Secured Land Title Transfer System in Australia using VPN based Blockchain Network

Mohamad Arsalan Sheikh*, Faryal Khattak**, Gul Zameen Khan***, Farookh Khadeer Hussain*

*School of Computer Science, University of Technology Sydney, Australia

**Department of Business Strategy and Innovation, Griffith University, Australia

***NLT Digital Solutions Australia

mohamadarsalan.sheikh@student.uts.edu.au, faryal.khattak@griffithuni.edu.au, gulzameenkhan@gmail.com, farookh.hussain@uts.edu.au

Abstract— **Blockchain technology has evolved as a secure method for storing important private and public record transactions. Transfer of land title is one such important public record. To this end, a blockchain-based system is proposed in the context of NSW (New South Wales) Australia in this paper. However, due to the decentralized and distributed nature of the blockchain network, it is prone to several security attacks. We have focused on the routing attacks, particularly on the delay attacks for the blockchain network. A VPN (Virtual Private Network) based blockchain network is proposed and implemented in this paper to mitigate the routing attacks. The results show that the proposed VPN-based blockchain network outperforms the traditional blockchain-based network in the presence of a routing attack.**

Keywords—**Blockchain, land records, VPN, routing attacks, Hyperledger Fabric**

I. INTRODUCTION

Blockchain technology has recently attracted tremendous attention, with many experts citing its potential applications in a variety of industries, markets, agencies, and governmental organizations [1]. Irrespective of different domains, the general architecture of blockchain approaches is relatively similar, with few differences in terms of tools, software, and applications. The most important and unique factor of blockchain technology is that the information is stored in a completely secure manner within the blocks of the blockchain's transactions [2].

The significance of blockchain technology in preserving trustworthy digital records has been the focus of attention of several researchers. This is equally important in safeguarding the govt’s important records and assets as well protecting valued records of private organizations and financial instituitions. In [3], some of the limitations, risks, and opportunities with the implementation of blockchain technology for a land registry system are discussed. Land registration refers to a system whereby a government entity records ownership and land-related rights. The land registration system, title transfer system, and information system provide evidence of title, facilitate transactions, and prevent fraud. An outdated and manual land record system could lead to several problems such as delays in ownership verification, slow down of legitimate transactions, and e-land misappropriation [4]. The authors in [5] discussed the progress of two countries (Honduras and Georgia) use cases of land record modernization by adopting blockchain technology. In addition to technology-related factors such as infrastructure and readiness, the socio-political factors were also considered important during the digitization process. Thus, the implementation of blockchain technology in the land title transfer system needs to be discussed in the context of a specific country and its conditions.

The administration of land utilizing Information and Communication Technology has been a core focus of governments in developing counties. In Australia, every state has its own e-land administration system. The common initiatives include providing land information online, electronic conveyancing, digital lodgment of survey plans, and online access to survey plan information [6]. Updating land titles involves several stack holders sharing their data. Since these stack holders are usually geographically located on different locations and the land title records are stored at a central location maintained by a state or federal government/entity. Therefore the most prominent mode of communication for the stack holders to access this information is the Internet, which is not secure, available to everyone (not private). Blockchain technology provides a solution by decentralizing data to provide access to only intended users.

When a blockchain is distributed involving different stack holders, there is a high probability that the blockchain network will be implemented on geographically distributed nodes. As a result, there is a need to transfer data between the nodes over the Internet which is an IP based network. As IP network is insecure, the information exchanged between the nodes may be exploited by several attacks such as routing attacks, eclipse attacks, Distributed Denial of Service (DDoS) attacks, unauthorized access, man in the middle attacks, code and SQL injection attacks, and privilege escalation attack etc.

In this paper, we focus on routing attacks. Apostolak et. al [5] discussed two kinds of routing attacks, namely partitioning and delay attacks, along with their potential impact on Bitcoin. A blockchain network is split into two or more than two disjoint components by an attacker, affecting the exchange of data between these disjoint parts. In this way, the attacker can intercept all information that is exchanged between these partitioned components by exploiting the vulnerabilities in the Border Gateway Protocol (BGP), which does not validate the origin of routing announcements. Thus, the attacker can advertise false prefixes claiming that it has a better route to a node in one of the portioned components and can intercept the traffic between the nodes.

Similarly, in a delay attack, the attacker intercepts the blockchain network traffic, delaying block propagation on the corresponding connections. Bitcoin is centralized from the Internet’s routing perspective because 20% of the Bitcoin nodes are hosted in less than 100 IP prefixes. This centralization of Bitcoin nodes in a few networks and prefixes, combined with the centralization of mining power in few pools, paves the way for networking attacks such as partitioned and delay attacks. The authors [5] have proposed short-term and long-term solutions to reduce these attacks.

