Condensed Cryptographic Currencies Crash Course (C5)

Aljosha Judmayer
SBA Research
ajudmayer@sba-research.org

Edgar Weippl
SBA Research
eweippl@sba-research.org

ABSTRACT

"*Bitcoin is a rare case where practice seems to be ahead of theory.*" Joseph Bonneau et al. [3]

This tutorial aims to further close the gap between IT security research and the area of cryptographic currencies and block chains. We will describe and refer to Bitcoin as an example throughout the tutorial, as it is the most prominent representative of such a system. It also is a good reference to discuss the underlying block chain mechanics which are the foundation of various altcoins and other derived systems. In this tutorial, the topic of cryptographic currencies is solely addressed from a technical IT security point-of-view. Therefore we do not cover any legal, sociological, financial or economical aspects.

The tutorial is designed for participants with a solid IT security background but will not assume any prior knowledge on cryptographic currencies. Thus, we will quickly advance our discussion into core aspects of this field.

This tutorial is a modified version of the tutorial held at WWW2016 [9]. It incorporates received feedback and customized content.

Keywords

Cryptographic currencies; block chain; blockchain; Bitcoin

1. INTRODUCTION

With a current market capitalization of approximately 9 billion dollars, Bitcoin has demonstrated that a decentralized cryptographic currency which currently handles roughly 200.000 transactions per day [2] is technically possible. Since its launch in 2009, by an entity referred to as Satoshi Nakamoto [11], the topic of cryptographic currencies has attained widespread recognition.

The new field of cryptographic currencies and consensus ledgers, commonly referred to as *block chains* (or *blockchains*), is receiving increasing interest from various different communities [10]. These communities are very diverse and amongst others include: technical enthusiasts, activist groups, researchers from various disciplines, start-ups, large enterprises, public authorities, banks, financial regulators, business men, investors and criminals. The scientific community in general adapted to this emerging and fast moving field of cryptographic currencies and consensus ledgers relatively slowly.

This was one reason that, for quite a while, the only resources available have been the Bitcoin source code, blog-forum-posts, mailing lists and other online publications. Also the original Bitcoin paper [11] which initiated the hype was published online without any prior peer-review. Following the original publication spirit of the Bitcoin paper, a lot of innovation in this field has always come from the community itself in form of online-publications and online-conversations and not from established peer-reviewed scientific publishing.

This spirit of fast free software development, combined with the business aspects of cryptographic currencies, as well as the interests of today's time-to-market focused industry, produced a flood of publications, whitepapers and prototypes. This quickly advancing hype has led to an absence of systematization and deficits in the theoretical understanding of this new domain.

This tutorial aims at further closing this gap and presents a well-structured introduction to this broad field from a technical viewpoint. Since the archetype for modern cryptographic currencies and consensus ledgers is Bitcoin, we describe the inner workings of this protocol in detail and discuss its relations to other derived systems.

2. METHODOLOGY

A web based challenge environment will be available online for all participants during the tutorial. As a practical exercise and a method of gamification we hand out small amounts of Bitcoin to the participants as a reward for solved challenges during the tutorial. Therefore, we encourage all participants to bring their laptops to be able to participate. The challenges range from quiz questions, that can be solved with the help of a browser, to small practical tasks.

During the tutorial, we provide various references for further studies. Those references link to a comprehensive bibliography containing relevant scientific publications in this field as well as the most important online resources [1].

[1] https://allquantor.at/blockchainbib/

CCS '16 October 24–28, 2016, Vienna, Austria.

ACM ISBN 978-1-4503-4139-4/16/10..

DOI: http://dx.doi.org/10.1145/2976749.2976754

3. OUTLINE OF THE TUTORIAL

History of cryptocurrencies: This should give a quick overview of the history of cryptographic currency research, and their roots which date back to 1980's and David Chaums publications in that field [4, 5, 6].

Ingredients for proof-of-work based cryptocurrencies: Here we quickly go through the required cryptographic concepts for current mainstream cryptocurrencies and block chains. This includes the notion of proof-of-work (PoW) schemes [1, 7]. Thereby, we will cover the basic characteristics of the schemes used in Bitcoin. The main goal of this chapter is a recap to bring everybody on the same level for the next chapter.

