Univeristé Libre de Bruxelles

PhD Thesis Proposal

Bitcoin Cryptographic Primitives and Beyond

by

Thomas Suau

Supervisor: **Pr. Christophe Petit**

June, 2023

Abstract

In this proposal, I wish to give you an overview of what could be built as academic research on top of Bitcoin protocol as cryptographic primitives and studies on Bitcoin Improvements Proposals (BIPs)[1]. The protocol is constantly evolving as shown by the mailing list linuxfoundation : `https://lists.linuxfoundation.org/pipermail/bitcoin-dev/`.
Recently, many protocols were arrived on top of Bitcoin [1–4]. We find a lack of academic research about last protocol updates' and some features are not regarded in the scope of cryptography.

What I'm purposing is a proof of soundness for major BIPs especially look deeper in the proof proposed in BIP 341[5] (Taproot)[2]. If proof is sound, purposed an aggregation of different security proofs of main BIPs to compose my first work.
After this, take a moment to analyse soundness of protocols built on top of Bitcoin like Lightning Network [3, 7], RGB [4] and the most recent Ark [8] not released now.
A deeper study of the core protocol could be made following recommendations in [9] and new articles.
At the end, try to purpose an algorithm to check security of top layer on Bitcoin or BIPs. At least a checking protocol, to allow everyone to check it's implementation on top of Bitcoin protocol.
The goal of this submission is both to be allow to conduct research on the Bitcoin Protocol[10] and protocols built on top of it, especially focus on soundness ; and to participate in cryptography research oriented on blockchain protocols focus on Bitcoin.

[1]For more details about BIP see : BIP 0001, where you can find all BIPs history.
[2]When we find briefly introduced [6] and this taproot security proof.

Contents

1 State of the art

Bitcoin is a protocol developed and deployed since 2009 [11]. It has several different applications and forms which can be given. A good summary of the Bitcoin challenges and considerations was given in [9] published in 2015. In a more general way we can focus on challenges for Ethereum [12] and in the Blockchain industry [13] with focusing on cryptographic challenges.

The Bitcoin Protocol is vast and it concerns several different fields. It's an economic proposal based on computer sciences with electrical, banks, computer sciences, cryptography and human considerations [9, 14].

Many related articles are today based on the economic [15, 16] or business [17] and electrical aspect[18–20] of the protocol. There are many investors, politicians [21] and citizens [22, 23] which are engaged with Bitcoin. Many communities are trying to use Bitcoin to their own interest and needs [14, 24].

For a complete overview about Bitcoin protocol you can check [25] which is *Mastering Bitcoin*, a reference about all technical aspects of Bitcoin.

For signature building on this protocol and blockchain in general we have [26–28], with use of ECDSA (Elliptic Curve Digital Signature Algorithm) under *secp256k1* curve group for Bitcoin. We can see in [26] that many new protocols are making use of Fully Homomorphic Encryption (FHE).

There is an important article [29] which argues to prove in theory that BIP 119 allowing creation of "sound Bitcoin token". Recently the new BIP 341 is introducing many new features including new `OP_CODE` and key aggregation signature permitted by Schnorr Signature [3].

Many protocols are built on top of Bitcoin : Lightning Network [30, 31], RGB [4], or Ark [1, 8] [5].

According to [9] and [32] there is still a lack of soundness proof for many features present in Bitcoin. Many developments are continuing to enhance the protocol and I think we need to have strong academics researches on soundness and security proof of different protocols and cryptographic primitives [28, 33, 34].

Considering also the coding language `Rust`, is becoming a several used language for its performance, safety, and memory management [35–37]. It can be used to manage with specific component of the computer in a high-level abstractions way [38] and be useful for many cryptographic applications [39, 40] and zero trust architecture development [41], especially useful for Bitcoin protocol implementations.

[3] For a complete detail of this BIP and others you can visit BIP 341 | Github.

[4] Where we can find here the original description.

[5] The most recent that should allow more privacy with same advantages of Lightning Network.

2 Goals

As it told in state of the art section 1, there is a lack of sound study about last BIP implementations especially the last major BIP 341 [5]. Many developments are occurring on top of the Bitcoin protocol since this implementation without any prior proof of soundness.

2.1 BIPs are sound

The first goal is to prove that last BIP [5] is sound under Diffie-Hellman assumptions [42]. Ideally, we can also show that major implementations happened on Bitcoin was sound also.

2.2 Soundness of new protocols

Show that new protocols built on top of Bitcoin could be sound under classical cryptographic assumptions. If we can't prove this, find assumptions which are meaningful to talk about security for protocols like Lightning Network[30], RGB [43] [6], Ark and in last considerations Ordinals [7].

2.3 Algorithm

Make an algorithm to compute over Diffie-Hellman's assumptions the level of security for a given protocol built on top of Bitcoin[44].
This could be a goal more general than only Bitcoin or blockchain. Because of proof of soundness can be done, we can see in computation theory if we can transform proofs into a general algorithm.
By state of the art considerations 1 we can build this algorithm with `Rust` language which allow us to make several use of cryptographic primitives.

