Stanford Blockchain Protocol Analysis and Security Engineering 2018

Introduction & Overview

Byron Gibson

Contents

I. Introduction & Overview

Thank you all for joining us today. I'll provide a brief introduction to the main problems this conference aims to address, an overview of some of the presentation themes, and then conclude with a few thank you's.

What is "security" in a distributed ledger context?

For anyone here who may be new to the blockchain industry, it is worth clarifying what we mean when we talk about security in the blockchain context. It essentially refers to three design goals:

1. Data integrity: The blockchain ledger's transaction history is immutable and cannot be rewritten by anyone, "bad" or "good". It can be appended to by design, perhaps with new data taking precedence over old, but not rewritten or overwritten.

2. Fiduciary integrity: Any on-chain currency, token/s or other resources cannot be written into the ledger as having been double-spent. Eg, digital forgery and counterfeiting of the critical resources of the system are impossible. Further, the protocol ensures the fungibility of any native currency instrument.

3. System integrity: Attempts to prevent or interrupt the protocol from functioning normally and correctly are difficult and prohibitively expensive, if not impossible.

The Challenge

Blockchains integrate two of the most sensitive areas of computer science more-so than ever before - cryptography and distributed systems. The security engineering problem is thus:

1. They are subject to active opposition, rather than merely the laws of nature.
2. They have an inherent zero-defect requirement, because a defect of any severity can result in total breach and compromise of the system.
3. Failures tend to be catastrophic, yet can also be difficult to detect until after the damage is done.
4. There is a high-variance time lag between when flaws are introduced into the system and when they manifest as a breach or failure, from days to years.
5. Public/permissionless cryptocurrency is a (mostly) anonymous digital bearer asset – once stolen it is impossible to claw back and difficult to find the thief.
6. Almost all blockchain projects by nature represent a replacement or restructuring of some core IT system/s or FMI (Financial Market Infrastructure), rather than merely extending a tried-and-true core (as, say, an API or mobile app might).

As a result, the requirements for building and operating these systems are quite stringent.

II. Themes

The conference's themes this year provide some educational background on blockchain security, and highlight more granular developments in cryptographic primitives, programming interfaces, and consensus algorithms.

Adversarial Thinking & Security Intuition

A crucial first step for engineers and scientists entering the blockchain industry is in developing a security intuition for an unsecured, total adversarial operating environment, learning to think like the attacker. To that end we have presentations on various types of attacks against both blockchain protocols and blockchain hardware.

Cryptographic primitives

2017 saw promising new developments in cryptographic primitives that extend the capabilities of blockchain systems, and we highlight several of them. There may yet remain relatively low-hanging fruit here, and the further discovery and development of new cryptographic primitives and constructs in the coming years could have a major impact on the way blockchain systems are architected.

Programming interfaces

The development of programming languages and interfaces increasingly tailored to the unique needs of blockchain systems continues. Some are attempting to expand functionality within the constraints of Turing-incompleteness. Others are exploring ways of improving the assurance of Turing-complete languages.

Consensus & Secure Scaling

There have been numerous developments in both consensus algorithms and layer 2 protocols. The original blockchain consensus algorithm, Proof-of-Work, continues to see improvements in its scalability and decentralization. Additionally, new types of consensus algorithms that have been under development are coming online this year, as are Layer 2 protocols like Lightning and its derivatives. It will soon be possible to gather valuable empirical data on how these new systems behave in production.

III. Conclusion

While some aspects of blockchain technology can be contentious, the objective of this conference is to focus on common ground we all care about. Namely, exploring the links between blockchain systems engineering and computer science, and their effects

on security and assurance in production. We hope this conference can make a contribution to that end.

In closing, I would like to thank the Stanford Cyber Initiative, directed by Allison Berke, and the Stanford Computer Security Lab, co-directed by Dan Boneh, for co-hosting the conference. I would also like to thank our sponsors, who made it possible to extend the conference to three days this year. I would also like the thank our Program Committee for their support. Without them it would not have been possible.

Thank you also to everyone joining us, especially from out of town and overseas, and to everyone who submitted a presentation. We received more good submissions than we could include in the program, are grateful to everyone who submitted, and hope to keep in touch for next time.

Thank you, and now on with the program.