DeFi
AND THE
Future
of Finance

Course I:

DeFi Infrastructure

1. The History of Decentralized Finance

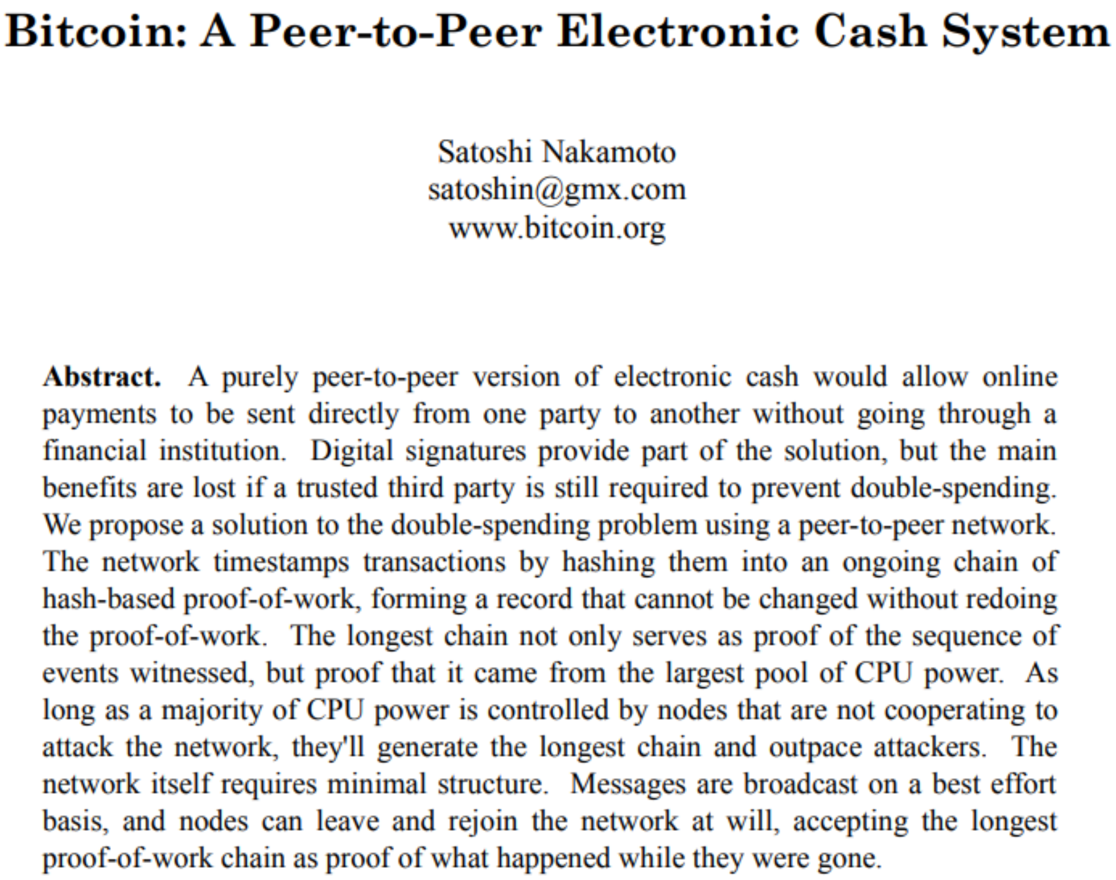
(v) Crypto Origins

Origins of DeFi

Bitcoin and cryptocurrency

- Stuart Haber and Scott Stornetta (1991) invent the blockchain idea to keep track of time stamping of documents
- Adam Back (2002) invents the Proof of Work idea. It is based on a key paper by Cynthia Dwork and Moni Naor (1992) that was aimed at eliminating junk mail (require the sender to do a computational task to send the email to you, while this is easy to do once – it is infeasible to do for millions of recipients)
- Satoshi Nakamoto (2008) put these ideas together to introduce bitcoin

Origins of DeFi



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

White paper October 31, 2008.
Program launched January 3, 2009.

Origins of DeFi

Bitcoin and cryptocurrency

- Bitcoin eliminated the key problem with digital currencies in the past (you can make a perfect digital copy and “double spend”)
- Every transaction would be kept in an immutable ledger (censorship resistant blockchain) and the ledger would be distributed across many different computers
- Cryptographic scarcity was enforced by a limit of 21 million bitcoins
- User sovereignty (only owner determines how to spend)
- Portability in that you can send or receive anywhere quickly and cheaply

Origins of DeFi

Comparison to fiat

- US dollar since 1971 is a pure fiat currency
- Demand comes from:
    - 1) taxes;
    - 2) purchase of goods denominated in USD; and
    - 3) repayment of debt in USD
- US economic expansions and contractions impact value
- Fed also has the ability to inflate

Origins of DeFi

Bitcoin vs. fiat

- Scarcity and self-sovereignty create the potential for store of value
- While untested, there is no direct link to economic activity or inflation, so there could be some hedging
- Bitcoin was originally intended to be a peer-to-peer currency. However, its deflationary characteristics and flat fees discourage its use in small transactions.
- Bitcoin is a flagship for other innovations in the crypto space

Ethereum and DeFi

Ethereum history

- Began in 2015 with Vitalik Buterin
- Allows for running of computer programs. So Ethereum is a distributed computational platform offering functionality via offering a “smart contract platform”
- Smart contracts control assets and data, and define interactions between assets, data, and network participants

Ethereum and DeFi

dApps

- Decentralized applications allow peers to interact directly and remove the need for a central clearing house for app interactions
- DeFi is fundamentally a competitive marketplace of financial dApps that function as various financial “primitives” such as exchange, lend, tokenize, and so forth.
- These dApps benefit from the network effects of combining and recombining DeFi products, and attracting increasingly more market share from the traditional financial ecosystem.

Next module

- Explore the details of the DeFi foundations including blockchain, cryptocurrency, smart contracts, oracles, stablecoins, and decentralized applications