2.4 Some extensions possible

We can extend the topic at other blockchains with making use of smart contract, zero-knowledge layers and oracle in a not proved sounded way [12, 32].

[6] We can notice that the name RGB for the protocol is a funny turn of events as we can see in What does 'RGB' stands for ?.

[7] Based on push text with `OP_CODE` and indexing it via its own tools Ordinals Repo.

3 Methodology

The methodology should follow three steps.

3.1 Reviewing and conferences

Based on work [29] and [42] proposed a cryptographic review of BIP 341[5]. Is everything sound into this BIP ?
Verify last `OP_CODE` proposed into this BIP in usual security framework requirements [42].
With the help of different researcher across the Europe (Olivier Pereira, David Naccache, Jean-Jacques Quisquater, Andreas M. Antonopoulos, ...) and events like Crypto economic systems MIT Digital Initiative, we can think that this goal should be done in a relative short period. This step, would allow us to have a better academic understanding about cryptographic challenges for BIPs and participate to the research community on this protocol.

3.2 Soundness of new protocols

After this work succeeded, I will be able to analyse consequences of the Taproot update (BIP 341). By this work I hope to be able to prove quite easily the soundness of Ordinals protocol and other protocols built on top of Ordinals.
The in-depth study of Lightning Network security [30, 31] should give indications to produce studies about RGB protocol security and Ark security. This can be a major goal very valuable in regards of importance of assets built on RGB and Ark aspiration's.

3.3 Algorithm

The final goal is to build a standard algorithm to allow test on every other protocols built on top of Bitcoin to be secure and sound under basics Diffie-Hellman assumptions as them took in Pinocchio Protocol [45].

Bibliography

[1] B. Keceli. *[bitcoin-dev] Ark: An Alternative Privacy-preserving Second Layer Solution*, (2023).

[2] C. Rodarmor and alt. *Ordinals Documentation*. `https://docs.ordinals.com/`, (2022).

[3] W. contributors. *Lightning Network – Wikipedia, The Free Encyclopedia*. `https://en.wikipedia.org/w/index.php?title=Lightning_Network&oldid=1147106094`, (2023).

[4] RGB. *What is RGB ?* `https://www.rgbfaq.com/faq/what-is-rgb`.

[5] P. Wuille, J. Nick, and A. Towns. *BIP 341 : Taproot: SegWit version 1 spending rules*. `https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki`, (2020).

[6] M. Fersch. *The provable security of elgamal-type signature schemes*. doctoralthesis, Ruhr-Universität Bochum, Universitätsbibliothek, (2018).

[7] P. Zabka, K.-T. Foerster, S. Schmid, and C. Decker, *Empirical evaluation of nodes and channels of the lightning network*, Pervasive and Mobile Computing **83**, 101584 (2022).

[8] *Ark - New L2 protocol*. `https://bitcointalk.org/index.php?topic=5453928.0`, (2023).

[9] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, (2015).

[10] A. Narayanan and J. Clark, *The concept of cryptocurrencies is built from forgotten ideas in research literature.*, ACMQueue (2017).

[11] S. Nakamoto, *Bitcoin : A peer-to-peer cash Electronic System*, Bitcoin.org (2008).

[12] S. Tikhomirov. *Ethereum: State of Knowledge and Research Perspectives*. In A. Imine, J. M. Fernandez, J.-Y. Marion, L. Logrippo, and J. Garcia-Alfaro, editors, *Foundations and Practice of Security*, pages 206–221, Cham, (2018). Springer International Publishing.

[13] D. Valdeolmillos, Y. Mezquita, A. González-Briones, J. Prieto, and J. M. Corchado. *Blockchain Technology: A Review of the Current Challenges of Cryptocurrency*. In J. Prieto, A. K. Das, S. Ferretti, A. Pinto, and J. M. Corchado, editors, *Blockchain and Applications*, pages 153–160, Cham, (2020). Springer International Publishing.

[14] J. Bohr and M. Bashir. *Who Uses Bitcoin? An exploration of the Bitcoin community*. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust*, pages 94–101, (2014).

[15] A. Zohar, *Bitcoin: Under the Hood*, Commun. ACM **58**, 104–113 (2015).

[16] J. R. Hendrickson, T. L. Hogan, and W. J. Luther, *The Political Economy of Bitcoin*, Economic Inquiry **54**, 925–939 (2016).

[17] M. A. Naeem and S. Karim, *Tail dependence between bitcoin and green financial assets*, Economics Letters **208**, 110068 (2021).

[18] H. Vranken, *Sustainability of bitcoin and blockchains*, Current Opinion in Environmental Sustainability **28**, 1–9 (2017).

[19] S. Nadarajah and J. Chu, *On the inefficiency of Bitcoin*, Economics Letters **150**, 6–9 (2017).

[20] L. Badea and M. C. Mungiu-Pupâzan, *The Economic and Environmental Impact of Bitcoin*, IEEE Access **9**, 48091–48104 (2021).

