SoK: Scalability of Blockchains

Mechanism Labs
Maaz Uddin, ...

September 2018

Abstract

TODO

1 Introduction

On November 28th, 2017, innovation studio Axiom Zen launched a product whose goal was to help build a better onboarding system of the Ethereum network. Cryptokitties took the cryptocommunity by storm, demonstrating that there were viable applications for consumers that could be deployed on blockchains. But more importantly, the success of the game proved a long-held view of distributed ledger technology systems - they weren't ready for real world applications. Cryptokitties began to clog up the ethereum network, leading to a "sixfold increase in total network requests" [1]. This made one thing clear, today's blockchains are not ready to scale for tomorrow's society.

1.1 Problem Definition

The emergence of blockchain technology has brought with it the ability to replace trusted third party intermediaries by disruping the current financial climate. Its potential applications offer a variety of uses that provide more accountability and require less trust to achieve. Blockchains put an emphasis on mitigating trust and giving power to the end-users through decentralization. They also stress strong tamper-evident and immutable characteristics via security implementations.

Current blockchains, however, are not scalable. The two most popular blockchains, Bitcoin and Ethereum, can only process upto 7tps and 15tps (transactions per second), respectively [**?**, **?**]. Whereas centralized entities today, like Paypal and Visa, can offer upto 450tps [2] and 56,000tps [3] - magnitudes of order more than most blockchains. If blockchains are to replace the current antiquated systems, then we must find a way to allow them to match the increasing demand of transactions in our world today. This then poses the question: How?

There are a myriad of scalability solutions today: off-chain solutions, alternative consensus, network changes etc. This paper aims to give an understanding of the various popular scalability solutions and the feasibility of each. We analyze each possible solution by looking at which layer(s) in the blockchain the solution lies. This is a key forethought, because in order to truly scale public blockchains, we must implement solutions at each layer of a blockchain. It is insufficient to scale just one layer.

2 Background and Related Work

TODO

3 Scalability Solutions From Different Perspectives - the Blockchain Stack

Like the internet, blockchains are divided into different layers. Each layer deals with a series of tasks that are required for the blockchain to run. The layers operate within themselves, but rely on the layers beneath them to operate correctly. This separation of responsibility instills a common computing paradigm known as abstraction.

The beauty of abstraction is that you can reinvent different aspects of each layer independently without necessarily worrying about how it might affect the other layers (so long as the endpoints connecting the layers are still intact). This allows us to ignore lower layer dependencies by simply considering them as a "blackbox".

This is a key consideration when diving into the scalability problem. Because many of the layers of blockchains are partitioned in such a way, we can isolate certain problems to specific layers and work towards making them more efficient without complicating the process with extraneous factors[1]. Below, we touch upon each layer of the blockchain stack starting from the bottom and moving up - Hardware, Network, Consensus, Sybil Control, and Application. We will then go into more detail about each layer in later sections, discussing the various solutions existing in each layer or how they may overlap over multiple layers.

3.1 Hardware

TODO

3.2 Network

TODO

3.3 Consensus

TODO

3.4 Sybil Control

TODO

3.5 Application

TODO

3.6 Non Blockchain Solutions

TODO

4 Hardware

TODO

[1] It is important to note that good scalability should consider scalable solutions at all layers and how they work in cohesion rather than in separation

5 Network

TODO

5.1 Block Size and Time

TODO

5.2 Segregated Witness

TODO

5.3 Light Clients

TODO

5.4 Sharding

TODO

5.5 Bitcoin-NG

TODO

6 Consensus

TODO

6.1 Alternative Consensus

TODO

6.1.1 Proof-of-Stake Based

TODO

6.1.2 Other Proof-of-X Protocols

TODO

7 Sybil Control

TODO

7.1 Proof-of-Work

TODO

7.2 Proof-of-Stake

TODO

8 Application

TODO

8.1 State and Payment Channels

TODO

8.1.1 Lightning and Raiden

TODO

8.1.2 Plasma

TODO

8.1.3 Truebit

TODO

8.2 Sidechains

TODO

8.3 Overlays

TODO

9 DAGs

TODO

9.1 GHOST, SPECTRE, PHANTOM

TODO

9.2 Avalanche

TODO

10 Gossip Protocol

TODO

10.1 Hashgraph

TODO

10.2 bloXroute

TODO

11 Discussion

TODO

11.1 Layer 2

TODO

11.2 Proof-of-Stake

TODO

11.3 Network

TODO

11.4 Non Blockchain Solutions

TODO

12 Conclusion

TODO

References

[1] ConsenSys. *The Inside Story of the CryptoKitties Congestion Crisis*, February 20, 2018

[2] 5 Things PayPal Holdings Inc Wants You to Know. *https://www.fool.com/investing/general/2016/02/04/5-things-paypal-holdings-inc-wants-you-to-know.aspx*

[3] Visa Inc. at a Glance. *https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf*