ISTANBUL TECHNICAL UNIVERSITY ★ INFORMATICS INSTITUTE

SECURE VIDEO STREAMING USING BLOCKCHAIN TECHNOLOGY FOR MOBILE DEVICES

M.Sc. THESIS

Nasim TAVAKKOLI

Department of Applied Informatics

Cybersecurity Engineering and Cryptography Programme

DECEMBER 2019

ISTANBUL TECHNICAL UNIVERSITY ★ INFORMATICS INSTITUTE

SECURE VIDEO STREAMING USING BLOCKCHAIN TECHNOLOGY FOR MOBILE DEVICES

M.Sc. THESIS

Nasim TAVAKKOLI
(707161008)

Department of Applied Informatics

Cybersecurity Engineering and Cryptography Programme

Thesis Advisor: Assoc. Prof. Dr. Enver ÖZDEMİR

DECEMBER 2019

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

MOBİL CİHAZLARINDA BLOKZİNCİR TEKNOLOJİSİ KULLANARAK GÜVENİLİR VİDEO AKIŞI

YÜKSEK LİSANS TEZİ

Nasim TAVAKKOLI
(707161008)

BİLİŞİM UYGULAMALARI ANABİLİM DALI

Bilgi Güvenliği Mühendisliği ve Kriptografi Programı

Tez Danışmanı: Assoc. Prof. Dr. Enver ÖZDEMİR

ARALIK 2019

Nasim TAVAKKOLI, a M.Sc. student of ITU Informatics Institute Engineering and Technology 707161008 successfully defended the thesis entitled "SECURE VIDEO STREAMING USING BLOCKCHAIN TECHNOLOGY FOR MOBILE DEVICES", which he/she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor :	**Assoc. Prof. Dr. Enver ÖZDEMİR** Istanbul Technical University	.....
Jury Members :	**Dr.Öğr.Üyesi Mehmet Akif YAZICI** Istanbul Technical University	.....
	Dr. Deniz SARIER TÜBİTAK	.....
		.....

Date of Submission : **15 November 2019**
Date of Defense : **13 December 2019**

To my mother and father,

FOREWORD

This thesis is dedicated to my family and specially my mother, for her endless love, support and encouragement throughout all stages of my life.

I would be glad to express my sincere gratitude to my precious advisor Assoc. Prof. Enver ÖZDEMİR for the continuous support of my master work. He always motivates me in solving my research problems. His guidance helped me in all the time of research and writing of my thesis.

“This work is supported in part by Istanbul Technical University (ITU) Vodafone Future Lab under Project No. ITUVF20190601P01.”

DECEMBER 2019 Nasim TAVAKKOLI

TABLE OF CONTENTS

Page

ABBREVIATIONS

WiFi	**:** Wireless Fidelity
4G	**:** 4th Generation
HD	**:** High Definition
UHD	**:** Ultra High Definition
5G	**:** 5th Generation
P2P	**:** Peer to Peer
PoW	**:** Proof of Work
PoA	**:** Proof of Authority
PoS	**:** Proof of Stake
DPoS	**:** Delegated Proof of Stake
PBFT	**:** Practical Byzantine Fault Tolerance
DDos	**:** Distributed Denial of service
IP	**:** Internet Protocol
VPN	**:** Virtual Private Network
D2D	**:** Device to Device
VoD	**:** Video on Demand
TPS	**:** Transactions Per Second

SYMBOLS

$\mathbf{P_x}$	**:** *x*th packet
$\mathbf{H(p_x)}$	**:** Hash of *x*th packet

LIST OF TABLES

Page

LIST OF FIGURES

Page

SECURE VIDEO STREAMING USING BLOCKCHAIN TECHNOLOGY FOR MOBILE DEVICES

SUMMARY

The data transfered to mobile device users compromise the majority of data streaming through internet and the high proportion of this data consists of video content. Mobile users' demand on high quality and fast video streaming lead researchers to seek new protocols and algorithms beyond the traditional methods on the subject. Caching and cooperative video streaming found its way to be a popular method in the wireless communication community amid this demand. Several improvement has been presented since the method's first appearance. On the other hand, due to the sole aim of providing fast data streaming to users, the security perspective of the methods were missed most of the time. Recent application of Blockchain to cryptocurrency Bitcoin has established this method a suitable alternative to various applications. In this thesis, Blockchain method is employed to alleviate security concerns of fast video streaming methods. The method describes how to attach Blockchain to current fast data transferring methods which exploit caching/distributing techniques in order to prevent malicious intrusions.

MOBİL CİHAZLARINDA BLOKZİNCİR TEKNOLOJİSİ KULLANARAK GÜVENİLİR VİDEO AKIŞI

ÖZET

Mobil cihaz kullanıcılarına aktarılan veriler, internet üzerinden veri akışının çoğunu tehlikeye atar ve bu verilerin yüksek bir kısmı video içeriğinden oluşur. Mobil kullanıcıların yüksek kaliteli ve hızlı video akışı talep etmesi, araştırmacıların konuyla ilgili geleneksel yöntemlerin ötesinde yeni protokoller ve algoritmalar aramasına neden olmuştur. Önbelleğe alma ve işbirliğine dayalı video akışı, bu talebin ortasında kablosuz iletişim topluluğunda popüler bir yöntem olma yolunu buldu. Önbelleğe alma yönteminin ilk görünümünden bu yana birçok gelişme sağlanmıştır. Öte yandan, sunulan yöntemlerin sadece kullanıcılara hızlı veri akışı sağlamaya odaklandığı için, genelde yöntemlerin güvenlik perspektifi göz önünde bulundurulmamıştır. Blockchain'in şifreli para birimine son uygulaması Bitcoin, bu yöntemi çeşitli uygulamalara uygun bir alternatif olarak belirlemiştir. Bu tezde, hızlı video akışı yöntemlerinin güvenlik kaygılarını hafifletmek için Blockchain yöntemi kullanılmıştır. Yöntem, Blockchain'in hızlı veri aktarma yöntemlerine, zararlı izinsiz girişleri önlemek için önbellekleme / dağıtma tekniklerinden yararlanan yöntemlere nasıl bağlanacağını açıklar.

