Solving Internet's Weak Link for Blockchain and IoT Applications

Title	Solving Internet's Weak Link for Blockchain and IoT Applications
Publication Type	Conference Paper
Year of Publication	2018
Authors	Chakraborty, Saurav, Thomas, Drew, DeHart, Joanathan, Saralaya, Kishan, Tadepalli, Prabhakar, Narendra, Siva G.
Conference Name	Proceedings of the 1st ACM/EIGSCC Symposium on Smart Cities and Communities
Publisher	ACM
Conference Location	New York, NY, USA
ISBN Number	978-1-4503-5786-9
Keywords	authentication, blockchain, cryptography, Decentralized security, Digital signing, Encryption, hardware security, Human Behavior, Internet of Things, IoT, Key storage, Metrics, policy-based governance, Private keys, pubcrawl, resilience, SECP256K1, security weaknesses
Abstract	Blockchain normalizes applications that run on the internet through the standardization of decentralized data structure, computational requirements and trust in transactions. This new standard has now spawned hundreds of legitimate internet applications in addition to the cryptocurrency revolution. This next frontier that standardizes internet applications will dramatically increase productivity to levels never seen before, especially when applied to Internet of Things (IoT) applications. The blockchain framework relies on cryptographic private keys to sign digital data as its foundational principle. Without the security of private keys to sign data blocks, there can be no trust in blockchain. Central storage of these keys for managing IoT machines and users, while convenient to implement, will be highly detrimental to the assumed safety and security of this next frontier. In this paper, we will introduce decentralized and device agnostic cryptographic signing solutions suitable for securing users and machines in blockchain and IoT applications.
URL	http://doi.acm.org/10.1145/3236461.3241976
DOI	10.1145/3236461.3241976
Citation Key	chakraborty_solving_2018

security weaknesses SECP256K1 resilience pubcrawl Private keys policy-based governance Metrics Key storage IoT Internet of Things Human behavior Hardware Security encryption Digital signing Decentralized Security Cryptography blockchain