Security Assessment of Blockchains in Heterogenous IoT Networks

Invited Presentation

Jay Jemal
ECE Department
Morgan State University
Baltimore, USA
ahjem1@morgan.edu

Kevin T. Kornegay
ECE Department
Morgan State University
Baltimore, USA
kevin.kornegay@morgan.edu

Abstract: *As Blockchain technology become more understood in recent years and its capability to solve enterprise business use cases become evident, technologist have been exploring Blockchain technology to solve use cases that have been daunting industries for years. Unlike existing technologies, one of the key features of blockchain technology is its unparalleled capability to provide, traceability, accountability and immutable records that can be accessed at any point in time. One application area of interest for blockchain is securing heterogenous networks. This paper explores the security challenges in a heterogonous network of IoT devices and whether blockchain can be a viable solution. Using an experimental approach, we explore the possibility of using blockchain technology to secure IoT devices, validate IoT device transactions, and establish a chain of trust to secure an IoT device mesh network, as well as investigate the plausibility of using immutable transactions for forensic analysis.*

Index Terms—*Accountability, Blockchain, Heterogenous, Immutable, IoT, Network, Security, Tracking, Transparency.*

I. INTRODUCTION

In recent years blockchain technology has attracted great interest from researchers, computer scientists and domain experts in various industries, including banking, finance, real estate, transport, supply chain and healthcare to mention a few industries. This interest initially stemmed from the popularity of Bitcoin [2] and their corresponding platforms, which is a cryptographic currency framework that was the first application of blockchain.

Different Blockchain platforms extend the capabilities of the Bitcoin blockchain by adding support for "smart contracts." Smart contracts are computer programs that directly control exchanges or redistributions of digital assets between two or more parties according to certain rules or agreements established between involved parties. Ethereum's programmable smart contracts enable the development of decentralized apps (DApps) [1], which are autonomous, operated services cryptographically stored on the blockchain that enable direct interaction between end users and providers.

978-1-7281-1151-3/19/$31.00 ©2019 IEEE

This paper focuses on Blockchain technology for securing IoT in Heterogenous network setting.

In this work, we explore the possibility of using Blockchain technology to secure IoT devices, secure IoT device transactions, and to establish a chain of trust platform to secure IoT device mesh network and using transactions on the blockchain for forensic analysis. We will take a multi-phase approach developing different blockchain platform flavors such as NEO, Ethereum and Hyperledger. Public, private and hybrid blockchain platforms are used to test a variety of use case scenarios. In parallel, we will develop IoT mesh network testbed using different IoT devices using Raspberry PIs and ZedBoards. This testbed will be deployed in a blockchain platform for IoT device authentication, secure transaction verification and transaction auditing. Blockchain smart contracts are used to implement different use cases on the testbed to determine the viability of blockchain for IoT security. A business intelligence and data analytics capability will also be implemented to analyze test data such as side channel attacks, brute force and other IoT security vulnerabilities.

The remainder of this paper is organized as follows: Section 2 provides an overview of IoT security challenges in heterogenous networks. Section 3 provides an overview of blockchain and its potential for securing IoT heterogenous network. An experimental approach is presented in Section 3. Blockchain and its role in IoT security is presented in Section 4. A discussion of the challenges and future work is given in Section 5 and outlines future work and references are given in Section 6.

II. IOT IN HETEROGENOUS NETWORK CHALLENGES

The Internet of Things (IoT) is an ecosystem of ever-increasing complexity and bound to be a multi-trillion dollar industry in the near future. According to IoT experts as indicated in Figure 1, it's predicted to reach 6% of global economy by 2020. IoT has been utilized in every industry from life science to entertainment, health and wellness spaces. As IoT devices continue to permeate our day-to-day activities such in home automation, and disaster management, security becomes a paramount concern. The recent security attacks on IoT devices has given criminals countless opportunity to exploit unsecured IoT devices.