Ağ teknolojisinin son zamanlardaki ilerlemesi ve dijital içerik endüstrisinin hızlı büyümesi, multimedya hizmetlerini, özellikle video akış hizmetlerini, aboneler arasında giderek daha popüler hale getirmektedir. Video akışı uygulamalarının çoğu, videoyu bir kaynak sunucudan kullanıcıların büyük bir nüfusuna dağıtmayı içerir. İstemci-sunucu modeli, makul sayıda kullanıcıyla iyi çalışır. Bu nedenle flaş kalabalıkları video sunucusunu kolayca çökertebilir ve bu durum ölçeklenebilirlik sorunuyla sonuçlanır. Ayrıca kullanıcı tarafında ise değişik faktörler WiFi veya 4G bağlantısının video akışındaki sağladığı hızı etkileyebilir. Bu tür problemleri önlemek adına P2P teknolojisi, video akışı uygulamaları için popüler bir çözüm haline gelmiştir. P2P ağlarında, bir istemci sunucudan veya eş düğümlerden paketleri indiren bir alıcı görevi görürken aynı zamanda indirilen paketleri diğer eş düğümlere dağıtan bir tedarikçidir. Bu şekilde, eş düğümlerin bant genişliğinin ağa yüklenmesi verimli bir şekilde kullanılır ve sunucunun yükü hafifletilir. Alıcı eşler aynı zamanda diğer eşler için potansiyel göndericiler olduğundan, ağa katıldıkça sistem kapasitesi artar ve bu da ölçeklenebilirlik sorununu daha düşük maliyetli bir şekilde çözer. P2P teknolojisi üzerinden önbellek paylaşımı yapan uygulamalar video akışı için uygun bir çözüm sunsa da, güvenli değildir ve DDos, kötü amaçlı yazılım, virüs ve bant genişliği daraltma gibi siber saldırılara karşı savunmasızdır.

Mevcut P2P video akışı uygulamalarında kötü niyetli paket dağıtımını önlemek adına ağ üzerinden birbirine bağlanan düğümlerin birbirini tanıması ve güvenmesi şart. Ancak ağ'a bağlanmak isteyen cihazların sayısı artınca bunu sağlamak pek mümkün değil, veya bittorrent yöntemiyle video akışı yapan uygulamalarda, P2P ağına

bağlanan cihazlar kötü niyetli paket almamak için IP adreslerini VPN kullanarak diğer düğümlerden gizlemek zorundalar, ancak VPN kullanmak güvenli paket dağıtımını sağlamak için yeterli değildir. Bazı VPN'ler düşük dereceli şifrelemele yöntemleri kullandıkrarı nedeniyle güvenliği tamamen sağlamayabilirler. Ayrıca genellikle bant genişliği ve hız sınırlamalarına neden olurlar veya P2P trafiğine izin vermezler.

P2P ağ üzerinden eş düğümler arasında dağıtılan paketlerin içeriği kontrol edilmediği için bu paketler zararlı yazılım içerebilir. Bahsedilen güvenlik açığını kapatmak için Blok zincir teknolojisi kullanılarak yeni bir sistem tasarlamış bulunuyoruz. Bu tezde öneliren yöntemde yeni sistemde P2P ağına bağlanan düğümlerin kimliği doğrulanıyor ve aynı zamanda dağıtılan video paketlerinin içeriği kontrol ediliyor. Böylece kötücül düğümler ve paketler ağ içeresinde işlem yapamıyor ve P2P ağ üzerinden yapılan video akışının güvenliği sağlanıyor.

Sunulan yöntemde, aynı bölgedeki cep telefonu kullanıcıları için güvenli bir akış deneyimi sağlayan bir video akış yöntemi tasarlanmıştır. Sistem, mobil cihazların birbirine bağlanabileceği ve canlı akış sırasında ara belleğe alınmış verilerini P2P ağı üzerinden paylaşabileceği bir P2P ağı kurar. Bir ağın parçası olan aygıtların, kötü niyetli bir aygıttan kötü amaçlı paket almasını önlemek için paket alışverişi sırasında birbirlerine güvenmeleri gerekir. Önerilen yöntemde ağ güvenliğini ve bir kimlik doğrulama yöntemi sağlamak için Blok zincir teknolojisini kullanılıyor. Cihazlar arasında paket aktarımı sırasında hız önemli bir faktör olduğundan tasarlanan yöntemde Private Blockchain kullanılmaktadır.

Sunucudan indirilen her video paketi, ağ üzerindeki cihazlara (düğümlere) aktarılmadan önce, zincirdeki doğrulama düğümleri tarafından onaylanması gerekir, bu nedenle zincire kötü amaçlı paketler eklenmez. Her bir düğüm ağa katıldığında, ağdaki diğer düğümlerden blockchain verilerinin güncel halini alır. Blockchain verileri, video akışı sırasında ağdaki her düğüm tarafından indirilen paketlerin Hash değerini içerir. Ayrıca, her düğümün indirdiği paketlerin sayısını ve gönderen / alıcı düğümlerini ve video segmentlerinin bilgilerini içeren bir liste içerir.

Böylece düğümler listeye göre videonun her bir segmenti için diğer düğümlere istek gönderir. İsteği alan düğümler istenen paketleri P2P ağ üzerinden cihazlara gönderir. Daha sonra, her cihaz alınan paketlerin Hash değerini hesaplar ve zincirdeki ilgili paketin Hash değerile karşılaştırır. İki Hash değeri eşit olduğu sürece, cihaz kötü niyetli yazılım içermeyen doğru paketi aldığından emin olur.

Ağ üzerindeki düğümler sunucudan indirdikleri video paketlerinin Hash değerini yeni bir blok olarak zincire eklemek istediklerinde ise doğrulama düğümleri bloğun zincire eklenip eklenemeyeceğine karar verir.

Sonuç olarak, video paketleri doğrulayıcı düğümler tarafından doğrulanarak kötü niyetli paketlerin ağ üzerinden dağıtımı engellenecektir.

Önerilen yöntem, ilk canlı video akışı ve ikinci istek üzerine video olmak üzere iki açıdan tartışılabilir. Cihazlar, canlı etkinlikte önbelleğe dayalı güvenli bir P2P ağı arasında paylaşır. Sonuç olarak, ağ canlı akışın başlangıcından itibaren yayınlanan tüm segmentleri ve bunların Hash değerlerini içerir. Bu nedenle, bir cihaz başlangıçta değil canlı akışın ortasında bile P2P ağına katıldığında, diğer düğümlerden önceki segmentleri güvenli bir ağ üzerinden alabilir. Önerilen çerçevenin değerlendirilmesi, Blockchain teknolojisini kullanarak P2P video akışı yöntemlerinin güvenlik sorunlarını ortadan kaldırmaktadır. Aslında önerilen yöntem, hem canlı hem

de VoD akışında hücresel veri kullanımını azaltırken mobil cihazlar için video akışının hızını ve kalitesini artıran blockchain teknolojisine dayanan güvenli bir P2P ağı sağlar.

Çalışma, verilerin arabelleğe alınmasını kullanan ve önbelleğe alınmış paketleri dağıtan yüksek oranda kabul edilmiş kooperatif video akışı yöntemlerine bir ek sunuyor. Bu eklenti, bu tür hızlı video akışı çerçevelerinin güvenlik ve gizlilik endişelerini gidermek içindir. Blockchain'in ekonomiden sağlık sektörlerine kadar çok sayıda uygulamaya uygulanabilirliği, önerilen yöntemde kullanılmaktadır. Çerçevemiz P2P video akışındaki güvenlik endişelerini azaltmış olsa da, gelecekteki çalışmalarda üst düzey güven için ek değerlendirmeler ve önlemler yapılacaktır.

