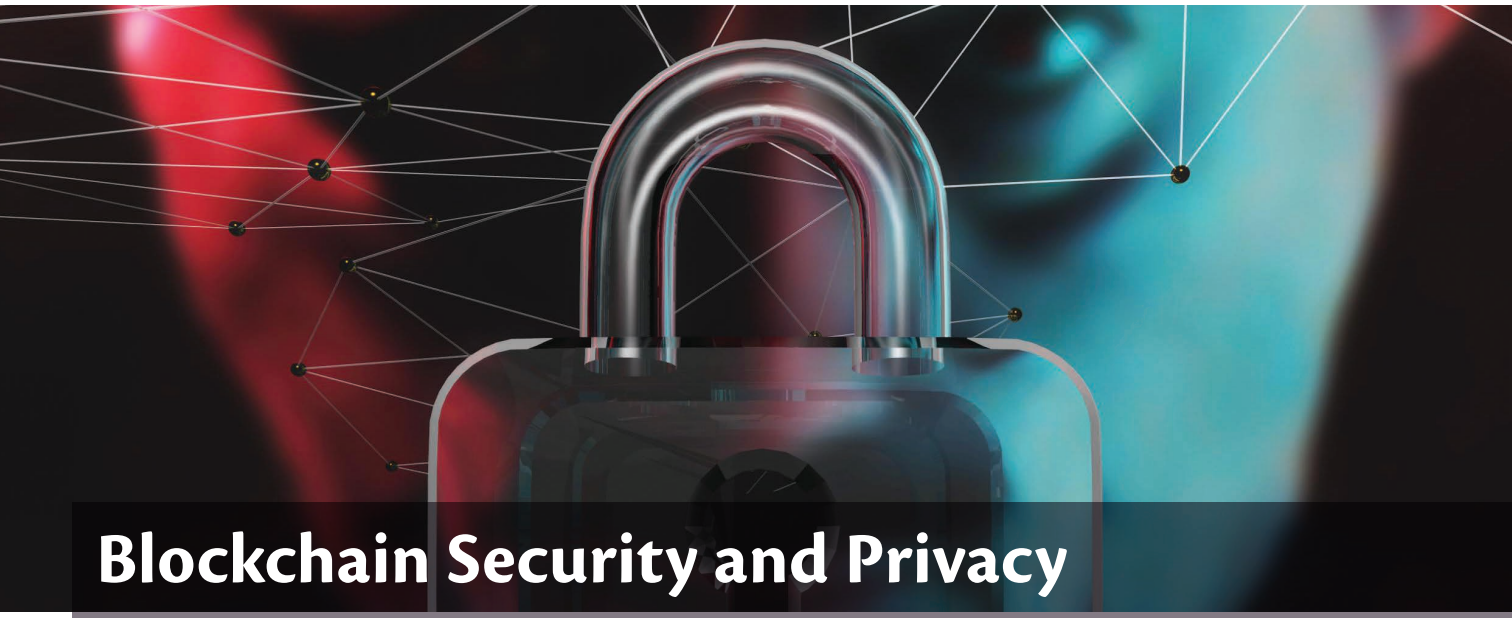

Blockchain Security and Privacy

Ghassan Karame | NEC Laboratories Europe
Srdjan Capkun | ETH Zurich

The blockchain emerged as a novel distributed consensus scheme that allows transactions, and any other data, to be securely stored and verified without the need of any centralized authority. For some time, the notion of blockchain was tightly coupled with a now well-known proof-of-work hash-based mechanism of Bitcoin. Today, there are more than a hundred alternate blockchains: some are simple variants of Bitcoin, whereas others significantly differ in their design as well as provide different functional and security guarantees. This shows that the research community is in search of a simple, scalable, and deployable blockchain technology. Various reports further point to an increased interest in the use of blockchains across many applications and to a significant investment in the development of blockchains by different industries. It is expected that the blockchain will induce considerable change to a large number of systems and businesses.

Distributed trust and therefore security and privacy are at the core of the blockchain technologies, and have the potential to either make them a success or cause them to fail.

This special issue aims at collecting the most relevant ongoing research efforts in blockchain security and privacy. We are very grateful to this community, especially for its vivacity and vast participation.

The issue starts with an introductory article written by Sarah Meiklejohn, "Top Ten Obstacles along Distributed Ledgers' Path to Adoption," which presents hindrances preventing the widespread adoption of the blockchain technology by the community and outlines potential avenues of research.

In their article, "A First Look at Identity Management Schemes on the Blockchain," Paul Dunphy and Fabien A.P. Petitcolas discuss a number of identity management schemes based on the blockchain and evaluate three schemes—uPort, ShoCard, and Sovrin—using a novel framework.

In "Tyranny of the Majority: On the (Im)possibility of Correctness of Smart Contracts," Lin Chen and colleagues tackle the correctness of smart contracts in the blockchain. More

1540-7993/18/$33.00 © 2018 IEEE Copublished by the IEEE Computer and Reliability Societies

specifically, they analyze consensus of smart contract results in decentralized systems and show that the correct execution results of smart contracts are not always accepted as consensus.

In "Blockchain Access Privacy: Challenges and Directions," Ryan Henry and colleagues discuss another important problem in the blockchain: privacy. They show that Tor offers limited privacy and illustrate the need for research "beyond Tor" to tackle important access privacy issues in contemporary blockchains.

"When the 'Crypto' in Cryptocurrencies Breaks: Bitcoin Security under Broken Primitives," by Ilias Giechaskiel and colleagues, presents an analysis of the effect of broken primitives on Bitcoin. This analysis leads to several suggestions for the Bitcoin migration plans and insights for other cryptocurrencies in case of weakened cryptographic primitives.

Finally, Rachid El Bansarkhani and colleagues extend this analysis in their article "PQChain: Strategic Design Decisions for Distributed Ledger Technologies against Future Threats," suggesting paths for a secure instantiation of the blockchain protocol, taking into account the presence of large-scale quantum computers and potential future attacks against the underlying hash functions.

We hope you enjoy this special issue! ■

Ghassan Karame received his MS in information networking from Carnegie Mellon University (CMU) in December 2006 and his PhD in computer science from ETH Zurich, Switzerland, in 2011. Between 2011 and 2012, he worked as a postdoctoral researcher at the Institute of Information Security of ETH Zurich. Since 2012, Karame joined NEC Laboratories Europe where he is currently the manager and chief researcher of the Security group. Karame is interested in all aspects of security and privacy with a focus on cloud security, SDN/network security, and Bitcoin/blockchain security. He is a member of IEEE and ACM and is the author of several papers and patent applications. More information can be found at http://ghassankarame.com. Contact him at ghassan@karame.org.

Srdjan Capkun is a full professor in the Department of Computer Science, ETH Zurich, and director of the Zurich Information Security and Privacy Center (ZISC). He was born in Split, Croatia. He received his Dipl.Ing. degree in electrical engineering/computer science from the University of Split in 1998 and his PhD in communication systems from EPFL in 2004. Prior to joining ETH Zurich in 2006, he was a postdoctoral researcher in the Networked & Embedded Systems Laboratory (NESL), University of California, Los Angeles, and an assistant professor in the Informatics and Mathematical Modelling Department, Technical University of Denmark (DTU). His research interests are in system and network security. One of his main focus areas is wireless security. He is a co-founder of 3db Access, a spin-off focusing on secure proximity-based access control. Contact him at capkuns@inf.ethz.ch.