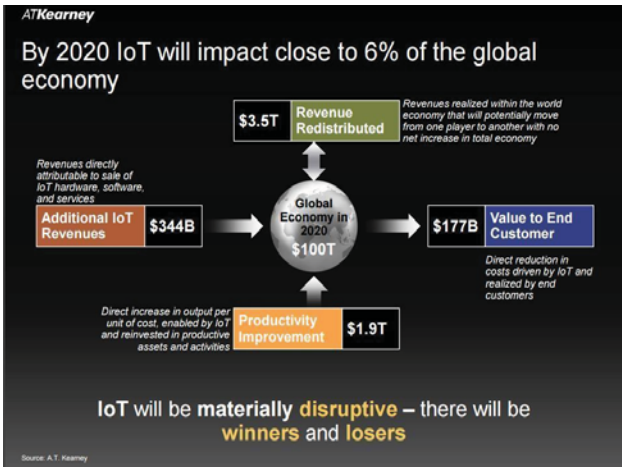

Figure 1 IoT impact prediction for year 2020

IoT security gets exacerbated when the devices are connected in heterogenous networks because cyber attacks can easily propagate with catastrophic consequences. There have been several IoT security solutions currently in place but given the rapid proliferation of IoT devices and complexity resulting from ubiquitous connectivity, new security frameworks are needed.

III. TYPES OF BLOCKCHAIN

A. *Blockchain overview*

This section gives an overview of blockchain and different aspects of blockchain platforms that provide additional support for smart contracts. The blockchain concept was introduced in 2008 by Satoshi Nakamoto and implemented the following year by Nakamoto as a core component of the crypto currency bitcoin, where it currently serves as the public ledger for all transactions on the network [1].

A blockchain is a decentralized computing architecture that maintains a growing list of ordered transactions grouped into blocks that are continually reconciled to keep information up-to-date. Only one block can be added to the blockchain at a time and each block is mathematically verified using cryptography to ensure it follows in sequence from the previous block to maintain consensus across the entire decentralized network. The verification process is also called "mining" or Proof of Work (PoW) [1].

Bitcoin crypto currency was implemented in 2009 as the first blockchain application. In the last few years, blockchain platforms have exploded today with thousands of public and private distributed blockchain applications (a.k.a. Dapps) running on different blockchain platforms.

Although the two dominant blockchain platforms are Ethereum [3] and Hyperledger [4], new platforms have emerged to overcome the deficiencies of older ones in terms of consensus and energy consumption efficiency. Ethereum has improved since its origination by enhancing the consensus algorithm from proof of work to a proof stake. A new blockchain platform called NEO focuses both on the consensus algorithm and digital identity. NEO uses a delegated Byzantine fault tolerant (dBFT) protocol, which is a modification of the standard proof of stake protocol. NEO nodes elect their representatives' nodes that determine NEO's governance model known as Proof of Authority. Those who hold NEO tokens can vote for delegates. These delegates. also called bookkeepers, maintain the network for everyone. Thus, NEO is faster and more efficient with an ability to make more finite decisions. These bookkeepers will have their digital identity known, making NEO much more compliant with national regulations. Thus, in the NEO platform a chain of trust can be established.

B. *Public vs. Private vs. Hybrid Blockchain*

Originally, blockchain was inherently thought to be public as it was originally designed to transact in a decentralized public network where nodes participate in consensus algorithm. However, as blockchain gains noteriety for enterprise applications, it becomes apparent that there are use cases that require permission-based transactions requiring the need for blockchain to get more traction.

In essence public and private blockchains have many similarities [5]:

• Both are decentralized peer-to-peer networks, where each participant maintains a replica of a shared append-only ledger of digitally signed transactions.

• Both maintain the replicas in sync via a protocol referred to as consensus.

• Both provide certain guarantees on the immutability of the ledger, even when some participants are faulty or malicious.

However, there are also significant differences between public and private blockchains.

Public blockchain and known participants

The sole distinction between public and private blockchains is related to who is allowed to participate in the network, execute the consensus protocol and maintenance of the shared ledger [5]. A public blockchain network is completely open and anyone can join and participate in the network. The network typically has an incentivization mechanism to encourage more participants to join the network. Bitcoin is one of the largest public blockchain networks in production today.

One of the drawbacks of a public blockchain is the substantial amount of computational power required to maintain a distributed ledger on a large scale. More specifically, to achieve consensus, each node in a network must solve a complex, resource-intensive cryptographic problem called a proof of work to ensure everyone are in sync.

Another disadvantage is the openness of public blockchain, which implies little to no privacy for transactions and only supports a weak notion of security. Both of these are important considerations for enterprise use cases of blockchain.

Private blockchain and enterprise

A private blockchain network requires an invitation and must be validated by either the network organizer or by a set of rules put in place by the network organizer. Businesses, who set up a private blockchain, will generally set up a permissioned network. This places restrictions on who is allowed to participate in the network, and only in certain transactions. Participants need to obtain an invitation or permission to join. The access control mechanism could vary: existing participants could decide future entrants; a regulatory authority could issue licenses for participation; or a consortium could make the decisions instead. Once an entity has joined the network, it will play a role in maintaining the blockchain in a decentralized manner [5].