1. INTRODUCTION

Video streaming is continuously enlarging by the day, however a lot of elements are affecting its growth. As social platforms become more and more video-focused, the number of people who prefer watching videos instead of reading a content increases. Therefore, video contents get shared more than texts and photos by users. As a result, great proportion of audio/video content is displaced with streaming and video became as a key to ideal social media marketing. Between 2015 and 2018, social media advertisements expenditure has continuously increased yearly. We've seen video ads frequently on YouTube, Facebook, Instagram or during watching movies or series on any other platforms. Actually, they are basically everywhere. Moreover, YouTube reports that more than 70% of YouTube video watchtime comprised of mobile devices [1]. Users spend more time watching videos on their phones than any other device and 80% of global connections will be smartphones by 2025 [2]. Watching Tv on mobile devices have become a habit and Netflix is even testing mobile-only tariff plans. Despite the rise of internet-based video streaming services, complying with the requests for high-quality video is challenging.

Several key factors can affect the speed provided by a WiFi or 4G connection. Number of Hot-spots or Cell towers to provide a good coverage, number of devices which are connected to the same Hot-spots or Cell towers and obstacles like buildings or other wireless devices can have an effect on the speed of wireless connection. Based on the recent Open Signal study, in 33 countries smartphone users now experience faster average download speeds using a mobile network than using WiFi [3]. In order to have high-quality streaming like HD, UHD or 4K, most of the time we need to use ethernet cable because routers give priority to hard-line connections and create more interference for other devices connected via WiFi. On the other hand, on a 4G network, stream videos can be on the highest settings like 1080P without any problems. Despite these, due to mobile operators WiFi strategies, smart phones will automatically switch from an expensive cellular connection to a known lower-cost-per-bit WiFi network

and small-cell access ignoring speed as a factor in their decision [3]. According to the Cisco Mobile Visual Networking Index Forecast [4], the amount of traffic offloaded from smartphones will increase from 57% in 2017 to 59% by 2022. Moreover, different cellular providers offer greater 4G coverage than others depending on the location and different models of smart phones pick up cell signals better than others. Consequently, users with different devices and cellular providers could have low/high quality video experiences.

The problem is that access to the internet is not enough, as phones become more accessible and the number of people start to use them is increasing. This is due to the fact that the infrastructure is high-priced. Even 5G cellular network technology would not be solution for these problem despite of its coverage, capability and limited bandwidth problems, as the financial aspects of expanding 5G have not resolved completely yet, and will be presumably a slow implementation in most of targeted areas where it is economically sensible.

1.1 Purpose of Thesis

This thesis presents a new method for fast and secure video streaming in mobile devices, in order to overcome cellular data usage and video streaming quality problems of smart phone users. Provided approach employs Blockchain technology to create a decentralized network where all devices can connect to each other directly. The blockchain technology allows devices to exchange data between each other through a Peer-to-Peer network without requiring a server or cloud. Moreover blockchain provides security in data transmission in comparison with other Peer-to-Peer methods.

In this method all smart phone users who can perform Peer-to-Peer (P2P) networking, can connect to each other through a secure private Blockchain network and watch the same video on their mobile phones at the same time via sharing their cache data. Users will distribute their downloaded cache through a reliable P2P network, which results in a high quality and fast video streaming experience with minimum mobile data usage.

1.2 Applied Technology Review

1.2.1 Blockchain technology

Blockchain is the technology behind Bitcoin [5], a Peer-to-Peer electronic cash system, which was introduced in 2008 by an anonymous person or a group under the name of Satoshi Nakamoto. Actually, Blockchain is a public distributed database holding a continuously growing list of records and has been executed and shared among participating parties. Participants can trust each other and perform transactions in a large peer-to-peer networks without of a centralized management. Trust is established by protocols, cryptography and computer codes. Each transaction is placed in groups called blocks. These blocks are chained to each other utilizing cryptographic hash function. Each block contains the hash of its own data along with the hash of previous block's data. This makes Blockchain practically immutable since changing a single block requires updating all previous blocks which is almost infeasible. The chained blocks are stored in network members' devices called nodes. Nodes can be any kind of devices such as computers, laptops, mobiles or large servers.

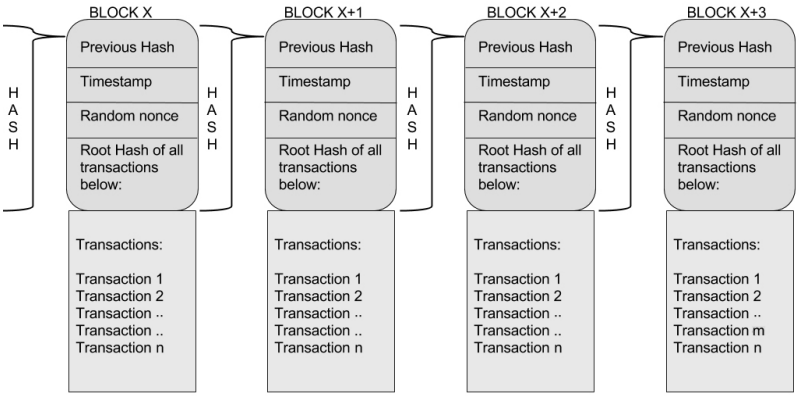

Figure 1.1 : Blockchain block structure.

Nodes of a blockchain are connected to each other through a Peer-to-Peer network and exchange the latest transactions stored in Blockchain. Actually, each node contains a copy of the chained blocks and when a new transaction takes place in Blockchain, it is shared among all nodes. In the case of adding a new block to the chain, based on consensus mechanism [6] of Blockchain, the nodes among network can decide which block is verified to be added and contains valid information. Once the verified block is

added to the chain it is distributed among all nodes on the network. Other nodes accept the new block and save it in the transaction data while all transactions within the block can be performed based on the history of the blockchain.

Blockchain technology allows people to communicate directly through a P2P network. Voice and video calls, emails, pictures and instant messages travel directly from A to B, maintaining trust between individuals no mater how far apart they are. By employing math and cryptography blockchain technology provides a boundless public ledger where once a data added to the chain, it is pretty much impossible to change that data. This makes blockchain partially an immutable Peer-to-Peer network. The uses of blockchain technology are endless even though, Blockchain first raised with a cryptocurrency in the literature, other assets could also be recorded publicly and sequentially through a blockchain network. Actually blockchain provides an open decentralized database of every transactions involving value such as money, goods, property, work or even votes.

1.2.2 Blockchain classification

Considering blockchain as a virtual ledger, this technology can be used in different areas not just in a cryptocurrency. On the other hand, utilizing a fully public Blockchain might not be efficient always. Blockchain technology is classified in three genres as Public Blockchain, Private Blockchain and Consortium Blockchain [7, Ethereum Blog].

