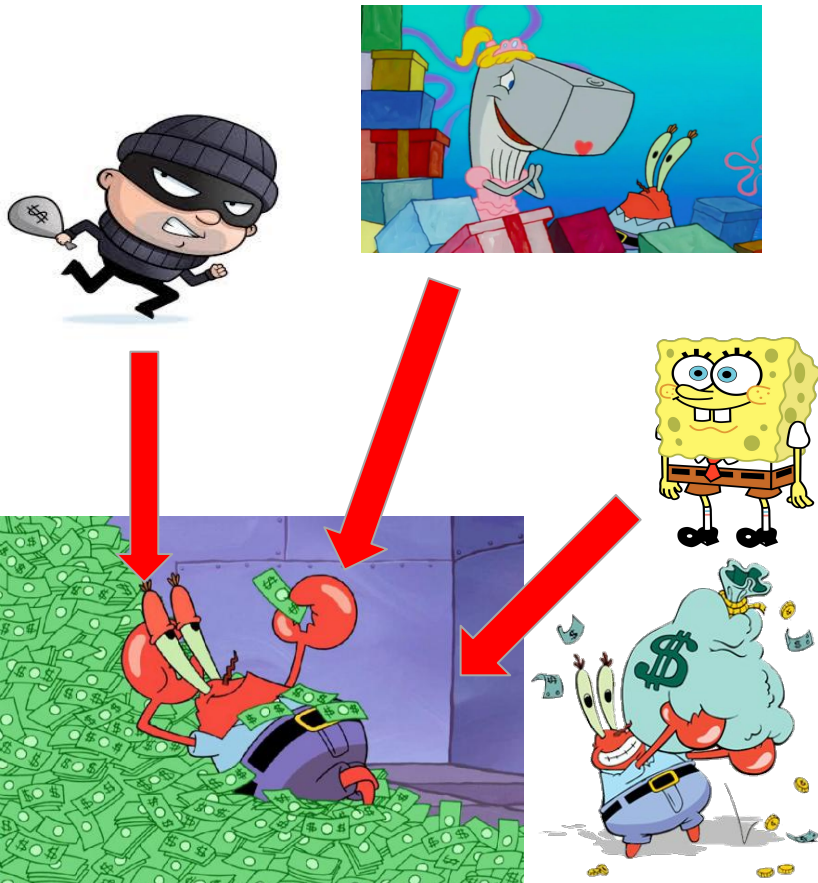
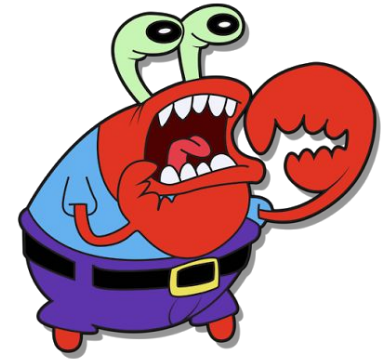