Hybrid blockchain and enterprise

As the name suggests, hybrid blockchain lies between the two extremes of public and private and enjoys characteristics of both private and public blockchain. Hybrid blockchain network members or particular dominant entities determine which transactions remain public or be confined to a smaller group of members.

Hybrid blockchains consisting of public and private states of a network ensures that every transaction is private but still verifiable with an immutable record on the public state of blockchain. In its public state, each transaction gets approved by a massive network and is essentially secure and trustworthy. Hence, there is no need for a central governing body or an exhaustive chain of intermediaries for supervision. So, any change to a transaction will undergo an agnate approval process making it next to impossible for a single actor to meddle with the transaction or entries.

While the public state of a hybrid blockchain gives everyone (who has joined the network) equal rights to view, modify and append their consent to a transaction, the identity of transacting parties is never disclosed to all the visible network participants. However, this anonymity is something not acceptable to financial institutions and regulated industries that have strict Know Your Customer (KYC) standards. Moreover, the unrestricted visibility of public state of network exposes all the data to a colossal network—a factor that discords with data confidentiality obligations as well as their business concerns.

This anonymity of public state is successfully combated by the private state of hybrid blockchain—the state that is most suitable for financial institutions. Although it's decentralized, secure, transparent and immutable like its public analogue in most cases, it restricts the rights to view, modify and append/approve transactions to selective members. In simple words, if a network member(s) do not want its transaction data to be visible or accessible without their permission, they can earmark particular rights to view, modify or get into consensus with different members. For example, consider a transaction where Member 1 is allowed to view the payment entries, Member 2 can only edit the specific entries and Member 3 is the one who assents the transaction. [6]

IV. BLOCKCHAIN AND IT'S ROLE IN IOT SECURITY

This section presents the proposed testbed architecture, design approach and functionality of a blockchain for secure IoT platform under development to explore the viability of blockchain technology for securing IoT networks.

Blockchain for IoT security was listed as one of the Nine IoT Predictions for 2019 IEEE publication. According to 2019 IEEE publication: The current centralized architecture of IoT is one of the main reasons for the vulnerability of IoT networks. With billions of devices connected and more to be added, IoT is a big target for cyber-attacks, which makes security extremely important.

Blockchain offers new hope for IoT security for several reasons. First, blockchain is public, everyone participating in the network of nodes of the blockchain network can see the blocks and the transaction stored and approves them, although users can still have private keys to control transactions. Second, blockchain is decentralized, so there is no single authority that can approve the transactions eliminating Single Point of Failure (SPOF) weakness. Third and most importantly, it's secure—the database can only be extended and previous records cannot be changed.

In the coming years manufactures will recognize the benefits of having blockchain technology embedded in all devices and compete for labels like "Blockchain Certified" [7].

According to Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things, IEEE publication [8], researchers have discussed current IoT security issues and how Blockchain address them using Blockchain for IoT security. For authentication and access control, Ethereum can provide authentication and access control to smart devices, services, and the data in IoT, which removes the dependent central parties and gets better efficiency compared to traditional access control models such as role-based access control, context-based access control, and capability-based access control. Users can pre-define access policies in smart contracts and generate several kinds of transactions. [8]

To protect privacy in an IoT system, consortium and private blockchain are usually involved. For entity privacy in IoT, blockchain uses pseudonyms, say public keys, to achieve anonymity. However, this is not strong enough in some real-world applications. Several cryptographic techniques can be combined to achieve full anonymity. Linkable ring signatures are well suited to sign a transaction that can hide the sender's identity in a spontaneous ring. Homomorphic commitments can hide the amount of currency in billing transactions. Zero knowledge proof of knowledge and zero knowledge argument of knowledge are perfect tools to convert any information in a transaction into random ones to restrain any third party from obtaining even one bit of the information. [8]

Blockchain for Secure IoT network possible use cases:

1. Secure IoT device authentication for mesh networks
2. Secure IoT devices transactions for mesh networks
3. Chain of trust IoT mesh network
4. Immutable transaction records for IoT mesh network forensic analysis

High level Architecture design approach

The Blockchain for secure IoT testbed will be designed by using open source software and tools to demonstrate the public, private and hybrid blockchain platforms. A multi-phase development approach will be used to implement different blockchain platforms such as NEO, Ethereum and private and hybrid to evaluate different scenarios. In parallel, we will build an IoT mesh network using different IoT devices such as Raspberry PI and ZedBoards. The testbed will deploy a blockchain platform for device authentication, device secure transaction verification and transaction auditing at any point and time. Business intelligence and data analytics capability will be incorporated to analyze test data from side channel attacks, brute force and other IoT security vulnerabilities. The analysis will help identify IoT security deficiencies; security weakness patterns and will provide remediation recommendations. The testbed architecture is shown below in Figure 2.

