Cryptographic Currencies Crash Course (C4)

Tutorial

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. [15]

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 a such a system. It also is a good reference to discuss the underlying block chain mechanics which are the foundation of various altcoins (e.g. Namecoin) 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 and 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.

Keywords

Cryptographic currencies; block chain; Bitcoin

1. INTRODUCTION

With a current market capitalization of approximately 3.5 billion dollars, Bitcoin has demonstrated that a decentralized cryptographic currency which handles roughly 130.000 transactions per day [13] is technically possible. Since its launch in 2009 by an entity referred to as Satoshi Nakamoto [38], the topic of cryptographic currencies has attained widespread recognition. With the success of Bitcoin several hundred other cryptographic currencies have been derived from it or developed from scratch.

The main attribute which most of these cryptographic currencies have in common is the block chain. It is responsible for confirming transactions and synchronizing the state of the underlying peer-to-peer network. Thereby, it relies on proof-of-work (PoW) [3, 38] puzzles as a method of issuing the coins and hardening the consensus. In general the block chain works as an append-only store which keeps a permanent ledger of all performed transactions in the system.

This underlying concept does not only allow the construction of decentralized currency exchange systems like Bitcoin, it also provides other applications scenarios like for example decentralized key-value stores for name registration like for example Namecoin [33]. Current efforts try to build more complex systems on top of theses structures like for example Certcoin [27] and Ethereum [25]. Certainly there are enough open challenges and topics for further research in this emerging field [15].

Although, we see a rise in Bitcoin related research recently [21, 45, 34, 42, 36, 29, 22, 15, 14, 30, 37, 24, 33] there still exists a gap between the latest proposals and prototypes developed by the cryptocurrency community [8, 7, 25, 47, 16] and the latest publications from the IT security research community. As stated in [15] in case of cryptographic currencies practice seems to be ahead of theory. Moreover, there is no official formal specification of the Bitcoin protocol, making it difficult to directly dive into the area without going through a lot of web pages [6], forum postings [12], github repositories and source code [41, 7], wiki articles [11, 9], mailing list conversations and BIPs [8]. Due to the lack of specification, the reference implementation *bitcoind* [10] is considered as the main reference and the de facto specification in case of Bitcoin [15, 37].

This tutorial should help to further close this gap and introduce the participants to the field of cryptographic currencies. The goal of this tutorial is to present the knowledge from various sources in a structure way and to provide researchers with the **practical fundamentals** of cryptocurrencies/block chains and practitioners with the **scientific background**.

2. METHODOLOGY

In this **half day** tutorial we survey the recent literature and illustrate the core functionality as well as the technical aspects of Bitcoin and hence cryptographic currencies in general from an IT security point of view. This includes theoretical background and cryptography, network and peer-to-peer aspects as well as some anonymity and traceability considerations. We will not cover any legal, sociological, financial and economical aspects of cryptocurrencies.

As a practical exercise and a method of gameification we **hand out small amount 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 in these challenges. The challenges reach

WWW'16 Companion, April 11–15, 2016, Montréal, Québec, Canada.
ACM 978-1-4503-4144-8/16/04.
http://dx.doi.org/10.1145/2872518.2891066.

from quiz questions, that can be solved with the help of a browser, to small practical tasks.

At the end we provide references for further studies and hand out a comprehensive bibliography containing the relevant scientific publications in this field as well as the most important online resources. This serves researches (e.g. graduate students) as a starting point for their research.

The key takeaways are:

- the practical fundamentals of PoW based cryptographic currencies
- a good understanding of the underlying block chain mechanics
- a overview of the related literature in this field
- a outlook based on current directions and trends

3. STRUCTURE OF THE TUTORIAL

The high level agenda for the half day tutorial is described in this section. Each chapter is represented by one subsection. Since cryptographic currencies are a rapidly evolving field, small deviations in the agenda until the execution of the tutorial are possible.

3.1 History of crypto currencies

This should give a quick overview over the history of cryptographic currency research, and their roots which date back to 1980's and David Chaums publications in that field [18, 19, 20].

3.2 Ingredients for proof-of-work based cryptocurrencies

Here we quickly go over the required cryptographic concepts for current mainstream cryptocurrencies and block chains. This includes the notion of proof-of-work (PoW) schemes [3] and asymmetric cryptography. Thereby, we will cover the basic characteristics of the schemes used in Bitcoin, i.e. Elliptic Curve Digital Signature Algorithm (ECDSA) over secp256k1 [7], but avoid going into greater detail on the underlying mathematics [17, 40]. The main goal of this chapter is a recap to quickly bring everybody on the same level for the next chapter.

