Tutorial: Building Secure and Trustworthy Blockchain Applications

Chengjun Cai, Huayi Duan, and Cong Wang
Department of Computer Science
City University of Hong Kong, Hong Kong SAR, China
Email: chencai-c@my.cityu.edu.hk, hduan2-c@my.cityu.edu.hk, congwang@cityu.edu.hk

***Abstract*—Beyond cryptocurrencies, blockchain technologies have shown great potential in enabling a wealth of decentralized applications (DApps), including but not limited to trustworthy auction, election, autonomous organization. While public blockchains are well recognized to allow participants mutually unbeknownst to achieve consensus, financial/business organizations also find great interest in consortium blockchains for better organizational collaborations. We will touch both types of blockchain and corresponding applications in this tutorial. In particular, we will summarize existing blockchain technologies and applications, elaborate the principles of designing and implementing secure DApps, and analyze the security concerns therein. Through concrete examples, we will discuss common practices and pitfalls, such as on-chain/off-chain interaction, randomness generation, and various corner cases. If time permits, we will also go through the implementation of the cloud-based blockchain backbone that powers this tutorial, possibly covering a layered architecture, and discuss deployment choices and security issues along the way. The tutorial will be interspersed with revisiting the security and implementation rules, so that participants are expected to readily apply the tutorial content into real-world practice. The design principles elaborated in this tutorial will be transferable to participants' development of secure and trustworthy blockchain applications and systems in their own workplaces.**

I. Introduction

Since Satoshi Nakamoto introduced Bitcoin [1] in 2008, cryptocurrencies and blockchains have emerged as innovative tools that are useful for financial organizations and various other application scenarios, such as supply chains and health care systems [2]. There are two major types of blockchain: public or permission-less, consortium or permissioned. Upon the former one, applications can rely on transparent and immutable process/data logging, and everyone in the network can audit and prevent frauds. Such public blockchain is favored by services requiring the process/data logs to be publicly revealed for auditing. On the other hand, financial applications like mortgage system [3] usually seek better privacy protection and higher transaction performance, and thus turn to consortium blockchain instead. For example, a recent work [4] introduces "bank-intermediated ledger", with an interesting illustration for a decentralized banking system via consortium blockchain.

Developing decentralized applications on top of blockchain poses many unique challenges compared with traditional applications. The high-value nature of such applications, which may directly operate on millions of dollars, requires security to be built in with extra precautions and scrutiny, as even a minor error can be highly consequential [5]. Developers need to be equipped with totally different points of view and mindsets, with respect to distributed consensus, execution model, and economic incentives, in designing decentralized blockchain applications that meet security and performance requirements.

In this tutorial, we will establish a set of actionable design principles, which are distilled from concrete examples and hands-on illustration, to facilitate the development of secure and trustworthy blockchain applications, and the management of system security against various known attacks. In light of the various needs from real-world applications, we will choose example applications from both public and consortium blockchain. We hope that the content learned from this tutorial will be transferable to customizing blockchain applications in the participants' own workplaces.

II. Tutorial Format and Materials

This tutorial summarizes the existing blockchain technologies and applications, elaborate the principles of designing and implementing secure DApps, and analyze the security concerns therein. Through concrete examples, we will discuss common practices, challenges and pitfalls, such as on-chain/off-chain interaction, randomness generation, and various corner cases. If time permits, we will also go through the implementation of the cloud-based blockchain backbone that powers this tutorial, possibly covering an architecture of four layers (network, storage, consensus and user layer), and discuss deployment choices and security issues along the way. The tutorial will be separated into two parts, including principle elaboration and hands-on illustration of implementing a real-world consortium blockchain system. While the majority of the tutorial will be principle elaboration, these hands-on activities will be interspersed with revisiting the security and implementation rules, so that participants can readily apply the tutorial content into real-world deployments.

A. Design Principles

In this part, participants will first learn the basic core concepts about Bitcoin and blockchains, and existing blockchain technologies and applications. Particularly, two major types of blockchains, i.e., public and consortium blockchain, will be introduced and discussed. Participants will learn their differences in architecture, read/write access controls, application goals, and their respective research focuses in the literature.

Next, we demonstrate how to develop DApps on top of each type of blockchain with strong security guarantee. We will use concrete examples to illustrate common security challenges and pitfalls, for example the on-chain/off-chain interaction, randomness generation, cryptography usage, timing and race conditions, followed by best practices and practical countermeasures that can handle them. Our exposition will not only focus on the developer's side, but also draw on the attacker's perspectives. We hope that by the well-structured demonstration procedures, the essential principles will be distiled and effectively instilled into the audience.