Authorized licensed use limited to: UNIVERSIDADE DE SAO PAULO. Downloaded on September 21,2023 at 00:01:55 UTC from IEEE Xplore. Restrictions apply.

This includes routing-aware peer selection, maximizing the diversity of the Internet paths, monitoring the behavior of different connections to detect events like abrupt disconnections from multiple peers or unusual delays in block delivery, and end-to-end encryption. However, there is a need for a systematic design-level approach to mitigate these routing attacks.

The main contributions of this paper are listed below:

- We have proposed, developed, and implemented a blockchain-based network to transfer the land titles which is more secure, authenticated, and flexible than the traditional e-land system.
- Separate channels have been proposed and implemented in the blockchain network to segregate information shared among different peers. This approach not only enchances the security and privacy but also provides a mechanism to avoid unauthorized alteration to public records.
- A VPN-based solution has been proposed and implemented to mitigate the routing attacks in blockchain networks that are geographically distributed across different regions.

The remainder of the paper is organized as follows. In Section II, background knowledge is discussed, including land title transfer, blockchain technology, and IPSec/SSL VPN. Next, the proposed blockchain-based secured land title transfer system is presented in Section III, followed by results and discussions in Section IV. Finally, the paper is concluded in Section V.

II. Background

A. LAND Title Transfer

In Australia, land legislation is based on the Torrens principle of registration of title. Each state and territory have a central register of all land in the state which shows the owner of the land. The land title is the official record. It can also include information about mortgages, covenants, caveats, and easements [8]. A title or ownership of the land could be changed for several reasons: buying/selling, changing the ownership structure or type, family reasons, and change in commercial or agricultural circumstances, to name a few. In this paper, the focus is on changing/transferring the land title due to selling or buying purposes.

When a buyer buys land (residential, commercial, agricultural, industrial) from a seller in Australia, there are many stakeholders and laws involved in this process. The stakeholders and regulations may vary from one state and territory to another; however, the overall process usually consist of the following steps:

1. **Pre-approval of Loan**: In this journey, the first step is usually getting pre-approval for one's land loan from a financial institution such as a bank. It enables the buyer to indicate from the financial institution how much money they can borrow for buying the land.
2. **Sign Contract of Sale:** This is the written agreement outlining the terms and conditions pertaining to the sale of the land. It includes information such as the names and address of the buyer and seller, price of the land, name, and address of the selling agent, conditions of the sale and inclusions, and last but not the lease the settlement period. It will be either a conditional offer (containing specific conditions on which the sale relies) or an unconditional offer (when the purchaser has funds immediately available).
3. **Exchange Contracts:** Once the price and conditions are agreed upon, both the purchaser and seller sign the contract of sale document.
4. **Pay Deposit:** This is held in a trust account and cannot be accessed by the developer until settlement.
5. **Find a Settlement Agent:** There is a need to appoint a settlement agent/solicitor who will handle the paperwork involved with the purchase. At this point, any special terms and conditions of the sale are clarified.
6. **Finalize the loan arrangements:** At this stage all the mortgage documents are finalized and signed. The lender or mortgage broker assist with this process.
7. **Sign a Transfer of Land Document:** After the exchange of contract, a transfer of land document is signed. The document is then registered with the Land Titles Office/Register of Titles (by the owner or developer), so the property can be transferred into buyer's name.
8. **Register the Land Title:** This is an official record of ownership of the land and is kept by the Land Titles Office/Registrar of Titles. Once the purchase is officially registered, final settlement takes place, your mortgage becomes active, and the property is yours!

In NSW, the transfer of the title is managed by the NSW Land Registry Services, which operates the NSW land titles registry for the state government and the people of NSW [10]. To change the title, the seller, buyer, or the selling agent needs to fill a form known as Form 01T to Land & Property Information (LPI). In addition to this, they also need to provide a completed Notice of Sale (NOS) or Transfer of Land form, original Certificate of Title for the relevant property, lodgment fee, a statutory declaration of the names and postal addresses of the other joint tenants and any mortgagees if applicable.

B. Blockchain Technology

Blockchain can be implemented in two ways namely: permissions and permissioned. In a **permission less blockchain**, virtually anyone can participate, and every participant is anonymous. In such a context, there can be no trust other than that the state of the blockchain, prior to a certain depth, is immutable. **Permissioned** blockchains, on the other hand, operate a blockchain amongst a set of known, identified and often vetted participants operating under a governance model that yields a certain degree of trust. A permissioned blockchain provides a way to secure the interactions among a group of entities that have a common goal, but which may not fully trust each other [9].

Blockchain can be public or private. All the nodes have access to all ledgers in a public blockchain, meaning every node will have access to the full database. In a private blockchain, we can limit few nodes to access it. With the ability to coordinate their business network through a shared ledger, blockchain networks can reduce the time, cost, and risk associated with private information and processing while improving trust and visibility.

