
Discussion of
Cryptocurrencies and Decentralized Finance
-- Igor Makarov and Antoinette Schoar

Eswar Prasad

Cornell University, Brookings Institution, and NBER

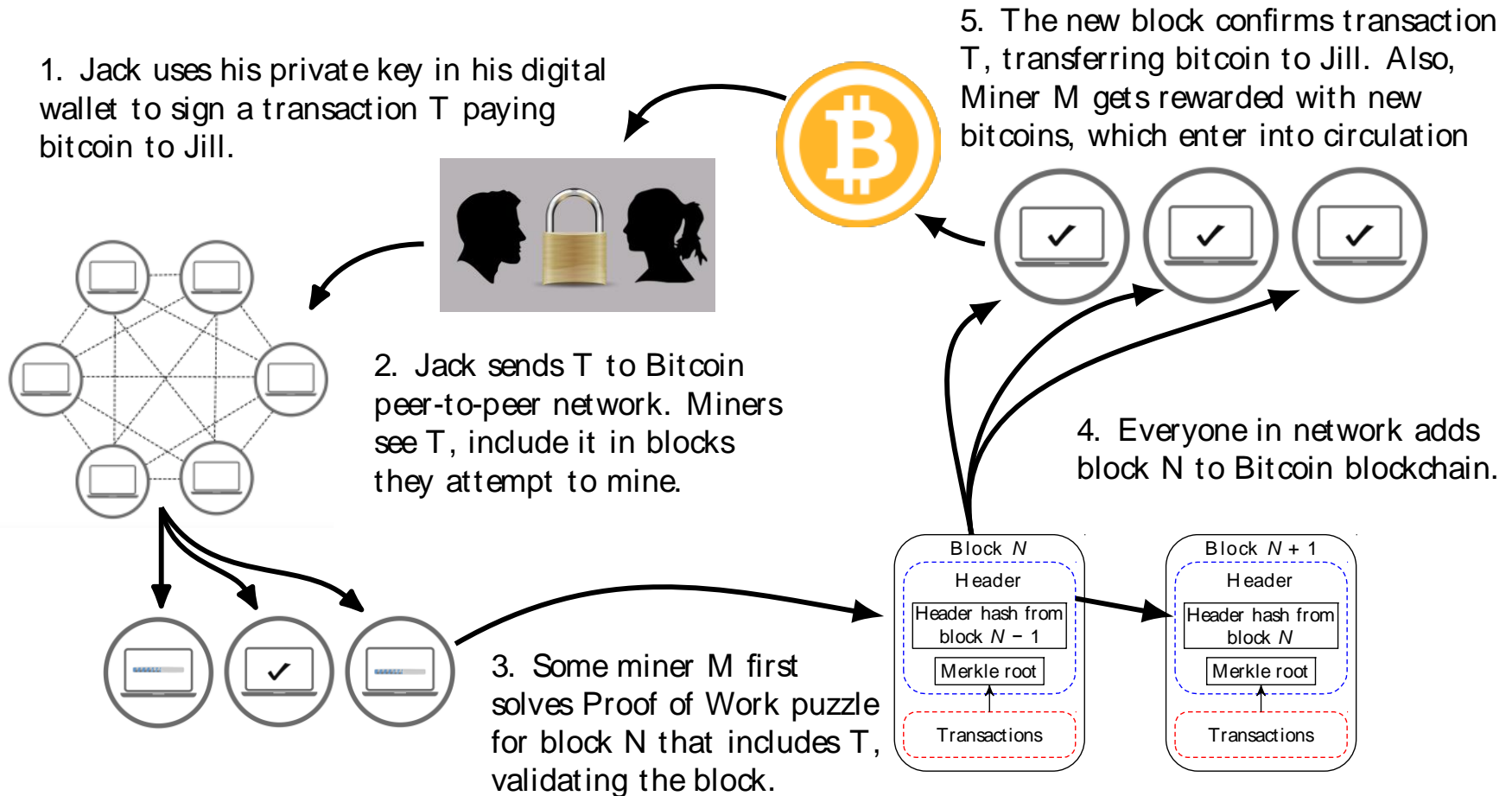
Bitcoin Sets Off a Revolution

- A system for electronic transactions without relying on trust
 - No trusted third parties or intermediaries
 - Using only digital identities (pseudonymity)
-

Technical Challenges

- Validating transactions without trusted party
 - Achieving consensus in decentralized manner, without trusted authority
 - Need easy, quick verifiability
 - Ensure immutability of transactions
 - Prevent double spending of digital currency
-

Figure 4–3. How Bitcoin Works



Bitcoin: The Bad

- Crummy medium of exchange
 - Unstable value
 - Slow processing time, low transaction volumes
 - Fuels dark web, illicit activities?
 - Weak anonymity
 - Lost Bitcoin: misplaced private keys
 - Speculative financial asset (scarcity value? Cap of 21 million Bitcoins)
 - Proof of Work damages the environment
-

Stablecoins

- Objectives: financial inclusion; faster, cheaper cross-border payments; efficient use of fiat currencies (thru tokenization)
 - Value to be backed by reserve assets (specific currency; basket of hard currencies)
 - Private, centralized verification
 - Concerns:
 - Shadow money flows (contra AML/CFT regulations)
 - Lack of regulatory oversight
 - Monetary policy implications
-

Key Elements of DeFi

Decentralized blockchains have

- Decentralized architectures: no centralized point of failure
- Decentralized governance: control rests with members of network, not central authority
- Decentralized trust: trust achieved through public consensus mechanism

But system is logically centralized—entire network of nodes that make up system linked and in commonly agreed-to state at all times.