1.2.2.1 Public blockchain

Public Blockchain could be termed as permission-less blockchain while any device from any where can join to the public blockchain network. Bitcoin is a cryptocurrency backed by public blockchain, which guarantees anonymity in identity yet transparency in transactions. Nevertheless, preserving anonymity and transactional transparency in parallel is costly, it decreases the bandwidth among nodes and whole blockchain have to be duplicated by the entire nodes at the local level in order to be aware of the latest status of the chain. This results in the slow transaction processing. Proof of Work (PoW) consensus protocol is mostly used for confirming transactions in a public Blockchain similar to Bitcoin [5].

Table 1.1 : Differences between public and private blockchain.

	Public Blockchain	Private Blockchain
Access Level	Anyone	Authorized Users
Participation	Anonymous	Identities are Known
Security	PoW, PoS	PoA, Pre-approved nodes
Performance	Slow transaction Speed	Lighter Blockchain, Fast Transaction speed

1.2.2.2 Private blockchain

A Private Blockchain is known as a permissioned Blockchain while only allowed devices can join to the network. Private blockchain doesn't provide anonymity in identity as public blockchain, but transactions are transparent. The difference is that only the nodes whom identity is authenticated are allowed to write data to the blockchain. As the nodes are distributed locally, as well as much fewer nodes take part in the ledger, the performance is more faster in compare with public blockchain.

Though Private Blockchain does not guarantee immutability as much as public Blockchain [6], it is faster as it uses different consensus protocols like Proof of Authority (PoA) with low requirement of computational power than PoW.

1.2.2.3 Consortium blockchain

A Consortium blockchain is somewhat like private blockchain. It provides efficiency and transaction privacy like the private one but it doesn't consolidate authority by one node. Transactions are low-cost and faster as good as possible, because they only are required to be verified by a few nodes which can be trusted to have very high processing power. Consequently, some of nodes in the network and not the entire network validate the new blocks. Briefly, while private blockchains might not be the appropriate option for establishing a worldwide cryptocurrency which is unidentified and untrustworthy, on the other hand they can be applied in practical applications, including industry specific IoT applications.

1.2.3 Consensus protocols

Consensus mechanism is set of rules which develops an incontrovertible contract system over Blockchain. Basically, consensus protocols keep all the nodes on a network synchronized and make them trust each other. Once nodes on the network want to validate a new block, they have to guarantee if the corresponding block follows the consensus rules. Actually the security of the chain is provided by consensus protocol. Proof of Work protocol, which is adopted by Bitcoin, is the most commonly utilized consensus protocol in public blockchains. Based on PoW algorithm, a miner must solve a cryptographic hard puzzle in order to add a new block to the chain. All nodes in the network will take a part in validating the new block, which makes the Proof of Work a time consuming process.

There are various consensus protocols whose rules differ depending on validation of blocks in Blockchain.

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Delegated Proof of Stake (DPoS)
- Practical Byzantine Fault Tolerance (PBFT)
- Proof of Authority (PoA)

2. RELATED WORKS

2.1 Peer-to-Peer Video Streaming

Accustomed client-server based video streaming solutions cost expensive bandwidth provisioning on the server [8]. P2P networking is an alternative paradigm to construct distributed network applications. Nowadays P2P streaming systems are preferred in order to provide live and on-demand video streaming services on the Internet at low server cost.

2.1.1 Popcorn time

One of the platforms that deals with video streaming problems is Popcorn Time [9]. It provides a lower bandwidth usage and high quality video steaming through a Peer-to-Peer network. Popcorn Time is a multi-platform streaming service, which utilizes BitTorrent [10] technology, to provide an easy video streaming without downloading the video to devices' memory. Users, which known as seeds, connect to a P2P network and start watching the videos at the same time they are uploading data. In other words, seeds are going to be uploading bits by bits of the movie for as long as they're watching it on Popcorn Time. While Popcorn Time reduces the usage of bandwidth on the provider's side and is easy to use, it isn't secure and is vulnerable to cyber attacks like DDos, malware, viruses and bandwidth throttling. In order to make the P2P connection secure, users have to hide their IP address from others as they connect to BitTorrent swarm. For this purpose, users have to use a good VPN to mask their IP address while using Popcorn Time. Though, some VPNs reduce risk but does not completely eliminate it due to their low-grade encryption. Also they usually come with bandwidth and speed limitations or do not allow P2P traffic.

2.1.2 Flixxo

The other Peer-to-Peer platform for video streaming is Flixxo. In 2016 Flixxo [11] was introduced as a decentralized video streaming platform. Flixxo is similar to Popcorn Time but it is legal and decentralized in addition to employing Blockchain technology. Actually, Flixxo combines BitTorrent [10] and smart contracts to create a legal, decentralized content distribution network. Flixxo creates a P2P network where authors can distribute their own content using Bit Torrent technology and get paid via a cryptocurrency. Flixxo allows true end users to pay a fair price for watching licensed content in a safe platform. Flixxo has it's own cryptocurrency named Flixx. Users who connect to the P2P network can watch the video for the price determined by the owner of the content. There is no advertisement during the videos but watching advertisement is one of the ways that you can earn Flixx. In this way, advertisers pay users and users pay authors using their earned Flixx without a third party involvement. Although this platform is reliable and motivating, it doesn't fully meet users' video requests as YouTube, Netflix or other video streaming platforms over internet. This indicates that users might not find all desired videos in such a platform.

2.1.3 Microcast

MicroCast [12] proposed and implemented a new system, which employs the resources on all smartphones of the group, such as cellular links and WiFi connections in parallel to improve the streaming experience. MicroCast allows users of smart phones, who are within proximity of each other, to watch the same video from internet at the same time. Each mobile phone utilizes its cellular network to download segments of the video from internet and uses WiFi network in order to connect other mobile devices. The devices that are connected to each other, share their downloaded segments through a peer-to-peer network. Consequently, all connected mobile phones will be able to watch the same video from any source in the internet with faster speed and high quality.

As stated in [12], Microcast is designed and implemented for a small number of users up to 6 or 7 whom are assumed know and trust each other. For instance, family members who want to watch the same movie on their phones in a car or a group of classmates who want to watch an educational video on their smart phones from

Table 2.1 : Comparison of the proposed method with previous methods.

Methods	Performance	Participants	Security
Popcorn Time	Fast	Anyone from Anywhere	VPN (not secure)
Flixxo	Slow	Anyone from Anywhere	Public blockchain (secure)
Microcast	Fast	Small group of People	Not Secure
Proposed Method	Fast	People at the same WiFi zone	Private blockchain

YouTube, can use Microcast to have a high quality and faster video streaming. Hence, in order to set up a reliable and secure peer-to-peer (P2P) network, users must know each other and trust each other, otherwise the connection will not be secure. Moreover, there are constraints in Microcast where only a small number of users who are within proximity of each other can build a peer-to-peer network and connect to each other.