We may also go through the implementation of the cloud-based blockchain backbone that powers this tutorial in a layered approach. In each of the four layers (network, storage, consensus, user) [4], we will introduce to the participants the existing technical choices for implementation and security concerns. For example, we will explain the latest attacks (e.g., DDoS and eclipse attacks [6]) in the network layer, system recovery strategies when encountering massive attacks, security strengths of difference consensus protocols, and possible security enhancements for securing user clients.

B. *Hands-on Illustrations*

During the tutorial, we will engage the participants in a series of hands-on illustrations, which are planned with the assistance of the Amazon cloud using its blockchain service [7]. Participants are expected to bring their computing equipments to participate in these hands-on activities. The aforementioned security principles and implementation guidelines will be revisited along these hands-on activities.

III. Expected Audience and Learning Outcomes

We expect two levels of competency for participants:

- Those who plan to do the hands-on activities on cloud are expected to be familiar with the Virtual Machine (VM) configurations and network gateway setups.
- Those who won't necessarily conduct the deployment experiments, but *are interested in* learning the blockchain application development and security principles.

Participants will develop a general taste of designing and implementing secure DApps in both public and consortium blockchain. They are expected to transfer the learning outcomes to customize applications according to their own service and performance goals. In addition, they will be possibly exposed to the underlying blockchain architecture and learn about security issues that should be properly handled.

Participants who are not familiar with cryptocurrencies and blockchains can expect to learn about the basic concepts and state-of-the-art of existing blockchain technologies. Those who are experienced cryptocurrency researchers might still learn about the practical technicalities in designing secure blockchain applications, and the differences in the architecture and service goals of the two types of blockchains.

Participants with computing equipments will have the opportunities to build up simple real-world blockchain application, learn how to apply best practices, and gain hands-on experiences. Those without computers are still able to understand the development cycle of working blockchain application, as well as general concepts and applicable principles.

Through this tutorial, we hope that the principles elaborated can be useful for participants to adopt (partially or in full) in their workplaces. We also hope that this tutorial can motivate community discussions on establishing standards for both public and consortium blockchain systems.

IV. Prior Similar-Topic Presentations by Authors

This tutorial will be given by three researchers who have developed several blockchain-powered applications, with research results published in IEEE INFOCOM'18 [8], ICDCS'18 [9], ICC'17 [10], and PAC'17 [11]. Cong Wang has given many presentations on data and computation outsourcing security, and privacy-enhancing technologies. He has taught a postgraduate course (CS6290 - "Privacy Enhancing Technologies"), including lecture topics on cryptocurrencies and blockchains. He has also presented the work [11] in the main track of IEEE PAC'17. Chengjun Cai has presented the work [10] in IEEE ICC'17 and the work [9] in IEEE ICDCS'18. Huayi Duan has presented and hosted demo of networked systems in ICNP'16.

Acknowledgment

This work was supported in part by the Research Grants Council of Hong Kong under Project CityU C1008-16G, by the Innovation and Technology Commission of Hong Kong under ITF Project ITS/168/17, by the National Natural Science Foundation of China under Project 61572412, and by AWS in Education Research Grant award.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Online at: http://www.bitcoin.org/bitcoin.pdf, 2008.

[2] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[3] D. Weinland, "Banks adopt blockchain for mortgage valuation system," Online at: https://www.ft.com/content/c856787c-9523-11e6-a1dc-bdf38d484582, 2016.

[4] E. Cecchetti, F. Zhang, Y. Ji, A. E. Kosba, A. Juels, and E. Shi, "Solidus: Confidential distributed ledger transactions via PVORM," in *Proc. of ACM CCS*, 2017.

[5] L. Breidenbach, I. Cornell Tech, P. Daian, F. Tramer, and A. Juels, "Enter the hydra: Towards principled bug bounties and exploit-resistant smart contracts," in *Proc. of USENIX Security*, 2018.

[6] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in *Proc. of USENIX Security*, 2015.

[7] Amazon, Online at: https://aws.amazon.com/partners/blockchain/.

[8] S. Hu, C. Cai, Q. Wang, C. Wang, L. Xiangyang, and K. Ren, "Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization," in *Proc. of IEEE INFOCOM*, 2018.

[9] C. Cai, Y. Zheng, and C. Wang, "Leveraging crowdsensed data streams to discover and sell knowledge: A secure and efficient realization," in *Proc. of IEEE ICDCS*, 2018.

[10] C. Cai, X. Yuan, and C. Wang, "Towards trustworthy and private keyword search in encrypted decentralized storage," in *Proc. of ICC*, 2017.

[11] ——, "Hardening distributed and encrypted keyword search via blockchain," in *Proc. of IEEE Symposium on Privacy-Aware Computing*, 2017.