Authorized licensed use limited to: UNIVERSIDADE DE SAO PAULO. Downloaded on September 21,2023 at 00:01:55 UTC from IEEE Xplore. Restrictions apply.

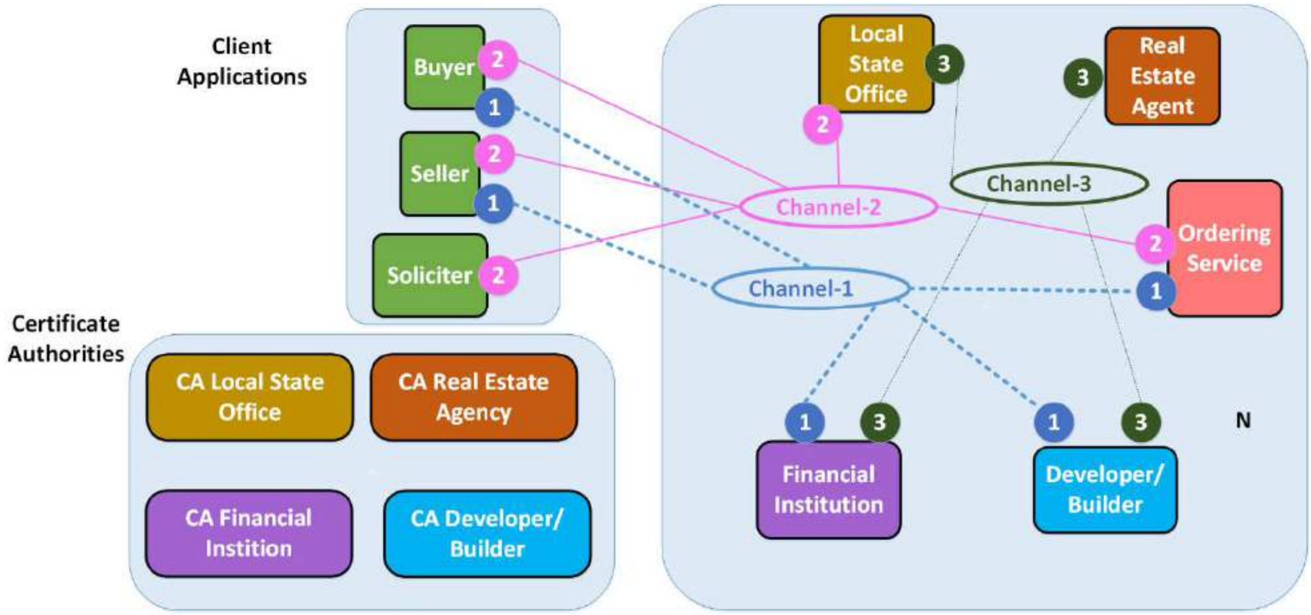


Fig. 1. Overview of Architecture of Blockchain Network

Hyperledger Fabric is one of the blockchain projects within Hyperledger. Like other blockchain technologies, it has a ledger, uses smart contracts, and is a system by which participants manage their transactions

Where Hyperledger Fabric breaks from some other blockchain systems is that it is **private** and **permissioned**. Rather than an open, permissionless system that allows unknown identities to participate in the network (requiring protocols like "proof of work" to validate transactions and secure the network), the members of a Hyperledger Fabric network enroll through a trusted **Membership Service Provider (MSP**

C. *IPSec and SSL VPN*

Virtual Private Networks (VPN) offer a secure data exchange over public network infrastructure. There are several kinds of VPN available today to enable logical connections over the Internet. The logical connection can be made at Layer 2, Layer 3, or Layer 4 of the OSI model. In this paper, we focus on analysing the performance of a blockchain-based network over Layer 3 and Layer 4. We assume the nodes of the blockchain network may belong to different organizations connected over the Internet. There are several options of VPNs to choose from, such as Generic Routing Encapsulation (GRE), Layer 2 Tunneling Protocol (L2TP), Multi Protocol Label Switching (MPLS), and Internet Protocol Security (IPSec) VPNs at Layer 3 whereas Secure Sockets Layer (SSL), Transport Layer Security (TLS) at Layer 4 [12][14].

IPsec is a framework of open standards for ensuring private communications over public networks. It is fundamentally a collection of several protocols that assist in protecting communications over IP networks. It is widely used by enterprises (small, medium, large), service providers, and governmental originations. The biggest advantage of IPsec framework is that it is supported by almost all popular vendors such as Cisco, Juniper, Palo Alto, HP, Aruba, FortiGate, etc. The basic components of the IPSec protocol suite are Encapsulating Security Payload (ESP), Authentication Header (AH), and Internet Key Exchange (IKE) protocols [13][14].

