Advanced Blockchain Storage
IN5420 Distributed Blockchain Technologies

Michael Eikeland

April 2018

1 IPFS

IPFS (InterPlanetary File System) is a distributed file system that uses technology and primitives commonly assosciated with blockchain technology. Amongst its goals is the vision to create a more permanent and persistent alternative to the Web. The IPFS Protocol is split into several sub-protocols that have different levels of abstraction in order to be able to use different underlying protocols. The sub-protocols are Identities, Network, Routing, Exchange, Objects, Files and Naming.

In IPFS nodes have identities (cryptographic hash of a public key), in order to give users their own namespace in the file system and to let them gain credibility or favor. This, in turn makes the system able to resist Sybil attacks.

IPFS has content-addressed objects, which means that its objects (e.g. files) are addressed (identified/named) after their contents using cryptographic hashes. This means that these objects have several interesting properties. For one, it means that the objects are immutable - if the contents of an object change, so does its address. But it also means that if in the distributed file system two objects have the same contents, they are redundant and replication can be limited. Users can *pin* these objects in order to make a persistent copy to their local storage.

To keep track of all objects, nodes maintain a DHT (Distributed Hash Table) containing the address of objects. This can be shared with other peers in the IPFS network and allow nodes to share their objects.

2 Elastico

Elastico is an alternative consensus protocol with a goal of scaling Bitcoin transaction throughput through sharding. This protocol assumes that Bitcoin consists of n processors that each have a fraction of the network's total computational power, f. It differs from Nakamoto consensus in that consensus is achieved through committees, a subset of processors, that agree on a subset of transactions. The committees and the subset of transactions are determined by a PoW (Proof-of-Work) that the processors find. The committees are of such a size that regular BFT algorithms can be used. Once a committee agrees on what transactions are valid, they are sent, with proof and signatures, to the ”final committee”. This committee that collects the results of all other committees and generate a block. According to the authors of Elastico, its performance in transaction throughput is linearly proportional to the total computational power of the network, which is an substantial improvement over Bitcoin’s current throughput of maximum 7 tx/sec.