Advanced Blockchain Storage.

The interplanetary File System (IPFS)

The IPFS file system is a peer-to-peer distributed file system which goal is to connect all devices with the same file system. The idea is to provide a high through-put content-addressed block storage model with content-addressed hyperlinks. This structure will form a generalized Merkle DAG, and using this structure is possible to build versioned file systems, blockchains …. Other peer-to-peer file-system applications were the well-known Napster, KaZaA and Bit Torrent. Nowadays BitTorrent maintains a massive deployment with millions of nodes. The problem is that these applications were not designed as infrastructures to built upon. IPFS combines different properties as: (i) Distributed hash tables that are used to coordinate and maintain the metadata about the peer-to-peer systems, (ii) BitTorrent features as BitTorrent exchange protocol strategy, how BitTorrent track the availability of file pieces, (iii) version control system, (iv) a self-certified filesystem (SFS) that proposes an implementation of a distributed trust chains and egalitarian shared global namespaces. Finally, IPFS protocol is divided into a stack of sub-protocol responsible for different functionality to manage and maintain : (i) managing node identity, (ii) manage the connection to other peers, (iii) maintaining the information in order to locate specific peers and object, (iv) a block exchange protocol (BitSwap) that governs block distribution, (v) to manage and maintain a Merkle DAG of content-addressed immutable objects with links, (vi) a file system inspired by Git, and (vii) a self-certifying mutable name system.

Other important goals of the IPFS file system are: (i) IPFS content needs to be able to move as fast as the underlying network permits, (ii) nodes be able to store and/or distribute content they explicitly want to store and/or distribute, and (iii) nodes will be able to express policies and subscribe to networks that allow/deny lists and policies that express content storage and distribution requirements.

A Secure Sharding Protocol for Open Blockchains

The authors of this paper propose a new distributed agreement protocol for permission-less blockchains called ELASTICO. This protocol scales transaction rates almost linearly using available computation for mining. The idea behind this is to use the computation power of the network to increase the number of transaction blocks selected per unit time. This protocol makes partitions or parallelizes the mining network into smaller committees, each of which processes a disjoint set of transactions called shards. The number of committees grows near linearly in the total computational power of the network. Each committee can run a classical byzantine consensus protocol to decide whether their agreed set of transactions. This protocol has different challenges as: (i) processors have no inherent identities or external PKI to trust, so a malicious processor can thus simulate many virtual processors and therefore create a large set of siblings, (ii) run a sharding protocol among the identities with a fraction of them are byzantine, and (iii) must assure that an adaptive adversary observing all the protocol runs does not gain significant advantage in biasing its operations or creating siblings identities.