AH provides integrity protection for packet headers and data, as well as user authentication. It can operate either in transport or tunnel mode. A new IP header is created for each packet in the tunnel mode, whereas the protocol does not create a new IP header in the transport mode. AH can provide integrity, data origin authentication, and replay detection. However, it does not provide confidentiality [15]. On the other hand, ESP can be used to provide only encryption, encryption, and integrity protection; or only integrity protection.

III. Proposed Blockchain-based secured Land Title Transfer System

We propose a distributed blockchain network system consisting of three major components: blockchain network, certificate authorities, and client applications, as shown in Fig 1. The major components of the proposed blockchain network N further consist of the participating stakeholders in land title transfer in the context of NSW. These stakeholders are local state offices, real estate agents, financial institutions, developers/builders, and one or more ordering services. These stakeholders can change from state to state or from one country to another depending on the process flow of the land title transfer system. The local state office is responsible for providing all the necessary documentation and forms, as explained in Section II. The real estate agent or the broker coordinates all the deals and is usually the main point of contact for a seller/buyer. The financial institution could be a bank or public/private financial entity that has provided a loan to the buyer. There is also another entity involved in the case of a new home/property construction, which is the construction company known as a builder. All these entities need to communicate with a certain entity which is called the Ordering Service. This could be anyone, but usually, it needs to be the state government.

The second component is the Certificate Authority (CA) who is responsible to authenticate all the other entities using a

Authorized licensed use limited to: UNIVERSIDADE DE SAO PAULO. Downloaded on September 21,2023 at 00:01:55 UTC from IEEE Xplore. Restrictions apply.

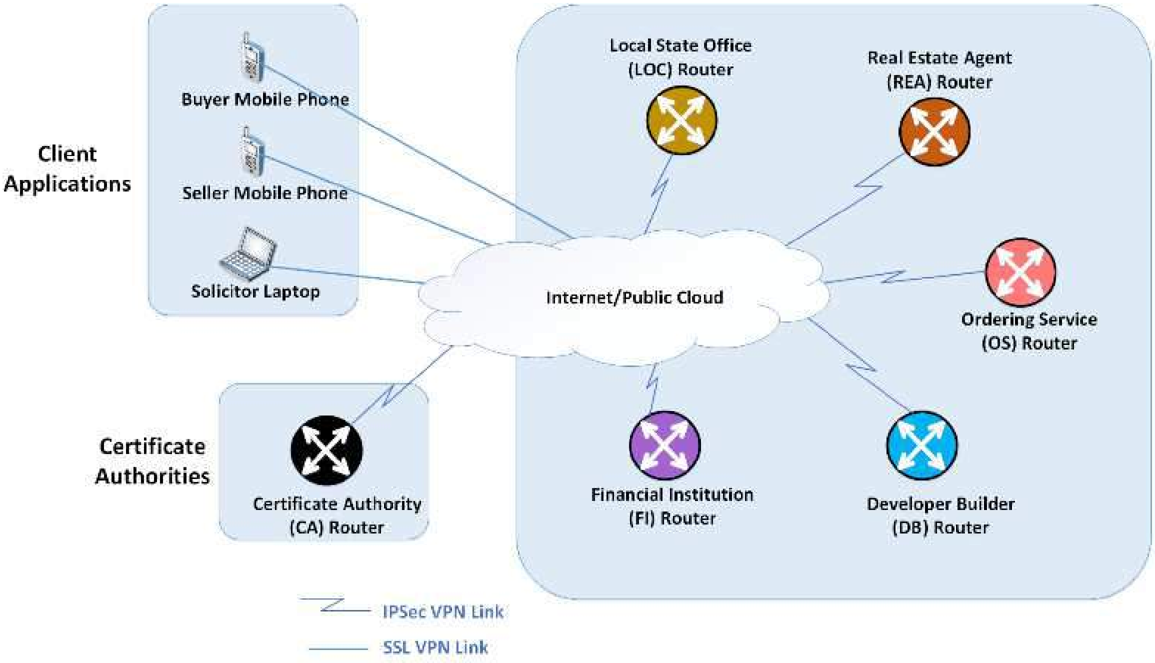

Client Applications
Buyer Mobile Phone
Seller Mobile Phone
Solicitor Laptop
Certificate Authorities
Certificate Authority (CA) Router
Local State Office (LOC) Router
Real Estate Agent (REA) Router
Internet/Public Cloud
Ordering Service (OS) Router
Financial Institution (FI) Router
Developer Builder (DB) Router
IPSec VPN Link
SSL VPN Link

Fig. 2. Overview of network implementation

digital signature. We have defined a separate CA for every stakeholder to segment and provide more internal security. This will also help organize an independent CA system for all entities as every organization can choose their existing root CA to authenticate the communication. Lastly, the third major component is the client-side applications which could be used by the seller, buyer, or any third-party solicitor (if any).