3.3 Bitcoin the archetype

In this chapter we outline how the everything fits together and forms a cryptocurrency like Bitcoin. Thereby, Bitcoin is discussed as an archetype for cryptographic currencies and block chains design [38, 28]. We go over the basic elements of Bitcoin and described how they work e.g.: Mining and the block chain [36, 2, 44], transactions and fees and block chain forks and double-spending. For selected examples we also dig into the Satoshi client source code [10], as this is the de facto protocol standard. We will also discuss how to keep your bitcoins safe [8, 31, 30]

3.4 Block chains mechanics in general

We generalize the concept of Bitcoin and cryptographic currencies and discuss derived systems based on Bitcoin (e.g. Namecoin) as an alternative application for block chain protocols. We go through the relevant literature concerning theoretical background, where we present the general probabilistic security assumptions behind cryptocurrencies by calculating and comparing Rosenfelds [44] and Satoshis [38] methods for describing the probability of double spending attacks. We discuss the general concept of block chains based on the Bitcoin reference implementation [10], the approaches taken in Namecoin [39] and the literature [28].

3.5 Network and P2P aspects

Building on the previous part, we discuss the network and P2P aspects of cryptographic currencies. Thereby, we describe the general functionality of *bitcoind* as this is the most widely used implementation for the network layer of cryptographic currencies. Regarding network and peer-to-peers aspects we will discuss propagations and topology issues [4, 23, 37, 29], methods of seeding and node discovery.

3.6 Traceability and anonymity

We trace transactions though the transaction graph and discuss the effectiveness of anonymity preserving methods like CoinJoin, Tor [5]. We demonstrate traceability of coins and entities and cover the relevant literature regarding privacy and anonymity aspects [26, 1, 43, 35, 46].

3.7 Open challenges and outlook

We present and quickly discuss currently unsolved challenges and recent proposals and prototypes developed and published by the cryptocurrency community.

4. TARGET AUDIENCE

The tutorial is specifically designed for an audience with solid IT security background. No security basiscs will be covered. We assume attendees to have at least knoweledge equivialent to the knowledge areas as defined in the ACM/IEEE CS curriculum [32] in the knowledge area information assurance and security i.e. *Foundational Concepts in Security* and *Cryptography*.

Participants will benefit more if they also have knowledge equivalent to: Principles of Secure Design, Defensive Programming, Threats and Attacks, Network Security.

For graduate students this tutorial offers a good overview of the field. Therefore, it is particulary interesting for those who plan new research which correlates with the domain of cryptographic currencies and block chains. Professors and lecturers can include content of this tutorial in their courses. The small challenges during the tutorial can also give further ideas for assignments.

5. BIO

Aljosha Judmayer received a master's degree in Software Engineering and Internet Computing at the Vienna University of Technology. 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.

7. REFERENCES

[1] Alex Biryukov and Dmitry Khovratovich and Ivan Pustogarov. Deanonymisation of clients in Bitcoin P2P network. *CoRR*, abs/1405.7418, 2014.

[2] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar. On bitcoin and red balloons. pages 56–73, 2012.

[3] A. Back et al. Hashcash-a denial of service counter-measure. `http://www.hashcash.org/papers/hashcash.pdf`, 2002.

[4] T. Bamert, C. Decker, L. Elsen, R. Wattenhofer, and S. Welten. Have a snack, pay with bitcoins. In *13th IEEE International Conference on Peer-to-Peer Computing*, 2013.

[5] A. Biryukov and I. Pustogarov. Bitcoin over tor isn't a good idea. *arXiv preprint arXiv:1410.6079*, 2014.

[6] Bitcoin community. Bitcoin developer guide. `https://bitcoin.org/en/developer-guide`. Accessed: 2014-10-14.

[7] Bitcoin community. Bitcoin github meta repository. `https://github.com/bitcoin/`. Accessed: 2015-06-30.

[8] Bitcoin community. Bitcoin improvement proposals (bips). `https://github.com/bitcoin/bips`. Accessed: 2015-06-30.

[9] Bitcoin community. Bitcoin protocol specification. `https://en.bitcoin.it/wiki/Protocol_specification`. Accessed: 2014-10-14.

[10] Bitcoin community. Bitcoin source code. `https://github.com/bitcoin/bitcoin`. Accessed: 2015-06-30.

[11] Bitcoin community. Bitcoin wiki. `https://bitcoin.it/`. Accessed: 2015-06-30.

[12] Bitcoin community. Bitcointalk forum. `https://bitcointalk.org/`. Accessed: 2015-06-30.

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

[14] J. Bonneau, E. W. Felten, S. Goldfeder, J. A. Kroll, and A. Narayanan. Why buy when you can rent? `http://www.jbonneau.com/doc/BFGKN14-bitcoin_bribery.pdf`.