Bitcoin and block chain mechanics: In this chapter we outline how everything fits together and forms a PoW based cryptographic currency. Thereby, Bitcoin is discussed as an archetype for cryptographic currencies and PoW based consensus ledger design. We go over the basic elements of Bitcoin and describe how they work e.g.: Blocks, transactions, mining and the block chain, Bitcoin scripting language, transaction fees, block chain forks, double-spending [12, 13, 3, 8]

Open challenges and outlook: We present and quickly discuss currently unsolved challenges.

4. INTENDED AUDIENCE

This **75 minutes** tutorial does not assume any prior knowledge on cryptopgrahic currencies. We assume good general knowledge of information security on a graduate CS student level with a focus on security. The goal of this tutorial is to present the knowledge from various sources in a structured way and to provide researchers with the **practical fundamentals** of cryptocurrencies/block chains and practitioners with the **scientific background**.

The **key takeaways** are: (I) the practical fundamentals of PoW based cryptographic currencies, (II) a good understanding of the underlying block chain mechanics, (III) a overview of the related literature in this field

Since we address this topic mainly from a technical point-of-view, we will not cover any legal, sociological, financial or purely economical aspects of cryptocurrencies.

5. BIO

Aljosha Judmayer received a master's degree in Software Engineering and Internet Computing at the TU Wien. He has five plus years experience in penetration testing as IT security consultant. At the moment, he is working as IT security researcher at SBA Research, where he is also working towards his Ph.D. degree on applications of cryptographic currencies and resilience aspects of distributed systems. His research interests include network security, applied cryptography and cryptographic currencies.

Edgar Weippl is Research Director of SBA Research and associate professor at TU Wien. After graduating with a Ph.D. from the TU Wien, Edgar worked in a research startup for two years. He then spent one year teaching as an Assistant Professor at Beloit College, WI. From 2002 to 2004, while with the software vendor ISIS Papyrus, he worked as a consultant in New York, NY and Albany, NY, and in Frankfurt, Germany. In 2004 he joined the TU Wien and founded the research center SBA Research together with A Min Tjoa and Markus Klemen. Edgar is member of the editorial board of Computers & Security (COSE), organizes the ARES conference and is General Chair of SACMAT 2015, PC Chair of Esorics 2015 and General Chair of ACM CCS 2016.

6. ACKNOWLEDGMENTS

This research was funded by COMET K1, FFG - Austrian Research Promotion Agency and by FFG Bridge Early Stage 846573 A2Bit. We want to thank Georg Merzdovnik for helping developing the challenge framework.

7. REFERENCES

[1] A. Back et al. Hashcash-a denial of service counter-measure. http://www.hashcash.org/papers/hashcash.pdf, 2002. Accessed: 2016-03-09.

[2] Blockchain.info. Bitcoin currency statistics. http://blockchain.info/. Accessed: 2015-06-30.

[3] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *IEEE Symposium on Security and Privacy*, 2015.

[4] D. Chaum. Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer, 1983.

[5] D. Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.

[6] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In *Proceedings on Advances in cryptology*, pages 319–327. Springer-Verlag New York, Inc., 1990.

[7] H. Finney. Reusable proofs of work (rpow). http://web.archive.org/web/20071222072154/http://rpow.net/, 2004. Accessed: 2016-04-31.

[8] J. Garay, A. Kiayias, and N. Leonardos. The bitcoin backbone protocol: Analysis and applications. In *Advances in Cryptology-EUROCRYPT 2015*, pages 281–310. Springer, 2015.

[9] A. Judmayer and E. Weippl. Cryptographic currencies crash course (c4). http://www2016.net/proceedings/companion/p1021.pdf, Apr 2016. Accessed: 2016-06-06.

[10] K. Krombholz, A. Judmayer, M. Gusenbauer, and E. Weippl. The other side of the coin: User experiences with bitcoin security and privacy. In *International Conference on Financial Cryptography and Data Security (FC)*, 2 2016.

[11] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, Dec 2008. Accessed: 2015-07-01.

[12] Narayanan, Arvind and Bonneau, Joseph and Felten, Edward and Miller, Andrew and Goldfeder, Steven. Bitcoin and cryptocurrency technologies. https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1, 2016. Accessed: 2016-03-29.

[13] F. Tschorsch and B. Scheuermann. Bitcoin and beyond: A technical survey on decentralized digital currencies. In *IEEE Communications Surveys Tutorials*, volume PP, pages 1–1, 2016.