In addition to the blockchain elements, we have defined several channels which are used for communication. The idea behind choosing several channels is to provide segregation and privacy. For example, channel-1 connects seller, buyer, financial service, builder, and ordering service. This could be used for fund transfer in the case of a deal between the seller and buyer. On the other hand, channel-2 is used to connect the seller, buyer, solicitor, local state office, and ordering service. This may be used for signing the different forms which the state government provides. Similarly, channel-3 is used by the local state office, builder, real estate agent, and financial institute. This is used for the official coordination to comply with the rules.

We discussed the Hyperledger implementation of the blockchain in the above paragraphs. In Fig. 2, the network details are illustrated. The implementation details are discussed in the next section. The proposed system consists of edge routers, namely: Local Estate Office (LOC) router, Real Estate Agent (REA) router, Financial Institution (FI) router, Developer/Builder (DB) router, Ordering Service (OS) router, and the Certificate Authority (CA) router. All these edge routers are connected to the public Internet. We discussed the details of the Internet as a network of different service providers. All these edge routers form full mesh IPSec links based on the channels (1,2,3). The client applications could run on a mobile phone or a laptop peering with the rest of blockchain networks via SSL or DTLS link.

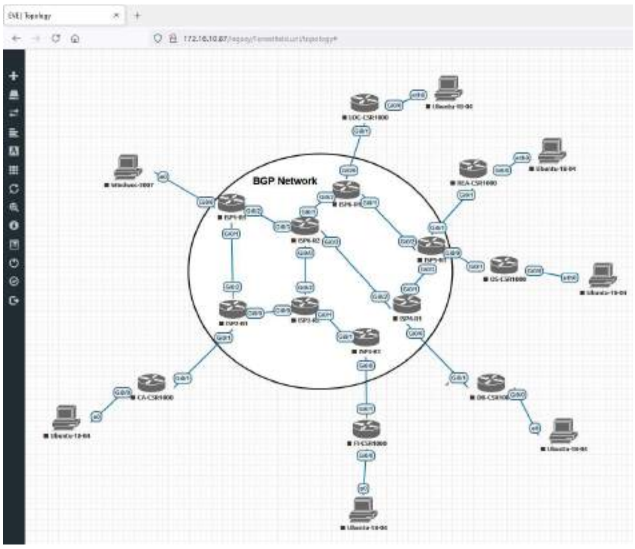
To implement the land title transfer system in Hyperledger Fabric, we have used NodeJS as a backend programming language. The smart contract is written based on the following entries as defined by the NSW land system [10].

- *Street address*
- *Reverse Street Address*
- *Certificate of Title (CT)*
- *Certificate of Authentication Code (CAC)*
- *Prior Title*
- *Documents*
- *Land Value*
- *Deeds - General register*
- *Cadastral records*
- *Survey Marks*
- *Parish/town index*

IV. Results and Discussions

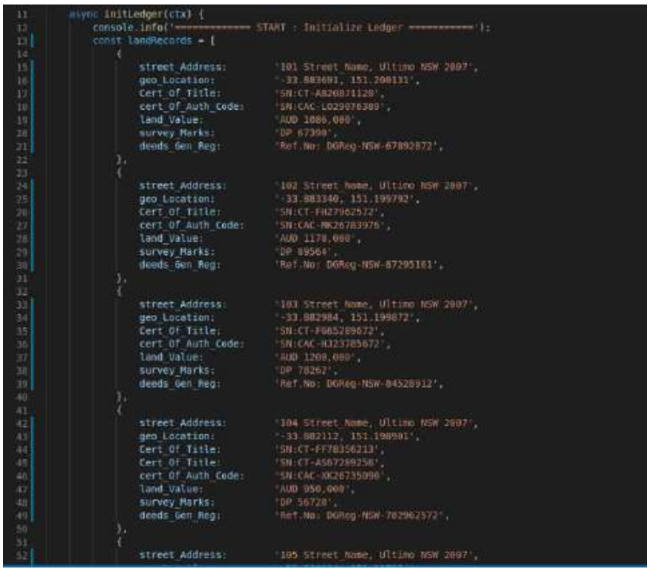
We have implemented the proposed VPN-based blockchain network in a nested Virtual Machine (VM) environment based on EVE-NG, a clientless multivendor network emulation software. The EVE-NG server has been setup on VMware Workstation 15 Player. Each Peer of the proposed system behind the edge routers (LOC, REA, OS, DB, DI, and CA routers) is implemented in separate docker containers running on Ubuntu 18.04 VMs. We have also emulated the client applications on a Windows 2007 VM. Thus, there are six Ubuntu 18.04 VMs and one Windows 2007 VM in our topology. It is assumed that all the Peers and the Certificate Authority VMs are running inside their internal organizations, data center, or their private/public clouds. Hence all these devices are behind an edge router. These edge routers are connected to each other via the public Internet, as shown in Fig 3. We have used Cisco CSR1000 router images for the edge routers. For the Internet, we have used a BGP network with six different Service Providers (SP) which are connected to each other using eBGP neighborship. Each SP and all edge routers are running in separate Autonomous Systems (ASes). There are 12 AS which are connected to each other with eBGP neighbors. We have used full mech iBGP neighnorship to connect routers inside an AS.

