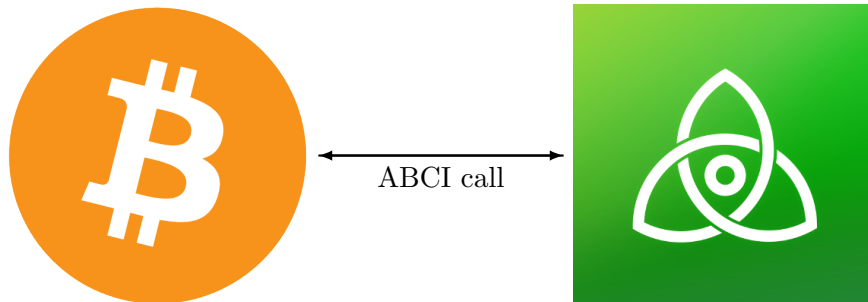




Bitcoin on Tendermint

Bitcoin is the first successful cryptocurrency, and has been running since early 2009. Bitcoin famously uses a lot of global electricity to run its proof of work based “Nakamoto Consensus” algorithm to extend its blockchain. Alternate cryptocurrencies have proposed an idea called *proof-of-stake*, which can run without using much electricity. We want to explore the idea of keeping the rest of Bitcoin’s properties, but replacing the proof-of-work system with a proof-of-stake system.

Tendermint is a proposed proof-of-stake system that implements just the consensus algorithm, but leaves the rest of the system for application developers to flesh out. On top of Tendermint’s consensus algorithm and its related API, we want to implement Bitcoin’s cryptocurrency aspects like the UTXO set, signature based spending, blockchain, multi-sig, advanced scripting, etc.



Requirements: This project involves understanding Bitcoin, and being able to separate its consensus layer from the rest of its cryptocurrency aspects. It involves learning about Tendermint’s Application Blockchain Interface (ABCI), and being able to implement Bitcoin’s features using this ABCI.

Programming knowledge of Go would be a plus, as Tendermint Core is implemented in Go. The ABCI is generic and other languages are supported as well.

Interested? Please contact us for more details!

Contact

- Tejaswi Nadahalli: tejaswin@ethz.ch, ETZ G97