Security assessment of blockchain-as-a-service (BaaS) platforms

Victor Akinwande
College of Engineering
Carnegie Mellon University, Africa
Kigali, Rwanda
vakinwande@cmu.edu

I. Introduction

Popularized by bitcoin [1] and with promises to disrupt several industries, blockchain is beginning to take the world by storm. Many big technology companies are moving swiftly to tap into this space in a bid to become market leaders. Their general approach being to commoditize blockchain by exposing a set of APIs and providing infrastructure that makes it easy for anyone to build a blockchain application and abstracts many of the technical details. This service approach is known as blockchain-as-a-service (BaaS).

Abstraction is crucial to ease of use. However, with no standard or protocol to guide implementation of BaaS platforms or even blockchain platforms, the various vendors implement as they choose. Understanding the technicalities, and security issues associated with BaaS is key. The major focus of this project is to assess the unique security threats and gains BaaS pose compared to generalized Platform-as-a-Service (PaaS) platforms given the structure of the data layer and implicit cryptography. Essentially, the research question is – what PaaS security concerns should cloud providers and customers not be worried about when providing or adopting a BaaS platform respectively? The motivation of this project is the increasing interest in blockchain technology.

II. Definitions

A. Blockchain

Blockchain in a general sense is a distributed public ledger - and stands as a trustless proof mechanism in which the architecture allows for disintermediation and decentralization of transactions [2]. Each transaction in the public ledger is verified by a consensus of a majority of the participants in the system, and is permanently recorded. Blockchain was developed first for bitcoin cryptocurrency.

B. Infrastructure-as-a-Service (IaaS)

IaaS is the delivery of hardware resources including storage, compute, and network as well as the associated software such as operating systems, virtualization, and a file system, as a service.

C. Platform-as-a-Service (PaaS)

Platform-as-a-Service solutions provide an application or development platform in which users can create their own application that would run on a cloud provider's infrastructure [10]. In other words, layered services atop IaaS simply exposing software and abstracting the underlying hardware.

D. Blockchain-as-a-Service

Blockchain-as-a-service (BaaS) is a "category of cloud computing services that provides a platform allowing customers to develop, run, and manage blockchain applications without the complexity of building and maintaining the infrastructure cryptographic requirements typically associated with developing and launching a blockchain application" [6].

III. Importance and Prior Work

Following the introduction of the bitcoin blockchain in 2008 [1], we have seen proposals of a wide scope of applications of the technology – ranging from business to business (B2B) contracts, separation of asset ownership, supply chain and as asset depositories among many others [9]. Since 2012, the trend – as determined by the frequency of search queries containing blockchain – has consistently increased.

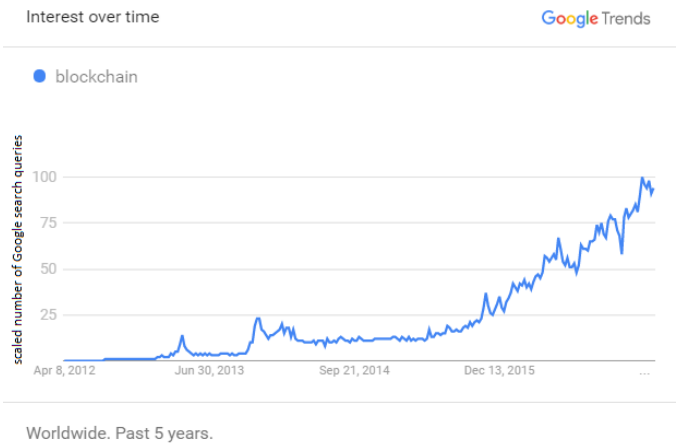

Fig. 1. Trend of interest in "blockchain". Source: Google trends

Organizations are beginning to look to the blockchain technology to tackle business challenges. However, leveraging

the technology to build applications requires a good knowledge of cryptographic engineering, which can be daunting and a scarce skillset in the labor market. This presents an opportunity for cloud providers to democratize the development of blockchain solutions by exposing a set of APIs that abstracts the complex cryptography and architecture needed. However, with no standard or protocol to guide implementation of BaaS platforms, the various vendors implement as they choose. While providing PaaS present its own security challenges, cloud providers looking to add BaaS need to realize that there are disparities in the threats, security challenges and limitations. As such, this project is crucial as it assesses the unique limitations, threats, and security concerns to deploying and maintaining a BaaS platform.