This thesis is presuming the scenario where all smart phone users who are in a campus, a shopping center, a hotel or all passengers in a train who are connected to the same WiFi network and also have their cellular connection using different mobile data operators providing distinct download speeds. The objective of this method is to provide a secure, fast and high quality video streaming experience to smart phone users, who are connected to the same WiFi, by employing Blockchain technology regardless of their data connection's speed.

3. PROPOSED APPROACH

In the present thesis, a video streaming method is proposed, which provides a secure and fast streaming experience for mobile phone users in the same zone. The scenario where a group of mobile devices which are in the same WiFi zone is considered. For example a group of students in a campus who are connected to the same WiFi and would like to watch a training video or an online webinar at the same time from their cell phones; or all passengers waiting for their flights in an air port, which are connected to the air port WiFi and want to watch the same movie or an important live soccer match at the same time using their mobile phones. These devices will connect to each other through a private blockchain network and will share their downloaded segments through a P2P network with each other directly through a secure channel.

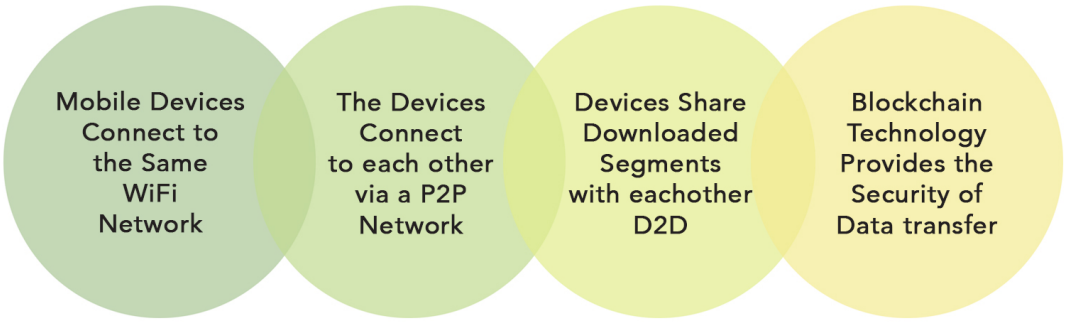

Figure 3.1 : Stages of proposed approach.

3.1 Network Structure

The proposed method in this thesis, sets up a P2P network where mobile devices can connect to each other and share their buffered data during live streaming with each other through the P2P network. P2P is the abbreviation for "Peer to Peer". In this kind of network, the "peers" are devices which are connected to each other directly over the internet without requiring a central server. As devices joined to a P2P network they can exchange data directly between each other on the network without the need of a third authority. In other terms, each device on a P2P network turns into a server as well as a client.

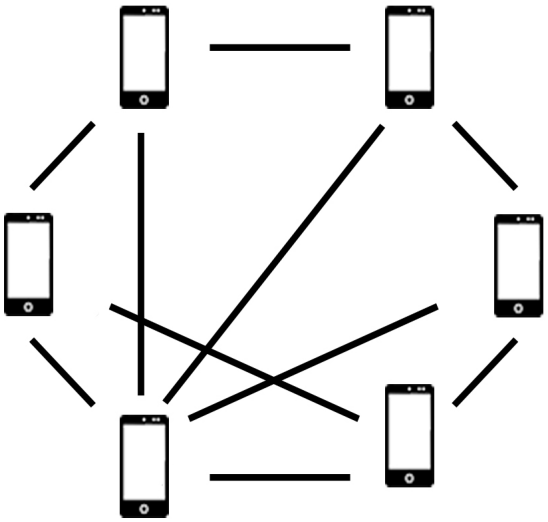

Figure 3.2 : Peer-to-Peer Network.

The popularity of streaming with cache and possible more applications are described in [12]. Each device will use its cellular data connection to download the video packets during the video streaming and as it is the part of P2P network, it would exchange the cached packets with other devices in the network. This process results in a faster video streaming with high quality and minimum cellular data usage.

3.2 Security Strategy

The other important point of concern is the security of Peer-to-Peer network since the passengers in the air port or the students in campus don't know each other. Devices which are the part of a network need to trust each other during packet exchange process to prevent receiving malicious packets from an adversary device. That is where the Blockchain comes in, our proposed method employs the Blockchain technology to provide security and a method of authentication for the network. Our approach targets the group of mobile devices in the same zone which are connected to the same WiFi (or at least in a close proximity for D2D connection) and want to watch the same video from the internet. The major objective is to provide a secure P2P network where the devices that don't trust each other can join the network and share their cached data during video streaming among this network. Since speed is an important factor during packet transfer between devices, private Blockchain has been selected for this purpose. Accordingly, only the devices with the same IP address (devices which are connected to the same WiFi), are allowed to join the network. Each packet needs to be confirmed

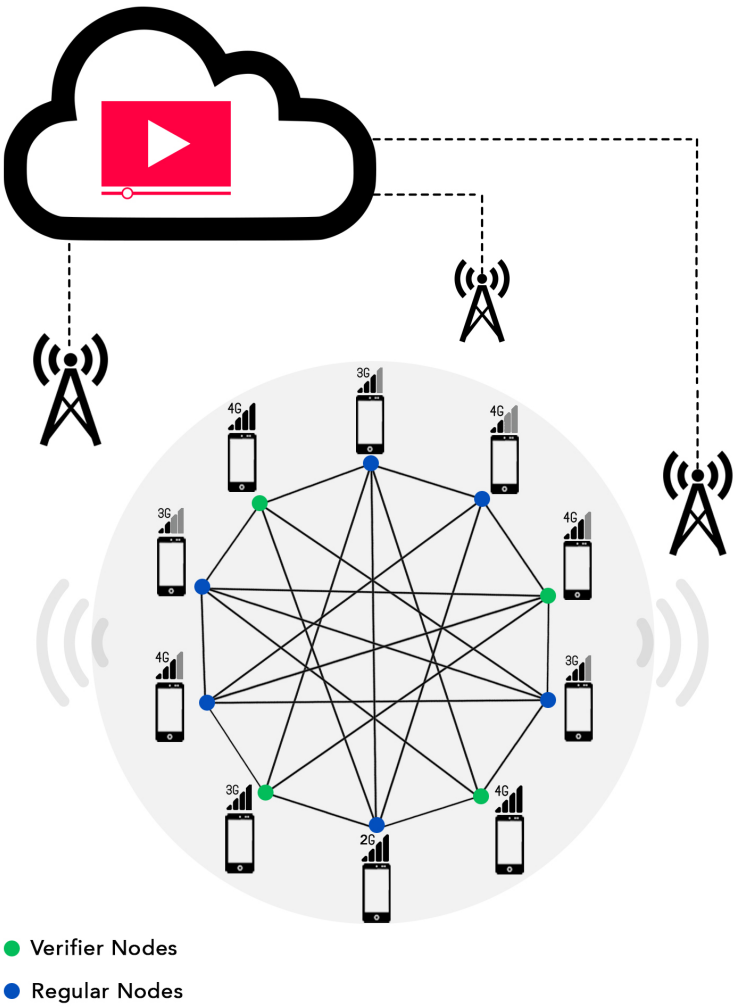

Figure 3.3 : Mobile phones in the same WiFi zone, with different cellular data, connected to each other through a P2P network and exchange the buffered packets during video streaming with each other. The verifier nodes define the packets which other nodes want to add to the chain.

by the verifier nodes in the chain before being transferred to other devices (nodes), therefore malicious packets will not be added to the chain. Figure 3.3 demonstrates the scenario of proposed framework.

