Hacking the Lightning Network - A protocol to scale Bitcoin [Draft]

Rene Pickhardt

January 9, 2019

Consider financially supporting my book writing effort!

Since this is an open source effort, I rely on the support of the community. In order to be able to work full time on this book, I need a budget of 21.21212121 Bitcoin (with current exchange rates).

Bitcoin via: `https://tallyco.in/s/lnbook/` or fiat money at: `https://patreon.com/renepickhardt`

[1] `https://github.com/renepickhardt/the-lightning-network-book/LICENCE`

[2] `https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode`

Contents

Chapter 1

Introduction

This book is a guide to understanding the Lightning Network as a technology to solve the scalability problem of Bitcoin. It will first introduce the basic concepts of the Bitcoin protocol. We will only make use of applied cryptography on a high level without the mathematical details. Therefore basically no cryptographic knowledge is needed to be able to follow through this book. For the sake of completeness some of the cryptographic details will be stated in the appendix. Thus the Bitcoin section should be understandable by any computer science (or similar) undergraduate student. As the Lightning Network is built on top of Bitcoin also the rest of the book should be easily understandable by the same audience. We conclude the first chapter by looking at some fundamental issues with bitcoin as a payment system and

explain the necessity for the Lightning Network.

We continue by explaining the theory and construction of the Lightning Network. We will understand how to construct payment channels via Revocable Sequence Maturity Contracts and how to solve the routing issues via Hashed Time Locked Contracts. These two forms of smart contracts allow for the Blockchain to be transformed from a transaction layer for payments to an enforcing layer of those contracts. Similar to the real world most contracts have never to be enforced via a court ruling but are negotiated bilaterally between consenting parties. In the same sense, we will understand that the Lightning Network reduces the load of the Bitcoin Network significantly by transforming it to be a contract enforcing layer instead of a value transaction layer.

After we understand the core contracts that enable the Lightning Network, we will look at the technologies to define a properly working protocol. We will study the transport layer with its Sphinx mix format and Onion routing first and move on to the gossip protocol which enables the creation of a peer to peer network.

After we understand the technical foundations of the Lightning Network, a practical guide is given. We look at the current wallets, implementations and tools for developers. We create some small Lightning Network applications to demonstrate how easy it becomes with the help of the Lightning Network to accept Bitcoin payments.

Finally, we look at some of the more advanced topics

of the Lightning Network. These are mainly relevant for researchers and developers who want to improve the protocol. We decided to include these topics because it seems plausible that users of the Lightning Network gain a clear picture of current trends and potential future enhancements.

One core principle of this book is that we introduce new concepts by formulating problem statements first. We will then try to understand why these problems existed and how the technologies in this book will be able to solve those problems. In many cases, we will derive more specific problems which we will tackle down in a similar fashion.

Chapter 2

Bitcoin

2.1 Introduction to Electronic Cash

Problem: How can we create a digital form of cash? With the invention of the micro controller which lead to the development of computers, the internet and smart phones we have seen that many things that existed physically exist in a digital version now. Examples could be:

- Photographs, video recordings and music tapes.
- Books, newspapers and other print publications.
- Postal services for sending mail.

- Archives and libraries.

Also a lot of communication has become digitally with services like email or instant messaging. It seems that a huge reason for society to adopt a technological breakthrough is that in many cases digital goods are more convenient than their physical counterparts. Take paper publications as an example: While it might be very convenient to carry around one book it is hardly practical to carry around your entire library. With modern electronic readers, it is possible to access the world's largest collection of textbooks on a single device. One can even easily store the entire Wikipedia - which as an encyclopedia is larger than any encyclopedia that has previously existed - on a small nano SD card. Remember such an SD card is smaller than your thumbnail.

With regard to cash, we can see a similar trend. Due to its sparsity gold served as one of the first universally accepted materials to serve as a currency. However using gold was not too practical as it is a heavy material and cannot be split easily. Physical coins and bills (which in the beginning were backed by gold) emerged. This form of cash is still used in all major countries of the world.[1] Similarly to carrying around a single book it might be highly convenient to carry around a 20 Euro[2] bill in order to buy some groceries. However we hardly see people

[1] althogh currency nowadays is not backed by gold anymore.