BaaS providers allow customers to provision a fully configured blockchain network topology in minutes. Infrastructure to run a specific implementation of the blockchain protocol is automatically provided. These implementations also called 'Apps' are usually tailored implementations of blockchain and distributed ledgers by a third-party vendor. An 'app' would typically provide majority of the abstractions key to deploying a blockchain application with features such as party identity abstraction, transaction linkage, transaction scripts, transaction distribution, blockchain – the standard on how each node stores transaction data, also called distributed ledger, and a means of distributed consensus [11]. These features are foundational. However, as mentioned before now, vendors implement as they choose. Every implementation of blockchain is usually slightly different and tailored to a specific use case, and it is out of the scope of this work to present these differences. As at the time of this writing, Azure provides the ability to deploy an Ethereum Consortium blockchain[1], a Quorum blockchain[2]– a fork of Ethereum tailored for financial transactions, Chain core blockchain[3], Corda[4], and a Strato blockchain[5] – another Ethereum based blockchain. IBM on the other hand, only provides the ability to deploy a blockchain based on Hyperledger fabric – an open source implementation part of the Linux Foundation's Hyperledger Project[5].

The bitcoin cryptocurrency is a system for electronic transactions without relying on trust while ensuring anonymity based on the blockchain [1]. A peer-to-peer network using proof-of-work records a public history of transactions leveraging a distributed consensus mechanism through voting with participant's CPU power where expressing their acceptance of valid blocks is done by working on extending them and rejecting invalid blocks by refusing to work on them.

With regards to the application of blockchain technology, Zyskind and Nathan [4], describe a decentralized personal data management system with focus on giving control to users over their data. The authors implement a protocol that leverages blockchain to act as an automated access-control manager without requiring trust in a third party.

Looking at the threats, Bradbury highlights the theoretical attacks to the most popular blockchain application - bitcoin. The 51% attack allows an attacker (pool of block miners or a single miner) with 51% of the hash rate, to theoretically be able to dominate which transactions are entered in the blockchain. A double spend attack involves communicating one transaction to a merchant and yet communicating a different transaction that spends the same coin that was first to eventually make it into the blockchain. Denial of service attacks can be used to compromise the network, and there are several possible kinds of attacks. One involves 'dust' transactions – very small transactions that send hardly any bitcoins, but which take up space in the blockchain.

With a rapidly increasing number of research done with related to blockchain, Yli-Huumo et al [3]. review relevant research on Blockchain technology with an objective to understand the current research topics, challenges and future directions regarding blockchain technology from the technical perspective. The paper showed that 80% of research in Blockchain is focused on revealing and improving limitations of Blockchain from privacy and security perspectives.

Lastly, Hashizume et al [8]. provide a categorization of security issues for Cloud Computing focused in the so-called SPI model (SaaS, PaaS and IaaS), identifying the main vulnerabilities and threats in this kind of systems.

IV. Methodology

The approach to answering the research question of this project involves a lot of literature review in the cloud computing domain and also in the blockchain domain. Existing and known security concerns, threats and limitations of PaaS would be juxtaposed with the properties of the blockchain technology to determine the extent to which they would applicable in BaaS.

Security would be categorized as CSP (cloud service provider) related vulnerabilities which represent traditional security concerns, those involving computer and network attacks, availability, and third party data control, which arises in cloud computing because user data is managed by the cloud provider and may potentially be exposed to malicious third parties.