In comparison with similar works [12], where the mobile phone users need to know and trust each other, and [10] which its security dependence on using VPN, proposed method guarantees the security of the network by employing Blockchain technology.

3.3 Framework

The proposed framework aims to design a secure Peer-to-Peer network which provides a fast and high-quality video streaming experience for mobile devices joined to the

network. For this purpose private Blockchain technology is employed. An algorithm is designed for this purpose, where the mobile devices which are connected to the same WiFi, can join to a Private Blockchain network and exchange their downloaded cache while they are watching a video from internet using their cellular data connection.

3.3.1 Algorithm

The algorithm pursues following steps:

- When a device wants to join the network the algorithm checks if its IP address belongs to corresponding WiFi network, if so then the device joins the network as a new node.
- Once a node joins to the network it receives the latest blockchain data from other nodes. The blockchain data contains the hash of packets that have been downloaded by each node in the the network during video streaming. It also contains a list consisting of the number of packets that each node has downloaded and senders/receivers nodes as well as information of video segments.
- Each node sends requests to other nodes for each segment of video according to the list. Each node sends the requested packets to the devices through the peer-to-peer network. Next, each device computes the hash of received packets and compares it with the hash of corresponding packet in the chain. As long as two hash values are equal, the device ensures that it has received the correct packet and not a malicious one.
- Whenever a node aims to add the hash of segment which has been downloaded by that node, to the chain as a new block, the verifier nodes decide if the block can be added to the chain or not. The node sends the downloaded packet and its hash value to the verifier nodes. In case the verifier nodes verified the packet as a normal packet, the hash value of packet will be added as a new block to the blockchain.

Figure 3.5 demonstrates the framework of proposed algorithm. In comparison with previous peer-to-peer video streaming methods, our proposed framework is focused on the security concern of P2P video streaming. As devices in the network share the buffered packets of video with each other the probability of receiving a malware, virus

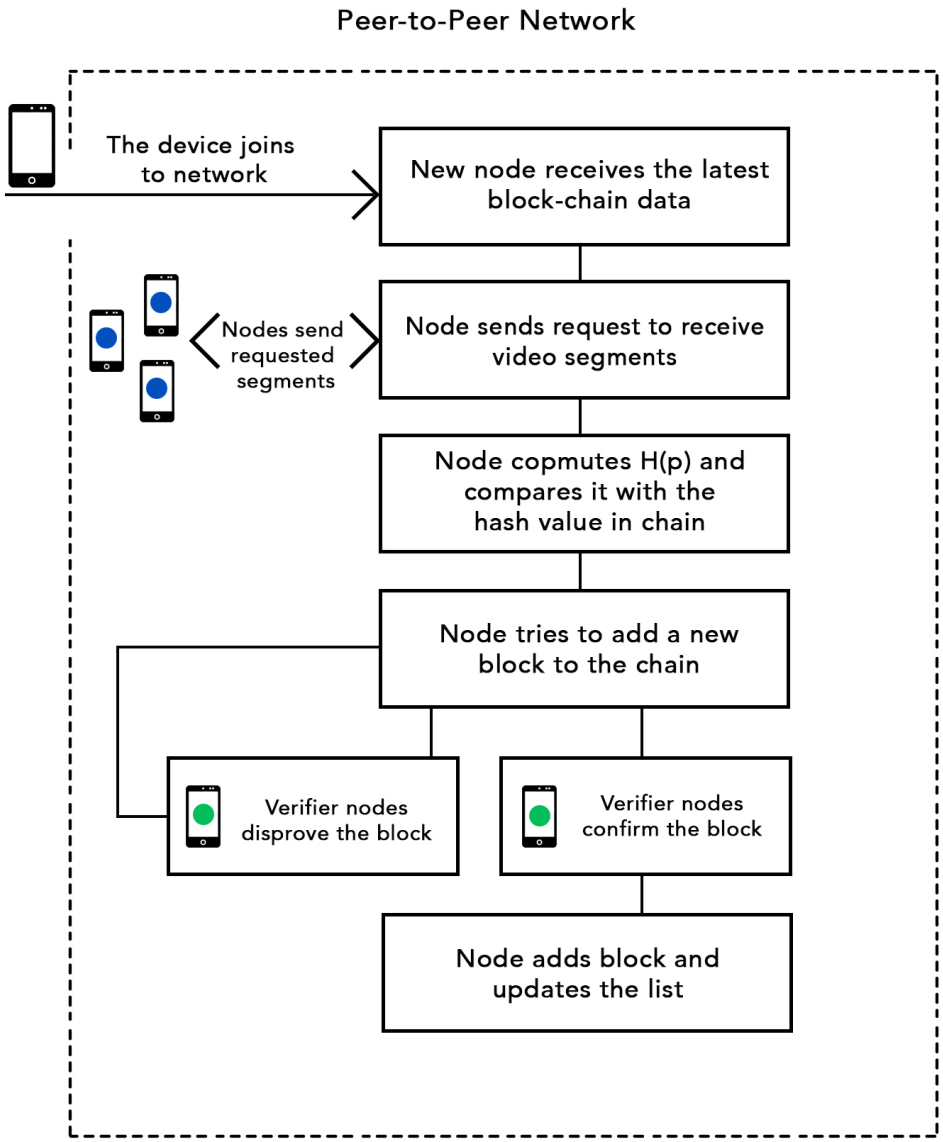

Figure 3.4 : Framework of proposed algorithm.

Algorithm 1: Pseudocode of proposed algorithm

Result: A new node joins to the P2P network and receives cached packets by other nodes among network.

1: Download the lates blockchain data
2: Send request to other nodes based on list
3: Compute the Hash of recieved packets
if $H(p_x) = H(p_x)inchain$ **then**
  use packet;
else
  ignore packet;
end

Result: A new block will be added to the chain.