Authorized licensed use limited to: UNIVERSIDADE DE SAO PAULO. Downloaded on September 21,2023 at 00:01:55 UTC from IEEE Xplore. Restrictions apply.



.

Fig. 3. Network Topology



```
async initLedger(ctx) {
    console.info('============= START : Initialize Ledger ===========');
    const landRecords = [
        {
            street_Address:       '101 Street Name, Ultimo NSW 2007',
            geo_Location:         '-33.883691, 151.200131',
            Cert_Of_Title:        'SN:CT-AB20871128',
            cert_Of_Auth_Code:    'SN:CAC-LO29076389',
            land_Value:           'AUD 1086,080',
            survey_Marks:         'DP 67390',
            deeds_Gen_Reg:        'Ref.No: DGReg-NSW-67892872',
        },
        {
            street_Address:       '102 Street Name, Ultimo NSW 2007',
            geo_Location:         '-33.883340, 151.199792',
            Cert_Of_Title:        'SN:CT-FH27962572',
            cert_Of_Auth_Code:    'SN:CAC-MK26783976',
            land_Value:           'AUD 1178,080',
            survey_Marks:         'DP 89564',
            deeds_Gen_Reg:        'Ref.No: DGReg-NSW-87295161',
        },
        {
            street_Address:       '103 Street Name, Ultimo NSW 2007',
            geo_Location:         '-33.882984, 151.199872',
            Cert_Of_Title:        'SN:CT-FG65289672',
            cert_Of_Auth_Code:    'SN:CAC-HJ23785672',
            land_Value:           'AUD 1200,080',
            survey_Marks:         'DP 78262',
            deeds_Gen_Reg:        'Ref.No: DGReg-NSW-84528912',
        },
        {
            street_Address:       '104 Street Name, Ultimo NSW 2007',
            geo_Location:         '-33.882112, 151.198981',
            Cert_Of_Title:        'SN:CT-FF78356213',
            Cert_Of_Title:        'SN:CT-AS67289258',
            cert_Of_Auth_Code:    'SN:CAC-XK26735090',
            land_Value:           'AUD 950,000',
            survey_Marks:         'DP 56728',
            deeds_Gen_Reg:        'Ref.No: DGReg-NSW-782962572',
        },
        {
            street_Address:       '105 Street Name, Ultimo NSW 2007',
```

Fig. 4. Smart contract code snippet

This will mimic a small version of the Internet, as shown in Fig. 3. We have allocated low memory (250MB) to each router as the whole system is running on Lenovo i7 Laptop with 32GB RAM Windows 10 host.

The hyperleder fabric 2.0 has been setup on the docker running in Ubuntu VMs. The smart contract is written in NodeJS, as shown in Fig. 4. We implemented a full mesh IPSec tunnel among all edge routers using the IKEv1 protocol. Then communication was set up between the Hyperledger, Peers, Ordering Service, CA, and client application using the Peer gossip data dissemination protocol [16] which is the underlying protocol of Hyperledger Fabric blockchain network.

As the blockchain messages are sent in a secure tunnel using the IPSec tunnel, they are less prone to routing attacks than the case when they are sent using the IP network. The primary known attacks on the blockchain transactions that are focussed in this paper are delay and partition attacks. As discussed in detail in [5], these attacks result from intercepting the ASes path attribute and then changing or prepending AS number to the AS-Path attribute of the BGP protocol to change the traffic flow path. As a result, the blockchain network is split into two parts, or the transactions are delayed, leading to double spending and other problems in the blockchain network. For an attacker to attack the BGP routes, the information of the data part of the Blockchain transaction packet or the information of the source/destination IP addresses is crucial. The other compromised parameter is the AS information of the nodes participating in the blockchain network, which could be a mining computer in public blockchains such as Bitcoins or the Peers/CA/OS/Client application in the private blockchain, which is the case of this paper.

