. This mechanism will build a solid ground to introduce a crypto currency mechanism called *TelCash* in order to use it universally by all telecommunication operators and users as an exchange platform to solve data exchange and roaming problems.

In addition, the proposed payment model can be implemented in totally decentralized form. The current structure requires the super node to process the transactions and validate incentive payments. In a decentralized system, the payments should be automatic without any interference form a third party. The main challenge in that case is the willingness of the nodes to pay after receiving services, and the controversies arising thereafter.

REFERRENCES

1. Automotive, Available online at https://in.reuters.com/article/us-autos-blockchain/blockchain-technology-moves-into-car-sharing-mobility-services-idINKCN1BA1PH
2. Baur, A.W., Bühler, J., Bick, M. and Bonorden, C.S., 2015, October. Cryptocurrencies as a disruption? empirical findings on user adoption and future potential of bitcoin and co. In Conference on e-Business, e-Services and e-Society (pp. 63-80). Springer, Cham.
3. Bradbury, D., 2013. Bitcoin's successors: from Litecoin to Freicoin and onwards. The Guardian, 25.
4. Conoscenti, M., Vetro, A. and De Martin, J.C., 2016, November. Blockchain for the Internet of Things: A systematic literature review. In Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of (pp. 1-6). IEEE.
5. Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V., 2016. Blockchain technology: Beyond bitcoin. Applied Innovation, 2, pp.6-10.
6. Energy: "Bitcoin energy consumption index." Available online at https://digiconomist.net/bitcoin-energy-consumption
7. Eyal, I. and Sirer, E.G., 2018. Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 61(7), pp.95-102.
8. Gencer, A.E., Basu, S., Eyal, I., van Renesse, R. and Sirer, E.G., 2018. Decentralization in bitcoin and ethereum networks. arXiv preprint arXiv:1801.03998.
9. Gionis, A., Indyk, P. and Motwani, R., 1999, September. Similarity search in high dimensions via hashing. In Vldb (Vol. 99, No. 6, pp. 518-529).
10. Hedera, Online resource available at https://www.hederahashgraph.com/platform
11. Hu, Y.C., Patel, M., Sabella, D., Sprecher, N. and Young, V., 2015. Mobile edge computing-A key technology towards 5G. ETSI white paper, 11(11), pp.1-16.
12. Hyperledger, Online resources available at https://www.hyperledger.org/
13. Iansiti, M. and Lakhani, K.R., 2017. The truth about blockchain. Harvard Business Review, 95(1), pp.118-127.
14. IoA, available online at https://www.coinspeaker.com/2017/11/11/internet-assets-financial-market-evolution/
15. Jacobovitz, O., 2016. Blockchain for identity management. The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva Google Scholar.
16. Kerner L., 2018, Is The Future Of Blockchains DAGs?, accessed online from https://medium.com/crypto-oracle/is-the-future-of-blockchains-dags-5-lessons-from-the-hashgraph-event-in-nyc-on-march-13th-ff0f7e0fa510.

17. King, S. and Nadal, S., 2012. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19.
18. Korpela, K., Hallikas, J. and Dahlberg, T., 2017, January. Digital supply chain transformation toward blockchain integration. In proceedings of the 50th Hawaii international conference on system sciences.
19. Kumar, K.; Liu, J.; Lu, Y.H.; Bhargava, B. 2013, A Survey of Computation Offloading for Mobile Systems. Mobile Network Applications, 18, doi:10.1007/s11036-012-0368-0.
20. LeMahieu, C., 2018. Nano: A Feeless Distributed Cryptocurrency Network. nano. org. Accessed on May, 3.
21. LiteCoin, available online at https://litecoin.org/
22. Merkle, R. C. (1988). "A Digital Signature Based on a Conventional Encryption Function". Advances in Cryptology-CRYPTO '87. Lecture Notes in Computer Science. 293. p. 369.
23. Mettler, M., 2016, September. Blockchain technology in healthcare: The revolution starts here. In e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on (pp. 1-3). IEEE.
24. Moura, T. and Gomes, A., 2017, June. Blockchain Voting and its effects on Election Transparency and Voter Confidence. In Proceedings of the 18th Annual International Conference on Digital Government Research (pp. 574-575). ACM.
25. Nakamoto S. 2009, Bitcoin: a peer-to-peer electronic cash system [Online], available: https://bitcoin.org/bitcoin.pdf
26. Omohundro, S., 2014. Cryptocurrencies, smart contracts, and artificial intelligence. AI matters, 1(2), pp.19-21.
27. Oztoprak, K. and Akar, G. B. 2008. Hybrid fault tolerant peer to peer video streaming architecture, IEICE transactions on communications, 91, 11, pp: 3627-3638, 2008.
28. Peters, G.W. and Panayi, E., 2016. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In Banking Beyond Banks and Money (pp. 239-278). Springer, Cham.
29. Rosenfeld, M., 2011, Analysis of bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980.
30. Samaniego, M. and Deters, R., 2016, December. Blockchain as a Service for IoT. In Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on (pp. 433-436). IEEE.
31. Sörensen, K., and Janssens, G. K., 2005. An algorithm to generate ll spanning trees of a graph in order of increasing cost, Pesquisa Operational 25(2), pp. 219-229

32. TelCoin Whitepaper v1.3, September 2018. Available online at https://www.telco.in/whitepaper.pdf
33. Underwood, S., 2016. Blockchain beyond bitcoin. Communications of the ACM, 59(11), pp.15-17.
34. Wang, L., 2013. Directed acyclic graph. In Encyclopedia of Systems Biology (pp. 574-574). Springer, New York, NY.
35. Wood, G., 2014. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151, pp.1-32.
36. Wu, X.;Wang,W.; Lin, B.; Miao, K. Composable IO: 2012, A novel resource sharing platform in personal Clouds. J. Supercomput. 61, doi:10.1007/s11227-011-0663-8.
37. Xia, F., Yang, L.T., Wang, L. and Vinel, A., 2012. Internet of things. International Journal of Communication Systems, 25(9), pp.1101-1102.
38. Zyskind, G. and Nathan, O., 2015, May. Decentralizing privacy: Using blockchain to protect personal data. In Security and Privacy Workshops (SPW), 2015 IEEE (pp. 180-184). IEEE.