[21] EUR-Lex, editor. *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937*, Brussels, (2020). European Union, European Commission.

[22] B. Bhushan, I. K. Mensah, and D. S. Mwakapesa, *The Drivers of the Behavioral Adoption Intention of BITCOIN Payment from the Perspective of Chinese Citizens*, Security and Communication Networks **2022**, 7373658 (2022).

[23] M. Sparkes, *El Salvador revamps bitcoin system*, New Scientist **253**, 8 (2022).

[24] A. F. Cifuentes, *Bitcoin en economías turbulentas: el potencial de las criptomonedas en Argentina y Venezuela*, Latin American Law Review **1**, 99–116 (2019).

[25] A. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly Media (2014).

[26] X. Du, C. Yuan, M.-x. Xu, and X.-m. Si, *Research on a New Signature Scheme on Blockchain*, Security and Communication Networks **2017**, 4746586 (2017).

[27] F. M. Jasem, A. M. Sagheer, and A. M. Awad, *Enhancement of digital signature algorithm in bitcoin wallet*, Bulletin of Electrical Engineering and Informatics **10**, 449–457 (2021).

[28] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow. *Elliptic Curve Cryptography in Practice*. In N. Christin and R. Safavi-Naini, editors, *Financial Cryptography and Data Security*, pages 157–175, Berlin, Heidelberg, (2014). Springer Berlin Heidelberg.

[29] M. Bartoletti, S. Lande, and R. Zunino. *Computationally sound Bitcoin tokens*. In *2021 IEEE 34th Computer Security Foundations Symposium (CSF)*, pages 1–15, (2021).

[30] A. Kiayias and O. S. T. Litos. *A Composable Security Treatment of the Lightning Network*. In *2020 IEEE 33rd Computer Security Foundations Symposium (CSF)*, pages 334–349, (2020).

[31] S. Tikhomirov, P. Moreno-Sanchez, and M. Maffei. *A Quantitative Analysis of Security, Anonymity and Scalability for the Lightning Network*. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 387–396, (2020).

[32] R. Singh, Pooja, A. K. Agarwal, R. Naaz, R. Kumar, and R. Vijay. *A Study of Cryptographic Primitives in the context of Blockchain's Data Integrity and Privacy*. In *2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART)*, pages 1589–1595, (2022).

[33] J. Li, Z. Lin, J. Caballero, Y. Zhang, and D. Gu. *K-Hunt: Pinpointing Insecure Cryptographic Keys from Execution Traces*. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, pages 412–425, New York, NY, USA, (2018). Association for Computing Machinery.

[34] K. Bjoernsen, *Koblitz Curves and its practical uses in Bitcoin security*, University of California, Santa Barbara.

[35] S. Klabnik and C. Nichols, *The Rust Programming Language, 2nd Edition*, No Starch Press, 2nd edition (2023).

[36] R. Jung. *Understanding and evolving the Rust programming language*. PhD thesis, Universität des Saarlandes, (2020).

[37] R. Jung, J.-H. Jourdan, R. Krebbers, and D. Dreyer, *Safe Systems Programming in Rust*, Commun. ACM **64**, 144–152 (2021).

[38] E. Holk, M. Pathirage, A. Chauhan, A. Lumsdaine, and N. D. Matsakis. *GPU Programming in Rust: Implementing High-Level Abstractions in a Systems-Level Language*. In *2013 IEEE International Symposium on Parallel & Distributed Processing, Workshops and Phd Forum*, pages 315–324, (2013).

[39] K. Mindermann, P. Keck, and S. Wagner. *How Usable Are Rust Cryptography APIs?* In *2018 IEEE International Conference on Software Quality, Reliability and Security (QRS)*, pages 143–154, (2018).

[40] D. Merigoux, F. Kiefer, and K. Bhargavan. *Hacspec: succinct, executable, verifiable specifications for high-assurance cryptography embedded in Rust*. Technical report, Inria, (2021).

[41] D. Hardin, *Hardware/Software Co-Assurance for the Rust Programming Language Applied to Zero Trust Architecture Development*, Ada Lett. **42**, 55–61 (2023).

[42] A. Roy, A. Datta, and J. C. Mitchell. *Formal Proofs of Cryptographic Security of Diffie-Hellman-Based Protocols*. In G. Barthe and C. Fournet, editors, *Trustworthy Global Computing*, pages 312–329, Berlin, Heidelberg, (2008). Springer Berlin Heidelberg.

[43] R. Linus and L. George, *ZeroSync: Introducing Validity Proofs to Bitcoin*, ZeroSync Association.

[44] D. Wikström. *Special Soundness Revisited*. Cryptology ePrint Archive, Paper 2018/1157, (2018).

[45] B. Parno, J. Howell, C. Gentry, and M. Raykova. *Pinocchio: Nearly Practical Verifiable Computation*. In *2013 IEEE Symposium on Security and Privacy*, pages 238–252, (2013).