[2] or whatever local currency you prefere

caring around 1000 times as much in order to buy a car or even more bills to buy a house. Physical money in large quantities seems to be too cumbersome. The traditional banking sector and financial industry has come up with solutions like wire transfer or cheques. Also we can observe the emergence of online banking, credit cards and online money transfer services. From a perspective of convenience, these services can be seen as a digital form of cash and are similarly convenient for the user like a digital book.

However we should state that while the digital solutions which the financial industry provided might be convenient, they cannot - in fact they must not - be seen as a real form of cash. Physical cash in the form of coins and bills is supposed to be yours if you have it in your pocket.[3] The digital alternatives however do only exist virtually on some computer. From a computer a technical point of view they are just an entry in a third parties database. Thus they are based on trusting this third party. If your digital cash service provider decides to deny you access to your funds or run with your money there is basically nothing you can do.[4] Such a scenario

[3]Technically in most countries the bills and coins belong to the country which issued the cash. However you are entitled to the monetary value printed on those bills. As long as the value of the bills is preserved you can be sure that you are able to spend your cash as long as others accept it.

[4]Of course in most jurisdictions there is the legal system pre-

can easily happen as we have seen with the bankruptcy of the famous bank Lehman Brothers in the summer of 2008. Many people that have trusted their cash to this bank have lost a fortune. While we have to be fair and attest that it was certainly not the fault of their digital and virtual cash systems that they filed for bankruptcy we see that trusting a bank to have a digital form of cash removes the most important property of cash. The fact that you (and only you) will own it. But the reason banks existed was not only to be a provider of a digital form of cash. They already existed before the digital age because people did not want to carry around vast amounts of money.

So the question remains: Can there be a better form of digital cash in comparison to the solution provided by the traditional banking industry?

Similarly to our example of e-books and physical cash (which we carry around with us) this form of digital or electronic cash should be stored on the digital device of the user. Thus it becomes just a piece of information. In this way the user is not dependent on a trusted third party.[5]

However computers and digital services seem to have

venting them from stealing your money.

[5]Of course as bitcoin and Lightning Network developers we should be aware of the fact that we still trust the hardware producers and the software of our operating system and the consensus mechanisms of the network and protocol.

a fundamental property that might make them useless for electronic cash systems. Information can easily be duplicated by copy and pasting. We remember that gold was used as one of the first mediums of exchange since it could not be duplicated.

To emphasize this issue again: A physical bill is actually transferred when making a payment. In contrast when spending a digital coin - as a piece of information - it can just be copied and duplicated. The recipient has no chance of knowing that the sender actually deleted the coin. If the sender did not delete the coin the sender would be able to spend the coin again by copying the information to another person. This process is called double spending. Obviously double spending sabotages the property that cash should act as a store of value. As the supply would be infinite a single coin would always be worthless.

We can conclude that electronic cash is only useful if we solve the problem of double spending electronic coins and create a limited supply of electronic coins.

One obvious solution is a central authority or custodian who understands who owns which coins and who allows cash transactions only if the sender has enough cash. While this solution works and is already implemented by traditional banks it does not solve our desire that we carry around our electronic coins in our devices and - even worse - we still need to trust third-party service with all the risks that we have experienced with the

collapse of Lehman Brothers.

Luckily in late 2008 a person or group under the pseudonym Satoshi Nakamoto published the Bitcoin paper. This major technological breakthrough showed the world how it would be possible to create a decentralized form of electronic cash in which every participant stores their own funds and copying those coins does not mean duplicating them (as only one copy can be spent).

2.2 Proof of Work and Blockchain

2.3 Scalability issues of blockchain technologies

Chapter 3

Lightning Network

Chapter 4

Practical guide

4.1 Lightning Wallets

4.2 Lightning Nodes

4.3 Lightning Application Development

4.4 Useful Applications and Tools

Chapter 5

Advanced Topics

- spam the blockchain

Chapter 6

Controversial topics

6.1 Consequences of decentralization

6.2 Custodial Services, Lightning hubs and banks

6.3 Privacy and regulatory challenges

6.4 Consensus, Forking and Altcoins

Appendix A

Cryptography

A.1 ECDSA

Once upon a time... This document shows how you can get ePub-like formatting in LaTeX with the `memoir` document class. You can't yet export directly to ePub from writeLaTeX, but you can download the source and run it through a format conversion tool, such as `htlatex` to get HTML, and then go from HTML to ePub with a tool like Sigil or Calibre. See `http://tex.stackexchange.com/questions/16569` for more advice. And they lived happily ever after.