RUB Faculty of Computer Science

www.informatik.rub.de

RUHR UNIVERSITÄT BOCHUM RUB

THE FACULTY OF COMPUTER SCIENCE CORDIALLY INVITES YOU

– Inaugural Lecture –

Prof. Dr. Ghassan Karame
Professorship for Information Security

"Reflections on a Decade of Blockchain Security Research"

Abstract

With the publication of the Bitcoin whitepaper in 2008, and the subsequent delivery of a corresponding open-source implementation two months later, a new class of "decentralized" currency was forged. Unlike previous electronic cash proposals, Bitcoin was rather straightforward, explained in a concise whitepaper, and relied on basic cryptographic constructs, such as hash functions and digital signatures. The working implementation confirmed that the system is practically feasible and scales to a large number of nodes.

Motivated by the wide success of Bitcoin, recent years have witnessed the surge of a considerable number of alternative blockchain proposals such as Dogecoin, Namecoin, Ripple, Ethereum, Corda, and Hyperledger Fabric, Chain, among others. Currently, the blockchain is rapidly gaining ground as a key technology, especially in the financial and retail sectors. Beyond these sectors, a number of practitioners further speculate that blockchains can change the way we see online applications today.

The rapid adoption of the blockchain technology was however only skeptically received by the research community. Researchers criticized the lack of governance in Bitcoin, the underlying economic model, and the security and privacy provisions of the system. The latter point received considerable attention in the security community; the literature features a sheer number of reported vulnerabilities and improvement suggestions.

In this talk, I plan to overview a number of security challenges pertaining to existing blockchains—effectively capturing almost a decade of my research spanning all layers of modern blockchain platforms. Namely, I will discuss the various security provisions of the popular and widely-deployed Proof-of-Work blockchains and outline effective countermeasures that we proposed to enhance the security of the system – some of which have already been incorporated in the official Bitcoin software and are currently being used by millions of users around the globe. Moreover, I plan to discuss the performance limitations of existing consensus protocols and discuss possible solutions that achieve low latency and high throughput without compromising the security of the system. Finally, I will outline the challenges in securing smart contracts and discuss our latest proposals to automatically detect and patch smart contract vulnerabilities.

When? 14th of June 2022, 02:00 PM

Where? Open Space of building MC (room 0.34, ground floor)

Anyone interested is warmly welcome to the lecture and the get-together afterwards.
Please register via https://informatik.rub.de/news/inaugural-lecture-ghassan-karame/.
We are looking forward to your participation!