Resource-backed Cryptocurrencies

— Ghada Almashaqbeh —
Columbia University

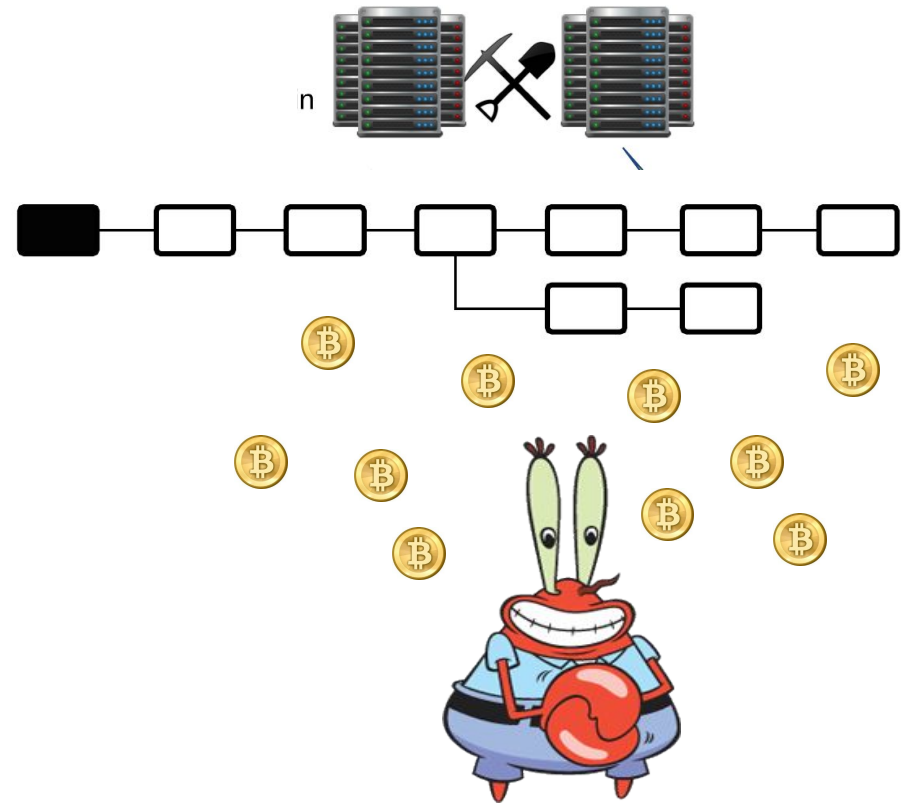
Nov. 2018

Once Upon A Time

Centralized Currency



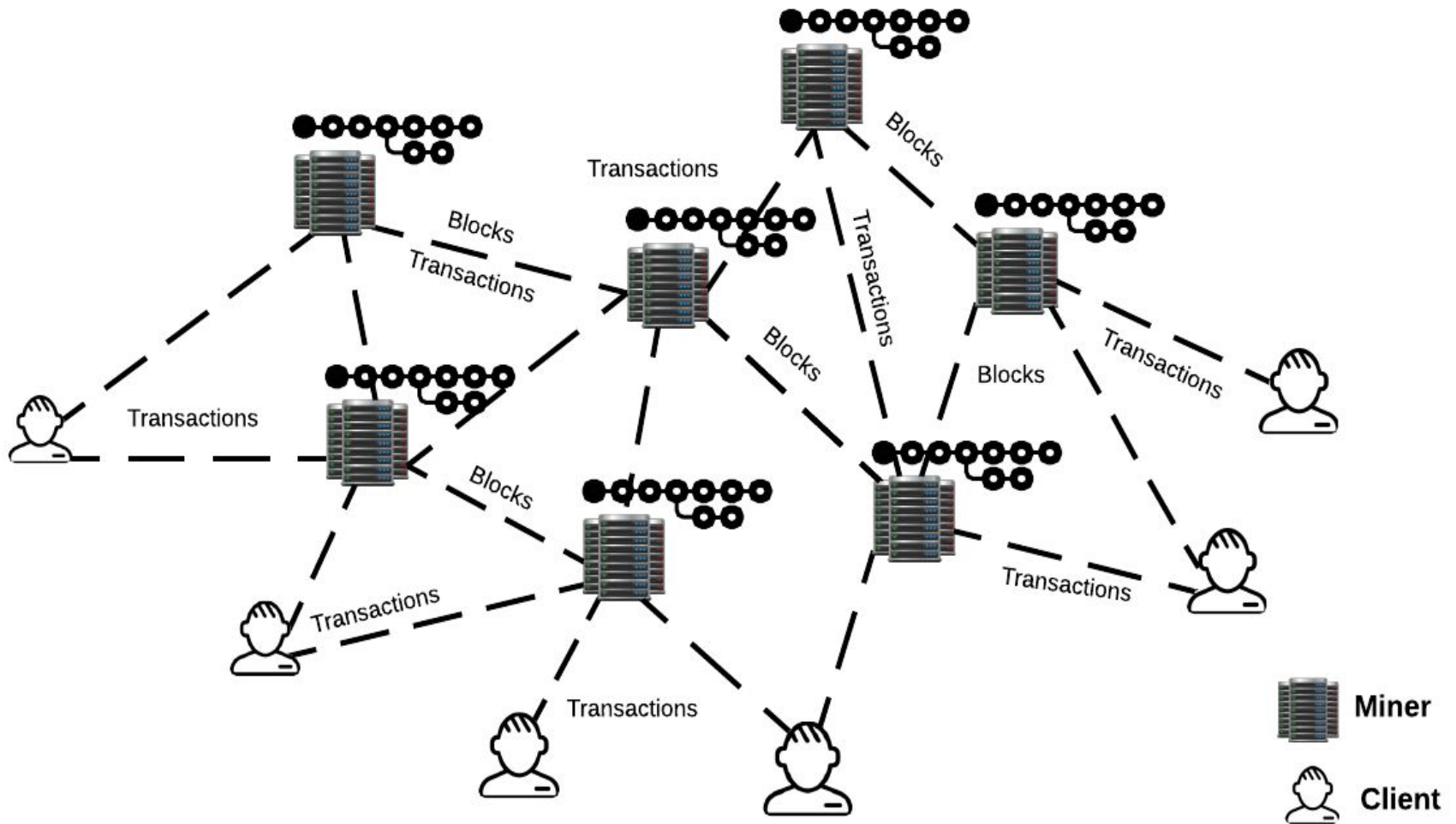
Decentralized Currency



Cryptocurrencies in a Nutshell

- A distributed currency exchange medium open to anyone to join.
- Utilize basic cryptographic primitives to control the money flow in the system.
- Main components:
 - **Players:** miners and clients.
 - **Transactions:** messages exchanged.
 - **Blockchain:** an append only log.
 - **Mining:** extending the blockchain.
 - **Consensus:** agreeing on the current state of the Blockchain.