With the use of IPsec tunnel, all messages of the Peer gossip data dissemination protocol are exchanged after the secure tunnel is setup. We have proposed a packet based on our model which consists of several headers as shown in Fig. 5. We have used the tunnel mode of ESP encapsulation to encrypt the original IP header of the edge routers and thus the attacker will not be able to see the original IP. This also adds ESP header and EPS trailer to authenticate and encrypt the rest of the packet. We have maintained the DTLS with UDP which is used by the Hyperledger fabric for encrypting blockchain data. By adding another layer of encryption using ESP, the original IP header is also encrypted which will reduce the attacks on any internal IPs.

We have analyzed the delay which could be taken by a packet over public Internet using an online tool [16]. This was measured from Sydney Australia to 25 different cities across the different parts of the world to get a practical packet delay over the Internet as shown in Fig 6. We repeated the delay test over 30 runs and then calculated the average to measure more realistic values. The minimum delay was recorded 11.5 - 12.35ms to Melbourne whereas the maximum delay 325.42 - 325.62ms was recorded for Moscow. These delays were randomly added to our service provider network/Internet to emulate a practical view of the blockchain network.

As shown in Fig. 3, the SP networks consist of several ASes. We have configured BGP on these routers as well as on the edge routers. The delays calculated in Fig. 6 are added to the SP routers. We have determined the delays in the presence and absence of a routing attack both for the proposed VPN-based method and the traditional blockchain method. We have emulated a practical routing attack which was presented in [5]. The results of the attacks were used in the SP network in our network topology.

Table 1. lists the average transmission delay of the proposed VPN-based blockchain network as compared to the

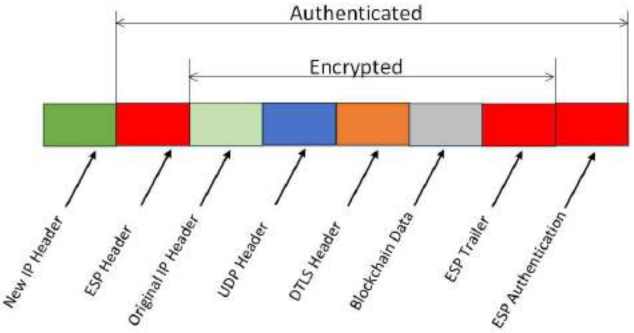


Fig. 5. Proposed Packet format

Authorized licensed use limited to: UNIVERSIDADE DE SAO PAULO. Downloaded on September 21,2023 at 00:01:55 UTC from IEEE Xplore. Restrictions apply.

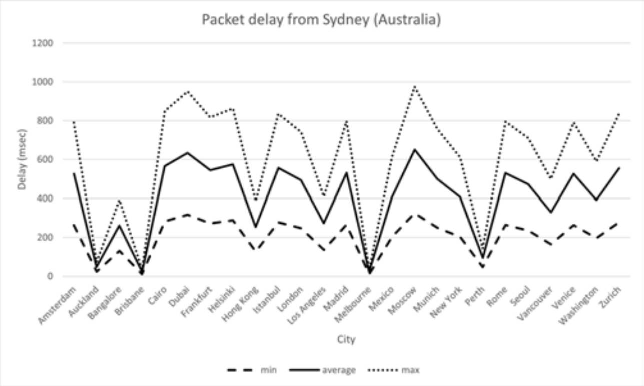


Fig. 6. Delay of a packet from Sydney to other cities

traditional Hyperledger fabric messages. The results calculated from the network topology show that the average transmission delay of a packet is 500ms in a traditional blockchain network, whereas 700ms (200ms increased) in the case of the proposed VPN-based blockchain network due to the extra overhead. However, when we modeled the routing attack as per the findings of [5], the packets were delayed up to 20 minutes in traditional blockchain, which leads to several problems. On the other hand, the VPN-based traffic is secured in two layers, as shown in Fig. 5. As a result, the attacker can not find the source or destination of the targeted traffic, thereby unable to predict its ASes. We observed that there could be an additional delay of up to 1100ms if an attacker filters traffic based on an Access list or AS filtering as listed in Table 1.

We have also calculated the overhead of the proposed packet size as compared to traditional blockchain traffic. Table II lists the different headers with their size both for the proposed and the conventional blockchain network. The overhead is only 2.98% for the security level that it provides.

TABLE I. AVERAGE TRANSMISSION DELAY OF PROPOSED AND TRADITION BLOCKCHAIN NETWORK

Protocol	**Average transmission delay**	
	Without routing Attack	***With Routing Attack***
Proposed method	700ms	1100msec
Traditional method	500ms	20 min

TABLE II. HEADER SIZE OF THE PROPOSED AND TRADITIONAL BLOCKCHAIN NETWORK

Header	***Size (bytes)***	
	Proposed Method	***Traditional Blockchain Method***
Ethernet	20	20
New IP header	20	N/A
ESP header	8	N/A
Original IP header	20	20
UDP header	8	8
DTLS header	13	13
Blockchain data	1407	1449
ESP trailer	2	N/A
ESP authentication	2	N/A

V. CONLCUSION

We have proposed a secured land tile transfer system based on a VPN-based blockchain network. A complete distributed system-level design has been proposed and implemented in the context of the NSW transfer title system onboarding all the major stakeholders. The system has been secured by implementing a VPN-based blockchain network wherein all the communication is encrypted and authenticated. The results show that the proposed method is more secure than the traditional blockchain communication in the presence of routing attacks.