V. Results And Discussion

A. *Cloud Resources in BaaS*

Before discussing some of the security issues it is important to highlight what cloud resources are typically utilized in a blockchain network deployed on the cloud and their configuration.

[1] https://www.ethereum.org/

[2] https://www.jpmorgan.com/country/US/EN/Quorum

[3] https://chain.com/technology/

[4] http://www.r3cev.com/

[5] http://blockapps.net/

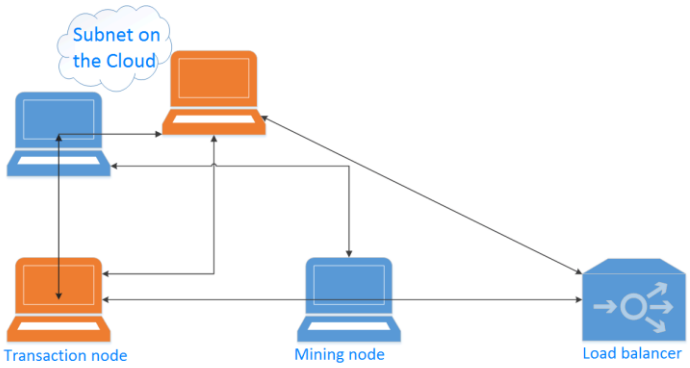

Fig. 2. Basic architectural overview of a blockchain network

- Transaction and Mining Nodes (compute) – Transaction nodes are used to execute smart contracts or submit transaction in the blockchain network, and mining nodes record transactions with the network and communicate with one another in the same subnet to come to a consensus on the underlying distributed ledger.
- Load balancer (compute) – The load balancer (LB) helps to maintain high availability, distributing requests appropriately among the transaction nodes in an availability set.
- Network interfaces (network) – The network interfaces provide a means for communication within the virtual network and between the customer implemented client and the transaction nodes or LB. The LB exposes an RPC, SSH or HTTP endpoint allowing requests to be submitted and executed in the network.
- Redundant storage (storage) – There is also a need for storage of the blockchain. CSPs typically provide – as seen in Azure, and IBM either locally, or geographically redundant storage needed particularly by the mining nodes to store the distributed ledger.

B. *Issues*

1) CSP vulnerabilities

CSP espionage and object vulnerability – Malicious providers and attacks leading to a host being breached has an impact on the privacy and integrity of the user's objects (pieces of data uploaded to a CSP's cloud). The general solution to this issue is homomorphic encryption, however this can be computationally expensive and not feasible for a genre of applications or in a resource constrained setup. With the blockchain shared data layer, the risk is higher. However, raw data is encrypted with the keys not stored on the nodes in the cases of on-blockchain data store implementations. This presents an added advantage of protection against attacks on objects stored by a user.

Transitions and constraints on languages – Solidity[6], and Truffle[7] are a couple of development tools that have recently been invented to make writing smart contracts in blockchain networks easier. Apart from the fact that the blockchain implementation and platform is done by vendors at will, the ecosystem of tools needed to develop and deploy an application leveraging BaaS is entirely developed by third parties – client interfaces and applications like geth and metamask are attack vectors to consider when procuring a BaaS offering.

2) Availability

Denial of service (DOS) – In PaaS environments, policy enforcement points (PEPs) intercept users requests to a resource and enforces authorization decisions. PEPs pose a high security risk as an exposure to a DOS attack can lead to dire consequences. With Byzantine fault tolerance, and consensus models a central part of blockchain implementations, BaaS provides to an extra safety net in dealing with DOS attacks.

Scalability and Centralization – In the blockchain world, performance and scalability as more nodes are added to the blockchain network is very important. The cloud excels in this regard. Providing high availability guarantees and the ability to scale seamlessly. However, the physical centralization of resources in BaaS as its currently being done poses a significant security risk. While CSPs, particularly azure, provide the ability to create multi-member cross-organizational blockchain networks these networks are still within the domain of one CSP. Unlike PaaS, a multi-provider configuration for BaaS is not available thus posing a risk of vendor lock-in as well as threats attributed to physically centralized systems.

3) Data related issues

Privacy and identity management – Sharing information comes with trade-offs. Exchanging attributes and verifying claims without being dependent on a central authority is a challenge in PaaS. Bringing an added advantage of increased transparency, permissioned blockchain networks can allow users to perform transaction verification while maintaining anonymity however processing transactions still requires some form verification from a trusted authority.

Summarily, the results of this study as discussed in this section is shown in table I below. Security concerns that exist in each service model is indicated as yes, or no if otherwise. In cases where the concern is partially mitigated by an extra security feature, an extra security option is assigned.

TABLE I. SUMMARY OF SECURITY CONCERNS

Security concern	PaaS	BaaS
CSP espionage	Yes	No
Object vulnerability	Yes	Extra security

[6] solidity.readthedocs.io

[7] truffleframework.co

Transitions	No	Yes
Language constraints	No	Yes
DOS	Yes	Extra security
Scalability	No	No
Centralization	No	Yes
Privacy	Yes	Extra security
Identity management	Yes	No

Other security issues that needs to be looked at carefully when deploying BaaS as a customer both from the vendor and the CSP ends include attacks to the blockchain memory, insecure APIs, information disclosure during sharing, data owning, and identity guessing attack in unpermissoned blockchains to mention a few.

VI. Conclusion

Setting up a blockchain network on the cloud is easy. Taking less than 10 minutes in some cases with the configuration and implementation of the cryptographic and communication components setup automatically. This of course reduces the barrier to entry for an organization looking to leverage blockchain for their business. However, as with the PaaS model, security issues still exist and needs to be taken seriously into consideration when choosing a CSP or blockchain vendor. A future research endeavor could entail looking at the specific security issues that are yet to be clearly addressed in each CSP or vendor implementation and also simulating a production environment to observe the limitation of the various implementation provider services.

References

[1] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*. bitcoin.org whitepaper, 2008

[2] Swan, M. *Blockchain*: *Blueprint for a new economy.* " O'Reilly Media, Inc.", 2015

[3] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. "*Where Is Current Research on Blockchain Technology?—A Systematic Review"*. Public Library of Science", (PLOS) ONE, 11(10), e0163477, 2016

[4] Zyskind, G., & Nathan, O. (2015, May). *Decentralizing privacy: Using blockchain to protect personal data*, In Security and Privacy Workshops (SPW) IEEE, May 2015 (pp. 180-184)

[5] Bradbury, D. (2013). "The problem with Bitcoin". Computer Fraud & Security, 2013 (pp 5-8).

[6] "Platform as a service." (2017, February 28). In Wikipedia, The Free Encyclopedia. Retrieved 15:14, March 22, 2017, from https://en.wikipedia.org/w/index.php?title=Platform_as_a_service&oldid=767853950

[7] "Consensus - Bitcoin Glossary". Bitcoin.org. Retrieved 4 April 2017, from https://bitcoin.org/en/glossary/consensus

[8] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B *An analysis of security issues for cloud computing*. Journal of Internet Services and Applications, 4(1), 5, 2013.

[9] "Use Cases — hyperledger-fabricdocs master documentation", Hyperledger-fabric.readthedocs.io, 2017. [Online]. Available: http://hyperledger-fabric.readthedocs.io/en/latest/biz/usecases.html#. [Accessed: 20- Apr- 2017].

[10] Shawish, Ahmed, and Maria Salama. "Cloud computing: paradigms and technologies." *Inter-cooperative collective intelligence: Techniques and applications*. Springer Berlin Heidelberg, 39-67 2014.

[11] "Eight Key Features of Blockchain and Distributed Ledgers Explained", dtcc.com, 2016. [Online]. Available: http://www.dtcc.com/news/2016/february/17/eight-key-features-of-blockchain-and-distributed-ledgers-explained [Accessed: 24-Apr-2017].