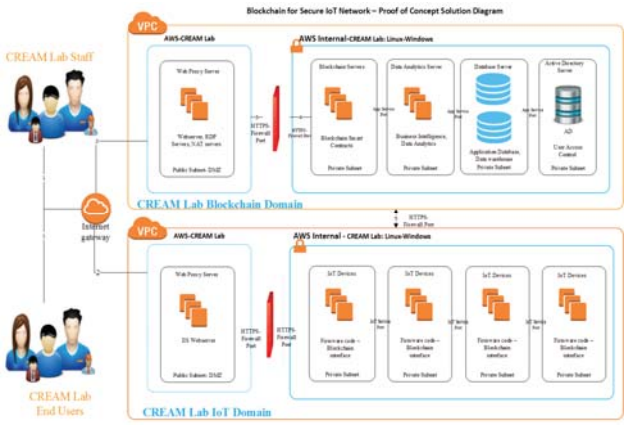

Figure 2 Blockchain for Secure IoT – Proof of Concept Solution diagram

Phase I – NEO platform and Raspberry devices experimental approach

The phase I experiment involves the creation of a virtual private cloud with multiple virtual servers and IoT devices. This implementation includes the NEO Blockchain platform and Raspberry IoT devices. A NEO blockchain a pub/sub code written in the python programming language, neo smart contract, and Web app written in Node.js are deployed on a Linux virtual machine. A windows server for Business Analytics was deployed for analysis and reporting. A collection of Raspberry IoT devices are connected to form a mesh network. The python programing language-based firmware code was deployed on the Raspberry IoT devices to respond to commands when executed from the Neo blockchain smart contract. The Raspberry IoT devices and contracts are managed from the Neo web app portal. A user who wants to execute a transaction authenticates to the Neo blockchain testbed through Neo wallet, once the user account and private key are verified then transactions can be sent to the Raspberry IoT devices, where the devices perform tasks. For phase II, smart contracts that execute critical IoT functionalities will be supported. Test data is captured in a database for display by the business intelligence dashboard.

V. Discussion And Future work

Challenges of Blockchain for IoT security network proposed solution

As discussed in the previous sections, blockchain technology has tremendous potential for solving IoT network security use cases. However, it's not without it's challenges, to mention a few:

a) Blockchain is still relatively new and there are a lot of skeptics
b) Stake stakeholders are still under the impression that it is associated with Crypto currency and don't see the value beyond financial industry applications
c) Blockchain platforms are evolving at a rapid pace with different technology stacks and tools
d) There is not enough technologist who can push blockchain to business team and articulate its benefits
e) Enterprises have already invested significant amount of money upgrading their platform to latest technologies and they demand strong cost/benefit analysis to migrate the costs associated with blockchain technology platforms
f) There are not enough blockchain technical resources to support the new platform cost effective solutions

Future work

The Blockchain is a promising technology for securing IoT network. We will continue to investigate different use cases by with different blockchain flavors (NEO, Ethereum and Hyperledger) and IoT devices. We will use a systematic approach and categorize our findings using data analytics. Furthermore, we will use big data analytics to preform predictive analysis using what-if analysis to take advantage of AI models that can be applied to enhance the security IoT device networks.

VI. References

[1] Johnston et al. 2014 - David Johnston, Sam Onat Yilmaz, Jeremy Kandah, Nikos Bentenitis, Farzad Hashemi, Ron Gross, Shawn Wilkinson, and Steven Mason. 2014. The General Theory of Decentralized Applications, DApps. GitHub, June 9 (2014)
[2] https://denominatorgroup.org/blockchain
[3] https://www.ethereum.org/
[4] https://www.hyperledger.org/
[5] https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/
[6] https://aws.amazon.com/blockchain/templates/
[7] https://iot.ieee.org/newsletter/november-2018/nine-iot-predictions-for-2019
[8] Yong Yu, Yannan Li, Junfeng Tian and Jianwei Liu. Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. IEEE Wireless Communications, Year: 2018, Volume: 25, Issue: 6, Pages: 12 – 18, IEEE Journals & Magazines