[15] 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.

[16] J. D. Bruce. The mini-blockchain scheme (a.k.a purely p2p crypto-currency with finite mini-blockchain). `http://www.bitfreak.info/files/pp2p-ccmbc-rev1.pdf`, Jul 2014. Accessed: 2014-04-05.

[17] Certicom Research. SEC 2: Recommended Elliptic Curve Domain Parameters, Sept. 2000.

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

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

[20] 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.

[21] G. G. Dagher, B. Bünz, J. Bonneau, J. Clark, and D. Boneh. Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 720–731. ACM, 2015.

[22] C. Decker, J. Guthrie, J. Seidel, and R. Wattenhofer. Making bitcoin exchanges transparent. In *Computer Security{ESORICS 2015*, pages 561–576. Springer, 2015.

[23] C. Decker and R. Wattenhofer. Information propagation in the bitcoin network. In *13th IEEE International Conference on Peer-to-Peer Computing*, 2013.

[24] S. Eskandari, D. Barrera, E. Stobert, and J. Clark. A first look at the usability of bitcoin key management. In *Workshop on Usable Security (USEC)*, 2015.

[25] Ethereum community. Ethereum: A next-generation smart contract and decentralized application platform - white-paper. `https://github.com/ethereum/wiki/wiki/White-Paper`. Accessed: 2015-06-30.

[26] M. H. F. Reid. An analysis of anonymity in the bitcoin system. In *2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing*, 2011.

[27] C. Fromknecht, D. Velicanu, and S. Yakoubov. A decentralized public key infrastructure with identity retention. *IACR Cryptology ePrint Archive*, Oct 2014.

[28] 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.

[29] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun. Tampering with the delivery of blocks and transactions in bitcoin. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 692–705. ACM, 2015.

[30] S. Goldfeder, R. Gennaro, H. Kalodner, J. Bonneau, J. Kroll, E. W. Felten, and A. Narayanan. Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme. `http://www.cs.princeton.edu/~stevenag/threshold_sigs.pdf`. Accessed: 2015-07-13.

[31] G. Gutoski and D. Stebila. Hierarchical deterministic bitcoin wallets that tolerate key leakage (short paper). In *Proceedings of the 19th International Conference on Financial Cryptography and Data Security (FC 2015)*. Springer, 2015.

[32] A. f. C. M. A. Joint Task Force on Computing Curricula and I. C. Society. *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*. ACM, New York, NY, USA, 2013. 999133.

[33] H. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, and A. Narayanan. An empirical study of namecoin and lessons for decentralized namespace design. `http://randomwalker.info/publications/namespaces.pdf`, 2015.

[34] R. Kumaresan, T. Moran, and I. Bentov. How to use bitcoin to play decentralized poker. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 195–206. ACM, 2015.

[35] I. Miers, C. Garman, M. Green, and A. D. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In *2013 IEEE Symposium on Security and Privacy*, 2013.

[36] A. Miller, A. Kosba, J. Katz, and E. Shi. Nonoutsourceable scratch-off puzzles to discourage bitcoin mining coalitions. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 680–691. ACM, 2015.

[37] A. Miller, J. Litton, A. Pachulski, N. Gupta, D. Levin, N. Spring, and B. Bhattacharjee. Discovering bitcoin's public topology and influential nodes. `http://cs.umd.edu/projects/coinscope/coinscope.pdf`, May 2015.

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

[39] Namecoin community. Namecoin source code (official). `https://github.com/namecoin/namecoin`. Accessed: 2014-10-14.

[40] NIST. FIPS 186-4: Digital Signature Standard (DSS), July 2013.

[41] K. Okupski. Bitcoin protocol specification. `https://github.com/minium/Bitcoin-Spec`. Accessed: 2014-10-14.

[42] R. Pass et al. Micropayments for decentralized currencies. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 207–218. ACM, 2015.

[43] D. Ron and A. Shamir. Quantitative analysis of the full bitcoin transaction graph. Cryptology ePrint Archive, Report 2012/584, 2012. http://eprint.iacr.org/.

[44] M. Rosenfeld. Analysis of hashrate-based double spending. *CoRR*, abs/1402.2009, 2014.

[45] T. Ruffing, A. Kate, and D. Schröder. Liar, liar, coins on fire!: Penalizing equivocation by loss of bitcoins. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 219–230. ACM, 2015.

[46] T. Ruffing, P. Moreno-Sanchez, and A. Kate. Coinshuffle: Practical decentralized coin mixing for bitcoin. In *Computer Security-ESORICS 2014*, pages 345–364. Springer, 2014.

[47] Satoshi Labs. Trezor: The hardware bitcoin wallet. `https://github.com/trezor`. Accessed: 2015-06-30.