DeFi Features

Advantages of decentralized systems:

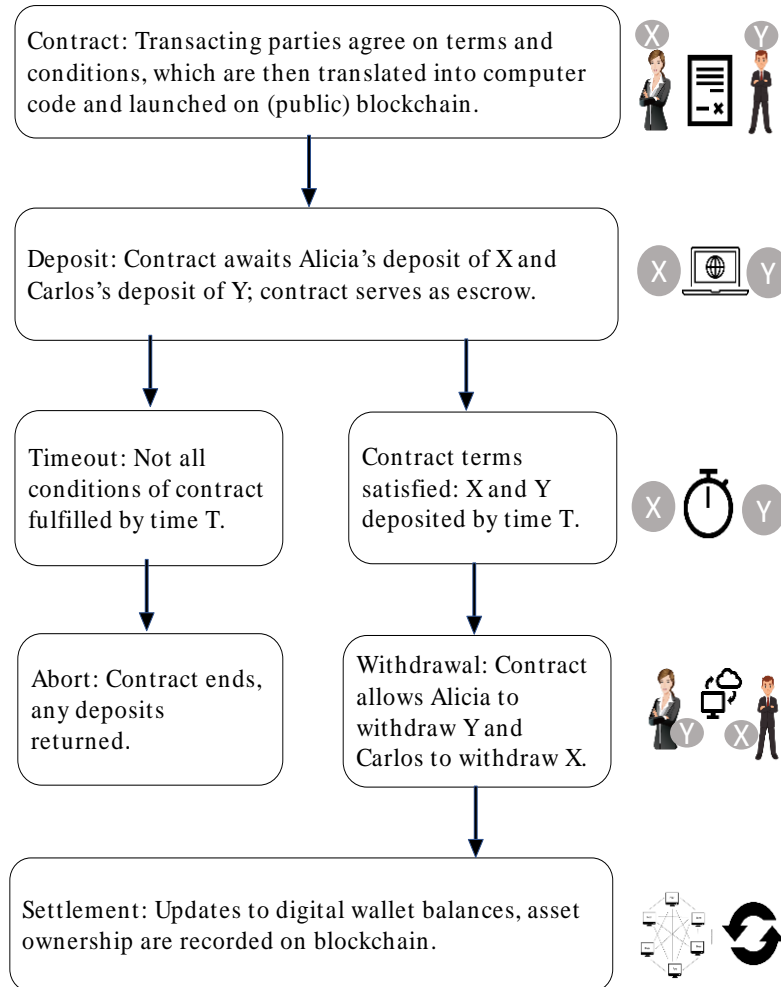
- Fault tolerance: no single point of failure
- Attack resistance: no central point vulnerable to attack
- Collusion resistant: difficult to collude

Features of decentralized system:

- Permissionless (anyone can use it)
 - Censorship resistant (no one can stop it)
 - Open (anyone can verify the execution of a transaction)
-

Figure 5-1. How a Simple Smart Contract Works

Alicia and Carlos want to swap X for Y, respectively, by time T (X and Y are digital tokens representing assets or payment).



DeFi in Practice

Smart contracts

Flash loans

- All elements of contract executed serially in batch operation on Ethereum: initiated, executed, and completed in a flash
- No collateral requirements; no default or liquidity risk
- Can be used for arbitrage

Liquidity mining (or yield farming)

- Compound: blockchain-based borrowing and lending app
-



DeFi: Financial Legos

Permissionless composability: Open-source technology enables connecting applications to build new financial products, services

User deposits cryptocurrency into loan contract, withdraws stablecoins collateralized by that deposit, puts stablecoins in yield-bearing contract. Multiple users pool stablecoins, build savings game—all of interest earned on pooled stablecoins awarded to lucky winner, others get initial deposits back.

- Open source aspect helps identify, eliminate security and other risks
- Compliance tools can also be “plugged in”

DeFi Risks

- Default and liquidity risk mitigated (in principle)
 - Technological vulnerabilities
 - Smart contract risk, larger attack surface
 - Front-running on certain protocols
 - Decentralized governance
 - Oracle vulnerabilities (on-chain to off-chain data transmittal)
-

(Why) Do We Need Cryptocurrencies, DeFi?

- ❑ Financial inclusion
 - ❑ Better payment systems: domestic, international
 - ❑ Lack of competition, innovation
 - ❑ Economic rents (concentration, inefficiencies, regulatory capture)
-

Policy/Regulatory Considerations

- Monetary policy
 - Implementation
 - Transmission
 - Financial stability
 - Spillovers into traditional finance
 - Integrity of financial system
 - External sector stability
 - Investor protection
 - Data -- privacy, confidentiality
-

Meta Issues

- ❑ What role for governments/regulators? Government's role not obvious in areas where private sector has efficiency advantage
 - ❑ Regulation that facilitates innovation but can identify and control systemic risks
 - ❑ How to ensure financial stability if traditional financial institutions (esp. commercial banks) decline in importance
 - ❑ Democratization of finance or greater concentration of wealth if benefits captured by large players/economic elites?
-