Security and Privacy in Blockchain Environments

Article · June 2017

CITATIONS
0

READS
248

2 authors, including:

Matteo Cagnazzo
Westfälische Hochschule
12 PUBLICATIONS **7** CITATIONS

SEE PROFILE

Security and Privacy in Blockchain Environments

The blockchain is currently one of the most-hyped technologies. In this short article we will try to sho, where current downsides in blockchain security and privacy are. We will explore how security and privacy can be enhanced by blockchain technology and outline the challenges ahead.

Problems of Blockchain Security/Privacy

Transactions are globally published and are not encrypted in most applications. If this data is personal data, for example “medical or financial data”, this leads to regulatory and legal problems, especially in Germany. One solution is to store only encrypted data in the blockchain, which leads to another problem: If the key to decrypt specific information is lost, the data may not be recovered accurately. Furthermore, if a key is stolen and published, all the data is forever decrypted in the blockchain since the data cannot be altered. However, blockchain can also help to improve defensive cybersecurity strategies, especially in terms of identity and access:

MITM Attacks

One attack scheme for man-in-the-middle (MITM) attacks is to get the Certificate Authority (CA) to provide the user with forged public keys (Public-Key Substitution MITM attack). This can lead to the decryption of sensitive information. In a blockchain approach whereby users put their public keys in published blocks, the information is distributed over the participating nodes with links to previous and following blocks. This makes the public key immutable and it becomes harder for attackers to publish fake keys. Furthermore, the single point of failure, the CA, is also distributed, meaning it is harder to bring this service down. Projects that try to solve this problem are: okTurtles[1]

Data Tampering

Since every transaction is signed and distributed over all blockchain nodes, it is practically impossible to manipulate data without the network knowing about it. How do you prove that Germany won the World Cup 2014? You do not have to prove it, since it is general knowledge that distributed across the people. In health care, the blockchain could be used to create immutable audit trails, maintain the integrity of health trials, and ensure the integrity of patient data shared across different medical environments.

DDoS Attacks

If DNS systems were based on blockchain technology, attacks like the one from Mirai botnet (https://www.dotmagazine.online/issues/security/gridlock-DDos) would be harder to successfully complete. Such a system would provide transparency and security. The DNS infrastructure could not be targeted if it was a distributed system, since the data is distributed and the data entries cannot be tampered with, due tothe append-only nature of the blockchain. The project okTurtle is also realizing a blockchain-based DNS service[1].

Privacy

The blockchain technology is a great example for the unrelatedness of security (at least in terms of immutability) and privacy. Whilst it is possible to design an immutable, tamper-resistant transaction, this transaction can be seen throughout all of the nodes on the network. The most promising research on privacy (or private transactions) for blockchain technology is currently zkSNARKs, which are implemented by zCash and Ethereum (zCash on Ethereum). The combination of both technologies makes it possible to implement anonymous payments, blind auctions, and voting systems. Since the mechanisms behind zk-Snarks are not trivial, they cannot be described in this short article. Please see [2][3] for further information.

Challenges

Even though privacy enhancing technologies are deployed, they still produce metadata. Statistical analysis will reveal “some” information, even if the data itself is encrypted, making, e.g., pattern recognition possible. Furthermore, scalability is an emerging challenge, since the consensus process is currently too expensive. If currency or any other value is traded on a blockchain-based application, a much higher transaction speed is needed. Ethereum is currently capable of 2.8 transactions per second, while bitcoin is capable of approximately 3.2 transactions per second. It takes so long because of the complex consensus process for each transaction (currently proof of work or proof of stake)[4][5]. Another attack to keep in mind is the 51%-attack or “Majority Hash Rate Attack”. If an organization or individual has 51% of the hash power, the attacker can reverse transactions he sent, prevent transactions from gaining confirmations, and prevent other miners from mining[6].

Conclusion

Cybersecurity threats emerge every day, while older threats still linger around and wait to be exploited once again. Blockchain technology will not be the holy grail of cybersecurity, but it is a powerful tool which can help to harden systems. Blockchain plays its strengths very well; if the system which it is disrupting is a centralized system with a single point of failure. If higher transaction speeds are possible, blockchain is a technology with use cases ranging from smart grids over the Internet of Things to a globally deployed and used currency system and smart contracts[7].

Bibliography

[1] https://github.com/okTurtles/dnschain
[2] https://blog.ethereum.org/2017/01/19/update-integrating-zcash-ethereum/
[3] http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf
[4] https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
[5] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.
[6] Rosenfeld, Meni. "Analysis of hashrate-based double spending." *arXiv preprint arXiv:1402.2009* (2014).
[7] Kosba, Ahmed, et al. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts." *Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE, 2016.