Proposal: A survey of data transfer and storage techniques in prevalent cryptocurrencies and suggested improvements

Sunny Katkuri

1 Survey of wire protocols

Methodology

There is no known similar work at the moment. A tentative list of cryptocurrencies that will be considered:

- Bitcoin, Bitcoin Cash and Litecoin: The protocol is well documented and will be re-summarized to fit the context of this document. This specification will be used as the reference for the rest of the protocols.
- Ethereum: The protocol is specified in parts in multiple wikis. The Falcon network decentralizatoin paper had to even look at reference implementations [1].
- Ripple: The whitepaper does not cover discovery or transfer. Information will have to be extracted from rippled, the canonical node implementation [2].
- DAG protocols
  1. IOTA: The Tangle paper [3] does not delve into wire specifics, this information will have to be extracted from code.
  2. Nano: Network specifics are vaguely mentioned in a wiki [6]. There is no known examination of what a block lattice structure [5] actually entails in terms of bandwidth.
- Hashgraph: Though not a cryptocurrency, hashgraph [4] is being presented as a viable alternative to blockchains and DAGs. It is interesting to look at the implementation-level implications of *gossip about gossip* and *virtual voting*.

Submit by: Feb. 16, 2018

2 A well-documented and generalized crawling library

Methodology

Crawlers have been published for Bitcoin [7, 8]. Analysis and visualizations are also similarly focused on Bitcoin and friends [9, 11]. The most popular node explorer for Ethereum is not open-source [10]. The goal of this section will be to publish a python module which encapsulates known topology discovery methods and implements new ones where needed. This module should be able to produce results in multiple output formats. An additional goal is to have a website which unifies maps and visualizations for all currencies under consideration.

Submit by: Mar. 2, 2018

3 Analysis of collected data

Methodology

This section is contingent on our crawler accumulating meaningful data. The primary sources for the work done here will be the methods outlined in papers such as Hijacking Bitcoin and others [12, 13, 14]. We will evaluate how these methods carry over to the P2P networks of the other currencies under consideration.

Submit by: Mar. 9, 2018

4 Improving data transfer efficiency

Methodology

Identify duplicate data transfers in the implementations of the currencies under consideration. Evaluate how techniques like Graphene [16] , compact blocks [15] and filters [18] and relay networks like Fibre [17] and Falcon [19] carry over to the other networks. Falcon does this for Ethereum already.

Submit by: Mar. 23, 2018

5 Contribute to current Ethereum research: Survey of sharding techniques

Methodology

Provide a comprehensive account of different sharding proposals [23, 24] till date and other scaling solutions like Raiden [20] and Lightning Network [21]. We will try to understand the reasoning behind the current state of the Ethereum sharding proposal [22]. An additional goal will be to become an active participant in the discussions surrounding the implementation roadmap.

Submit by: Mar. 30, 2018

6 A general purpose sharding simulation

Methodology

There is no current published project which provides a platform to simulate the effects of different sharding proposals. This platform's aim would be to provide an abstracted view of a blockchain with all the sharding primitives built in. The key goal will be to make the system intuitive and visual and provide an easy interface to tune different parameters.

Submit by: Apr. 6, 2018

7 Survey of data storage techniques

Methodology

This section will examine how transactions and blocks are stored and accessed on disk.

- Bitcoin, Bitcoin Cash and Litecoin: Specify the LevelDB [25] schemas and the code paths in which they are accessed. This specification will be used as the reference for the rest of the protocols.

- Ethereum: Describe the various tries [26] and how they translate to LevelDB schemas.

  Other currencies will be described as and when they are studied.

Submit by: Apr. 20, 2018

8 Improving data storage efficiency

Methodology

Implement Gavin's proposal [26] for UTXO protocols and evaluate its effects.

Submit by: May 4, 2018

References

[1] https://arxiv.org/pdf/1801.03998.pdf

[2] https://github.com/ripple/rippled

[3] https://iota.org/IOTA_Whitepaper.pdf

[4] http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

[5] https://raiblocks.net/media/RaiBlocks_Whitepaper__English.pdf

[6] https://github.com/clemahieu/raiblocks/wiki/Network-usage

[7] https://github.com/ayeowch/bitnodes

[8] https://github.com/shazow/btc-crawl

[9] https://cash.coin.dance/nodes

[10] https://www.ethernodes.org

[11] https://bitinfocharts.com/bitcoin/nodes-active/

[12] https://arxiv.org/pdf/1605.07524.pdf

[13] https://cs.umd.edu/projects/coinscope/coinscope.pdf

[14] https://www.sciencedirect.com/science/article/pii/S187705091400742X

[15] https://github.com/bitcoin/bips/ blob/master/bip-0152.mediawiki

[16] https://people.cs.umass.edu/ gbiss/graphene.pdf

[17] https://github.com/ bitcoinfibre/bitcoinfibre

[18] https://github.com/bitcoin/bips/blob/master/bip-0037.mediawiki

[19] https://www.falcon-net.org/

[20] https://raiden.network/

[21] https://lightning.network

[22] https://github.com/ethereum/sharding/blob/develop/docs/doc.md

[23] https://dl.acm.org/citation.cfm?id=2978389

[24] https://arxiv.org/abs/1611.06816

[25] https://en.bitcoin.it/wiki/Bitcoin$_{C}ore_{0}.11_{(}ch_{2})$ $:_{D}$
$ata_{S}toragehttps://easythereentropy.wordpress.com/2014/06/04/understanding - the - ethereum$

[26] https://gist.github.com/gavinandresen/e9177aae1183226937fca8e8cbfc5f79