GBBC Global Blockchain Business Council

Open Learning Forum

Security Services Using Blockchains: A State of the Art Survey

Tara Salman; Maede Zolanvari; Aiman Erbad; Raj Jain; and Mohammed Samaka
Washington University in St. Louis; Qatar University
Date Published: 8/7/2018

Executive Summary written by GBBC

Encryption and Authentication Services

Proper encryption and authentication can be achieved using public key cryptography, in which entities have access to both public and private information. The combination of public and private keys allows entities in a network to verify information coming from other entities. Entities sign a message with their unique private key; other entities can then use the entity's public key to verify the message's legitimacy.

The researchers state that authentication and encryption "are the most critical services in almost all of the current network applications." The system of encryption and authentication using public keys is known as public key infrastructure (PKI). Problems arise in PKI because it is centralized under a single trusted entity. Network users must trust that the entity controlling the PKI is honest and has not been compromised.

Blockchain can solve this problem by distributing and recording all events for PKI. Using blockchain, network users will not have to trust a single entity to control public keys; they will be able to ensure the legitimacy of keys themselves. The paper presents numerous blockchain-based PKI solutions, all of which improve upon traditional PKI solutions by implementing distributed, trustless blockchain ledgers.

Privacy Services

Privacy services enable a user to control their data on a network by maintaining an access control list (ACL). ACLs allow users to set rules on who can and cannot view their confidential data. One need only look at the controversies regarding the use, sale, and distribution of personal data by social media and genetic testing companies to understand the importance of data privacy. The increasing ubiquity of cloud computing and IoT devices further demonstrates the need for enhanced data privacy.

Existing data privacy services are burdensome, with complex cryptography that limits scalability. They tend to be somewhat murky on who owns the data, as the "owner generally is the party that decides the access control rules for the data." Finally, existing services do not factor in the lifecycle of data, as the researchers advocate for a framework that can "identify the phases, define the privacy requirement, and allow flexibility in the lifecycle changes."

Blockchain-based data privacy solutions would place a blockchain on top of user data, which would allow users to set ACLs with smart contracts or special blockchain management transactions. This would create a permissioned blockchain in which users have total control over their data and how it is used. While most of the solutions presented in the paper need to improve scalability, blockchain-enabled data privacy is an exciting prospect for consumers who would like to take back control of their personal information.

Data Provenance

Data provenance is the metadata that is created when information in a cloud computing system is changed, added, or deleted. For more information on data provenance and how blockchain can improve it, please see the GBBC's Executive Summary of ProvChain.

Integrity Assurance

Integrity assurance is another critical piece of the overall security puzzle; it ensures that data is not compromised, corrupted, or altered. End-to-end integrity assurance provides users with peace of mind, as they can be sure the data they are using is valid.

Traditionally, networks have provided integrity assurance using public key cryptography, in which unauthorized users are unable to alter data that is signed with a private key. This system works well until the private key is exposed, after which it becomes incredibly difficult to track the unauthorized user and determine which data is compromised. As with the other traditional security services, it also suffers for having a single point of failure.

The architecture of blockchain technology solves many of these problems outright: the blockchain records every transaction and automatically verifies the integrity of transactions. By verifying each transaction, blockchain has built-in integrity assurance, and with records of each transaction it becomes easy to track and identify an intruder.

Conclusion

Blockchain technology clearly has a significant role to play in the improvement of security services. Depending on its architecture, it does have some drawbacks: lack of true anonymity, computing power and time requirements, high communication overhead, and scalability limitations. The researchers suggest user anonymity and scalability are the two most difficult challenges to the application of blockchain technology. They also estimate that blockchain technology is not yet applicable for security services for "real-time and delay-sensitive applications." Overall, blockchain technology shows great promise for security services, but future research is necessary before it becomes a must-have for sensitive and fast-moving networks.