Bitcoin Overview

Topic summary

by Michael Eikeland

Central to Bitcoin is the concept of decentralization. Not having to rely on a trusted third-party authority (centralized) is one of the pillars of foundation in Bitcoin. This reveals several technical challenges: *Who maintains the ledger of transactions? Who has authority over which transactions are valid? Who creates new bitcoins?*

Consensus is an implicit challenge to overcome when talking of achieving decentralization. Consensus in a more general context is a fairly mature field of research in which there notably has there been several impossibility results. This has raised concerns around the viability of the Bitcoin consensus protocol. These impossibility results are however tied to very specific models that can not necessarily be compared to the characteristics of Bitcoin. Through observation of the Bitcoin network we can see that, though far from perfect, there is a working consensus protocol, though we may not be able to reaffirm under what assumptions and conditions it is optimal and working as desired.

A more technical in-depth explanation of Bitcoin's consensus protocol is that the proof-of-work model ensures that anyone can verify the integrity of a new block based on the existing shared state of facts. Because of the cryptographic properties used in the implementation. An untamperable blockchain is achieved, essentially guaranteeing the history of all transactions for every new block. Because of the resource intensive nature of the consensus algorithm, namely solving crypto puzzles, it is hard to perform persistent, lasting or impactful attacks against the network. Because it is resource intensive (in other words costly), the incentive to perform this work is that one claims a predetermined amount of bitcoins.

The Bitcoin ledger is a blockchain. It consists of an append-only chain of blocks that are linked together by including the "hash" of the previous block. Because the hash value is directly linked to the data of the block it implicitly provides security and tamper resistance in that an attacker would have to perform an infeasible amount of work in order to alter the ledger's history. The data-part of the block are the transactions that users on the Bitcoin network announce. Blocks are periodically produced with the goal being that the network produces a new block every 10 minutes on average. Every transaction may have multiple input and output addresses. It also specifies a script, a routine that describes under what conditions and the transaction is valid and redeemable.

While Bitcoin offers a lot of the same as traditional financial institutions offer it has some limitations. There have been questions regarding the lifetime of Bitcoin due to its use of cryptography. At the time of writing it is only allowed to handle a throughput of 7 transactions per second. However, the majority of the network decides the rules of the protocol, and new rules, changes and improvements can be implemented through forks.