1: Node sends the $H(p)$ to verifier node
2: verifier node computes the hash of p
if $H(p) = H(p_{downloadedfrommainsource})$ **then**
  Add packet as new block;
  Update the list;
else
  Refuse packet;
end

Figure 3.5 : Pseudocode of proposed algorithm.

or any malicious packet increases. This framework employs Blockchain technology in order to address this issue.

3.3.2 Block structure

The nodes of the blockchain network add the hash value of cached packets to the chain before transferring any packet to another node in the network. Once a node caches packet p_x during streaming, it computes $H(p_x)$ and sends its hash value to the verifier nodes, which already have access to packet p_x through main source. In the event the responsible nodes verify the packet p_x, $H(p_x)$ will be added to the chain as a new block. It is worth to mention that the block does not contain the packet itself but just its hash value, which is a unique fixed size value computed by a hash function, and identifies the packet. Accordingly, when a node joins the network and tries to download the blockchain data, it will receive the hash values of all segments of video downloaded by nodes among the network during streaming. Hence this process is not time consuming due to small size of hash values. Moreover, each block contains a list which informs the nodes about packet distribution among network. The list in each block includes the number of packets each node downloaded and also indicates each node owns which packets. For example the list proves node $A : \{p_1, p_2, p_4, p_5, p_8\}$, holds packets p_1, p_2, p_4, p_5 and p_8; and node $B : \{p_2, p_4, p_7, p_9\}$, holds packets p_2, p_4, p_7 and p_9. Therefore, when a node adds a block to the chain, it also updates the list in block and informs other nodes among the network. In addition to this, each block also

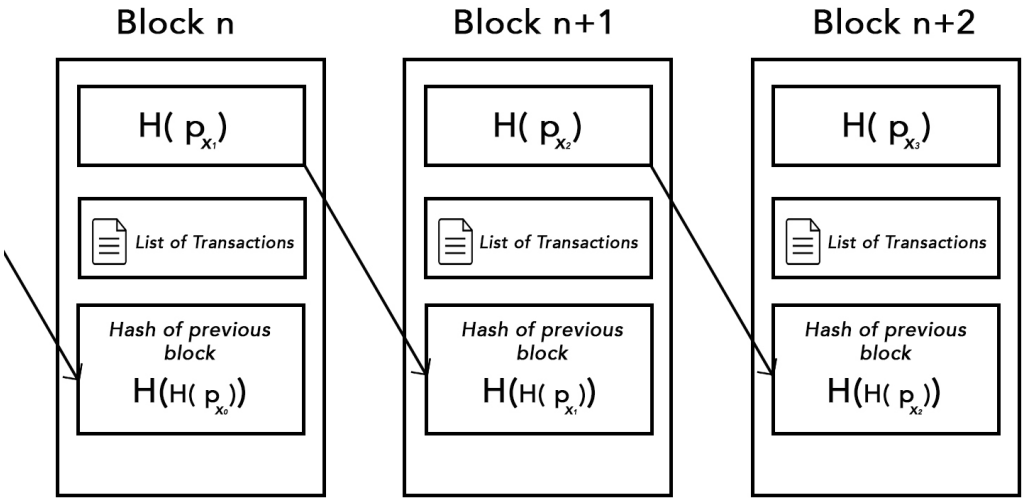

Figure 3.6 : Each block contains the hash of a cached packet, the list of transactions that demonstrate packet distribution, and the hash of previous block.

contains the hash value of previous block, which makes the chain immutable. Figure 3.6 illustrates the block structure of proposed method.

The nodes receive the blockchain data as they join the network, each node sends request the node that owns the packet it needs during video streaming. As an example, node C sends a request to node A for packets p_1, p_4, p_5, p_8 and it sends a request to node B for packets p_2, p_7, p_9. Once node C received packets from node A and B, it computes $H(p)$ for each packet, and compares it with the hash value of corresponding packet in the chain. As long as two hash values are the same, node C ensures that it has received correct packet.

3.3.3 Proof of authority

Proof-of-Work is a Sybil-resistance mechanism that leverages computation costs to self-regulate the network and allow fair participation. This works great in anonymous, open networks where competition for cryptocurrency promotes security on the network. However, in private/consortium networks the underlying ether has no value. Since speed is an important factor during packet transfer between devices, private Blockchain is employed to construct the P2P network of the proposed method. An alternative protocol, Proof of Authority (PoA), is more suitable for permissioned networks where all consensus participants are known and reputable. Without the need for mining, PoA is more efficient than PoW. The role of a miner in PoA is performed by a validator. The validators (known as authorities) in this algorithm are formally approved accounts whose identity is verified by an authorized public notary system and is kept public on-chain for cross-checking. PoA is a family of consensus algorithms for permissioned blockchain whose prominence is due to performance increases with respect to typical BFT algorithms; this results from lighter message exchanges. PoA is currently used by Parity and Geth, two well-recognised clients for permissioned setting of Ethereum. PoA algorithms rely on a set of N trusted nodes called the authorities. Each authority is identified by a unique id and a majority of them is assumed honest, namely at least N/2 + 1 [13]. The authorities run a consensus to order the transactions issued by clients. Consensus in PoA algorithms relies on a mining rotation schema, a widely used approach to fairly distribute the responsibility of block creation among authorities. Time is divided into steps, each of which has an authority elected as mining leader. There are two PoA implementations Aura and Clique where both work quite differently from each other. The two have a first round where the new block is proposed by the current leader (block proposal); then Aura requires a further round (block acceptance), while Clique does not [13].

3.3.4 Performance analysis

The performance metrics usually considered for consensus algorithms are transaction latency and throughput. In the specific case of private blockchains, the latency of a transaction t is measured as the time between the submission of t by a client and the

commit of the block including t. In comparison with PoW algorithm which is a CPU intensive consensus protocol, in PoA the latency is communication-bound rather than CPU-bound, as there is no relevant computation involved. Aura algorithm requires two message rounds for each block proposal in the first round the leader sends the proposed block to all the other authorities, in the second round each authority sends the received block to all the other authorities. A block is committed after a majority of authorities have proposed their blocks, hence the latency in terms of message rounds in Aura is 2(N/2+1), where N is the number of authorities. Clique algorithm requires a single round for block proposal, where the leader sends the new block to all the other authorities. The block is committed straight away, hence the latency in terms of message rounds in Clique is 1 [13]. An Ethereum test network is deployed and ran the contracts in that network in order to analyze the performance of private blockchain. The analysis is performed on a private blockchain development based on the Ethereum platform, using Go-Ethereum (Geth) client implementation. The PoA Geth implementation utilizes Clique algorithm. To limit the number of processed transactions, Clique algorithm allows creating one block per defined period of time. Numerous parameters can affect the network performance. The main parameters are Sealers Number, Block Time and Gas Limit.