REFERENCES

[1] D. Berdik, et al. "A survey on blockchain for information systems management and security" in Information Processing & Management 2021, 58(1), p.102397.

[2] S. Singh, A. S. M. S. Hosen and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," in *IEEE Access*, vol. 9, pp. 13938-13959, 2021, doi: 10.1109/ACCESS.2021.3051602.

[3] VL Lemieux, "Trusting records: is Blockchain technology the answer?", Records Management Journal. 2016 Jul 18.

[4] C. Heider and A Connelly, "Why Land Administration Matters for Development." World Bank Group 2016,

Available at: http://ieg.worldbankgroup.org/blog/why-land-administrationmatters-development

[5] R Benbunan-Fich, and A. Castellanos, "Digitization of land records: From paper to blockchain" Thirty Ninth International Conference on Information Systems, San Francisco 2018

[6] M. Kalantari et al., "An interoperability toolkit for e-Land administration". *Sustainability and Land Administration Systems, Department of Geomatics, Melbourne*, 2016, pp.213-222.

[7] M. Apostolaki, A. Zohar, & L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies" in 2017 IEEE Symposium on Security and Privacy (SP) pp. 375-392, May 2017.

[8] Patton, Rufford Guy. "The Torrens System of Land Title Registration." Minn. L. Rev. 19 (1934): 519.

[9] https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html

[10] https://www.nswlrs.com.au/

[11] Gaur, N., Desrosiers, L.; Ramakrishna, V.; Novotny, P.; Baset, S.; O'Dowd, A. Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer; Packt Publishing Ltd.: Birmingham, UK, 2018

[12] Bollapragada, V., Khalid, M., & Wainner, S. (2005). IPSec VPN Design. Cisco Press.

[13] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A. D., Ritchey, R. W., & Sharma, S. R. (2005). Guide to IPsec VPNs:.

[14] Elezi, M., & Raufi, B. (2015). Conception of Virtual Private Networks using IPsec suite of protocols, comparative analysis of distributed database queries using different IPsec modes of encryption. Procedia-Social and Behavioral Sciences, 195, 1938-1948.

[15] Kent, S. (2005). IP encapsulating security payload (ESP). Request for Comments: 4303.

Available at: http://tools.ietf.org/html/rfc4303?ref=driverlayer.com/web

[16] Eugster, Patrick T., et al. "Epidemic information dissemination in distributed systems." Computer 37.5 (2004): 60-67.

[17] https://wondernetwork.com/pings/Sydney

Mohammad Arsalan Sheikh received a bachelor's degree in computer science from Delhi University India in 2014 and a master's degree by research in computer science from University of Technology Sydney (UTS) Australia in 2019. He is currently pursuing his PhD studies in computer science from UTS Australia. Mr. Sheikh is also working as a Solution Architect with AWS Australia and has completed several challenging projects successfully. His main area of research is blockchain security and AI. He is a member of IEEE.

Faryal Khattak received a bachelor's degree in business and administration from the Institute of Management Studies Peshawar University Pakistan in 2013 and a master's degree in public administration and policy development

Authorized licensed use limited to: UNIVERSIDADE DE SAO PAULO. Downloaded on September 21,2023 at 00:01:55 UTC from IEEE Xplore. Restrictions apply.

from the Institute of Management Sciences Peshawar University Pakistan in 2016. She is currently pursuing her PhD studies from Department of Business Strategy and Innovation, Griffith University Australia. Her main research interests are land administration and e-governance.

Gul Zameen Khan received a bachelor's degree in computer systems engineering from UET Peshawar Pakistan in 2007 and a master's degree in computer engineering from Hanyang university South Korea in 2011. He completed his PhD in networks and security from Griffith University Australia in 2017. Dr. Khan has worked in the academia, industry, and R&D for 14 years in well reputed organization across different parts of the world.

Farookh Hussain received his PhD degree from Curtin university Australia in 2006. He is highly experienced researcher both in practical industrial research and theoretical research in fog and cloud computing, blockchain and data analytics. Prof. Dr. Hussain is currently working as the head of the discipline software engineering and as a professor in the department of computer science in UTS Australia.

Authorized licensed use limited to: UNIVERSIDADE DE SAO PAULO. Downloaded on September 21,2023 at 00:01:55 UTC from IEEE Xplore. Restrictions apply.