Cryptocurrency Pictorially



Are we Satisfied?

- Do cryptocurrencies support only a currency exchange service?

That was just the beginning!

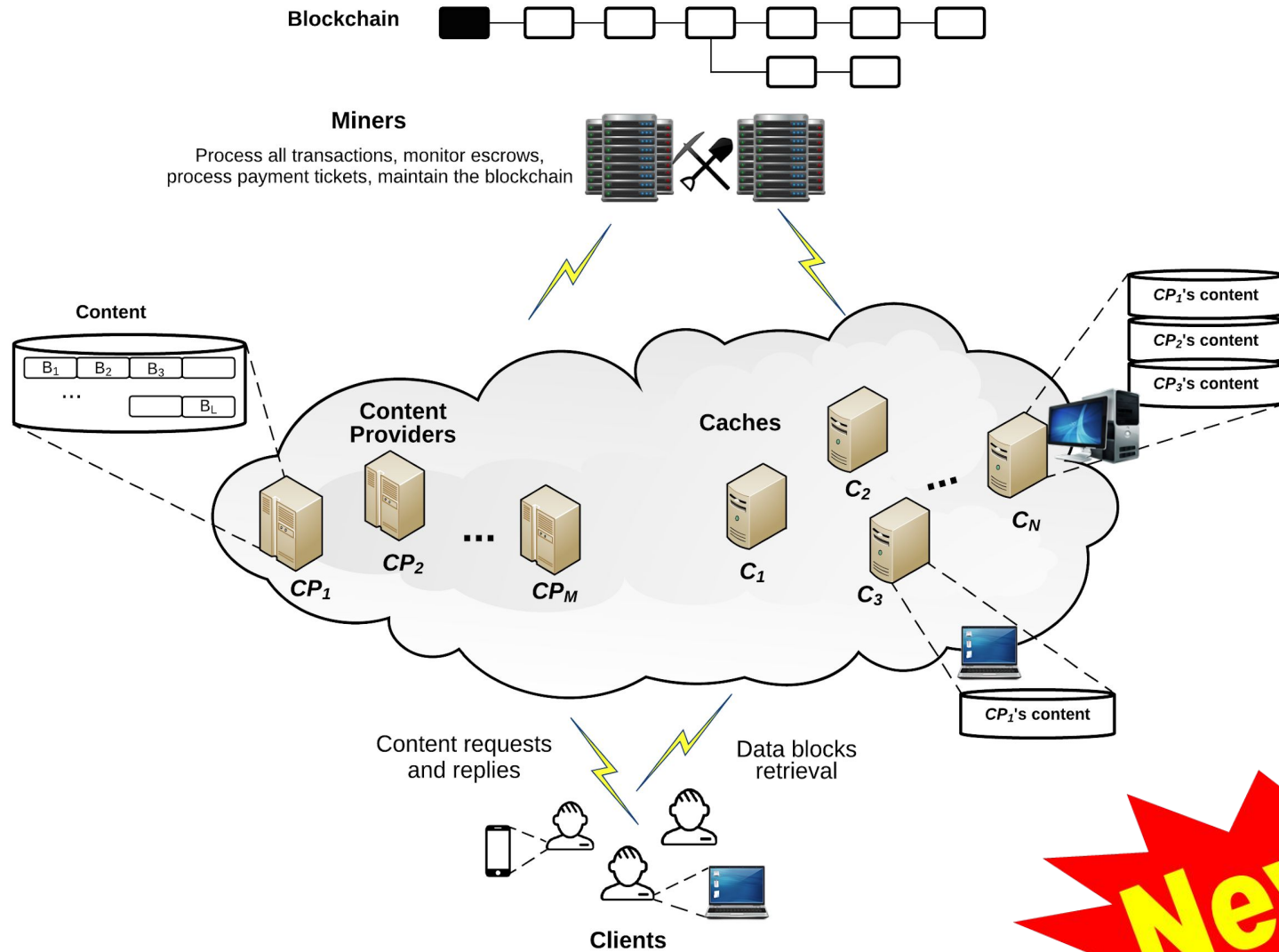
Resource-backed Cryptocurrencies

- Cryptocurrencies backed by a resource such as computation, storage, etc.
- The system provides a distributed service on top of a currency exchange medium.
- Anyone can participate in providing the service for others in order to collect cryptocurrency payments.
- Think of it as a monetary-incentivised distributed service system.

Examples

- Distributed file storage networks.
 - Filecoin, Storj.
- Computation outsourcing network.
 - Golem.
- Distributed video transcoding service.
 - Livepeer.
- And many more ...

CacheCash - A distributed CDN Service



New!

Several Building Blocks

- **ABC**
 - A cryptocurrency-focused threat modeling framework.
- **CAPNET.**
 - A Defense Against Cache Accounting Attacks on Content Distribution Networks.
- **MICROCASH.**
 - A practical decentralized micropayment scheme.
- And **CACHECASH.**

Questions?