- **Sealers Number:** In PoA network consensus is achieved by a majority agreement among the sealers nodes. A sealer node is a special client which is allowed to include blocks on the blockchain. Sealers are set in a whitelist in the blockchain genesis block. Once the blockchain is running, new sealers could be added by majority voting. To consider a block as valid, it must be validated by at least 51% of sealers. By increasing the number of sealers the network latency could be also increased. This can generate synchronization problems during the generation of blocks. It is necessary to study how the amount of sealers affects the performance of the network.

- **Block Time:** Clique consensus algorithm divides time into epochs. At the beginning of each epoch, a sealer is selected using a Round Robin algorithm as the leader to propose a new block. During the epoch, the leader validates transactions and includes them in the new block, and once the epoch is finished, it broadcasts the block to the other sealers. If the majority of the sealers accepted it, the block

can (finally) be considered as valid. In case that the leader delays in submitting the block, some back-up sealers can take its place and propose another block instead. The time between two consecutive blocks is called block time. Despite the fact that in PoA networks theoretical block time is fixed by configuration, it can fluctuates due to synchronization and network delays. That is why it is interesting to measure real block times given other varying blockchain parameters, e.g. number of sealers and Gas Limit (which determines the block size). The block time configuration parameter can be used to set the maximum network throughput, as evaluated in Gas Limit section.

- **Gas Limit:** Gas refers to the fee, or pricing value, required to successfully conduct a transaction or execute a contract on the Ethereum blockchain platform. Ethereum platform prevents transaction spamming and rewards block miners by charging a gas fee on transactions. Each block contains a maximum amount of gas that can be collected from transactions, defining a maximum block size. That gas limit could be set as a configuration parameter. In the long term, the block gas limit approaches a target gas limit set also as a configuration parameter (it can also be changed at runtime if needed). The theoretical maximum transactions per second (TPS) can be calculated using the following equation:

$$TPS = \frac{Gas_{limit}}{T_{xGas} * Block_{Time}} \tag{3.1}$$

The performance of private Ethereum is analyzed by setting up different values for Sealers Number, Block Time and Gas Limit. Based on these analysis, we propose to use block times between 10 and 15 seconds, to keep a high TPS. Block times between 15 and 20 seconds are also expected to lead to a good performance. The analysis guarantees the good performance of the network when the blockchain is supported by up to 20 sealer nodes. Consequently, the results can assumed satisfying for a video on demand streaming application based on private blockchain.

3.3.5 System evaluation

Mobile devices buffer video segments during a live video streaming. Different video streaming applications cache video fragments in various formats. For example Youtube application for android devices caches video segments in *.exo* format. As outlined

in [14], each fragment contains a portion of a stream and has its own 'order' which identifies that fragment. Only the specific application which has been cached the segments, can join them together and decode them in order to create a viewable video.

The proposed method can be discussed from two perspectives, the first live video streaming and second video on demand. The devices share their cached data during live stream among a secure P2P network. Consequently, the network contains all segments, which have been broadcasted from the beginning of live stream, and their hash values. Therefore when a device joins the P2P network even in the middle of live streaming and not from the beginning, it can receive the previous segments from other nodes through a secure network. The evaluation of proposed framework is eliminating security issues of P2P video streaming methods by employing Blockchain technology. Actually, the proposed method provides a secure P2P network based on blockchain technology, that increase speed and quality of video streaming for mobile devices while it decrease cellular data usage in both live and VoD streaming.

4. CONCLUSIONS AND FUTURE WORK

The work presents an add on to highly accepted methods of cooperative video streaming [12] which utilize buffering of data and distribute the cached packets. This add on is to remedy security and privacy concerns of such fast video streaming frameworks. The applicability of Blockchain to numerous applications from economy to health sectors is being exploited in the proposed method. Even though, our framework has diminished the security concerns in P2P video streaming, additional assessments and precautions will be performed in the future work for high level confidence.

REFERENCES

[1] **Url-1**, (2019), <https://www.youtube.com/yt/about/press>.

[2] **Url-2**, (2019), <https://www.gsmaintelligence.com/research/?file=b9a6e6202ee1d5f787cfebb95d3639c5>.

[3] **Url-3**, (2018), <https://www.opensignal.com/sites/opensignal-com/files/data/reports/global/data-2018-11/state_of_wifi_vs_mobile_opensignal_201811.pdf>.

[4] **Url-4**, (2019), <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html#_Toc1455210>.

[5] **Nakamoto, S.** *et al.* (2008). Bitcoin: A peer-to-peer electronic cash system.

[6] **Zheng, Z.**, **Xie, S.**, **Dai, H.**, **Chen, X. and Wang, H.** (2017). An overview of blockchain technology: Architecture, consensus, and future trends, *2017 IEEE International Congress on Big Data (BigData Congress)*, IEEE, pp.557–564.

[7] **Url-5**, (2015), <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains>.

[8] **Liu, Y.**, **Guo, Y. and Liang, C.** (2008). A survey on peer-to-peer video streaming systems, *Peer-to-peer Networking and Applications*, *1*(1), 18–28.

[9] **Url-6**, (2019), <https://popcorntime.sh/faq>.

[10] **Cohen, B.** (2003). Incentives build robustness in BitTorrent, *Workshop on Economics of Peer-to-Peer systems*, volume 6, pp.68–72.

[11] **Url-7**, (2018), Community based video distribution., <https://www.flixxo.com/docs/Whitepaper_0.6.pdf>.

[12] **Keller, L.**, **Le, A.**, **Cici, B.**, **Seferoglu, H.**, **Fragouli, C. and Markopoulou, A.** (2012). Microcast: Cooperative video streaming on smartphones, *Proceedings of the 10th international conference on Mobile systems, applications, and services*, ACM, pp.57–70.

[13] **De Angelis, S.**, **Aniello, L.**, **Baldoni, R.**, **Lombardi, F.**, **Margheri, A. and Sassone, V.** (2018). Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain.

[14] **Horsman, G.** (2018). Reconstructing streamed video content: A case study on YouTube and Facebook Live stream content in the Chrome web browser cache, *Digital Investigation*, *26*, S30–S37.

CURRICULUM VITAE

Name Surname : Nasim TAVAKKOLI

Place and Date of Birth: Tabriz, Iran 1989

E-Mail : tavakkoli17@itu.edu.tr

EDUCATION:

- **B.Sc.** : 2012, Payame Nur University of Tabriz, Information Technlogy Engineering
- **M.Sc.** : 2019, Istanbul Technical University, Cyber Security Engineering and Cryptography

PROFESSIONAL EXPERIENCE AND REWARDS:

- 2018, Received Master scholarship from Vodafone Future Lab

OTHER PUBLICATIONS, PRESENTATIONS AND PATENTS:

Kurt, G.K., Khosroshahi, Y., Ozdemir, E., Tavakkoli, N. and Topal, O.A., 2019. A Hybrid Key Generation and a Verification Scheme. IEEE Transactions on Industrial Informatics.