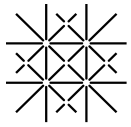


University of Basel

Center for Innovative Finance

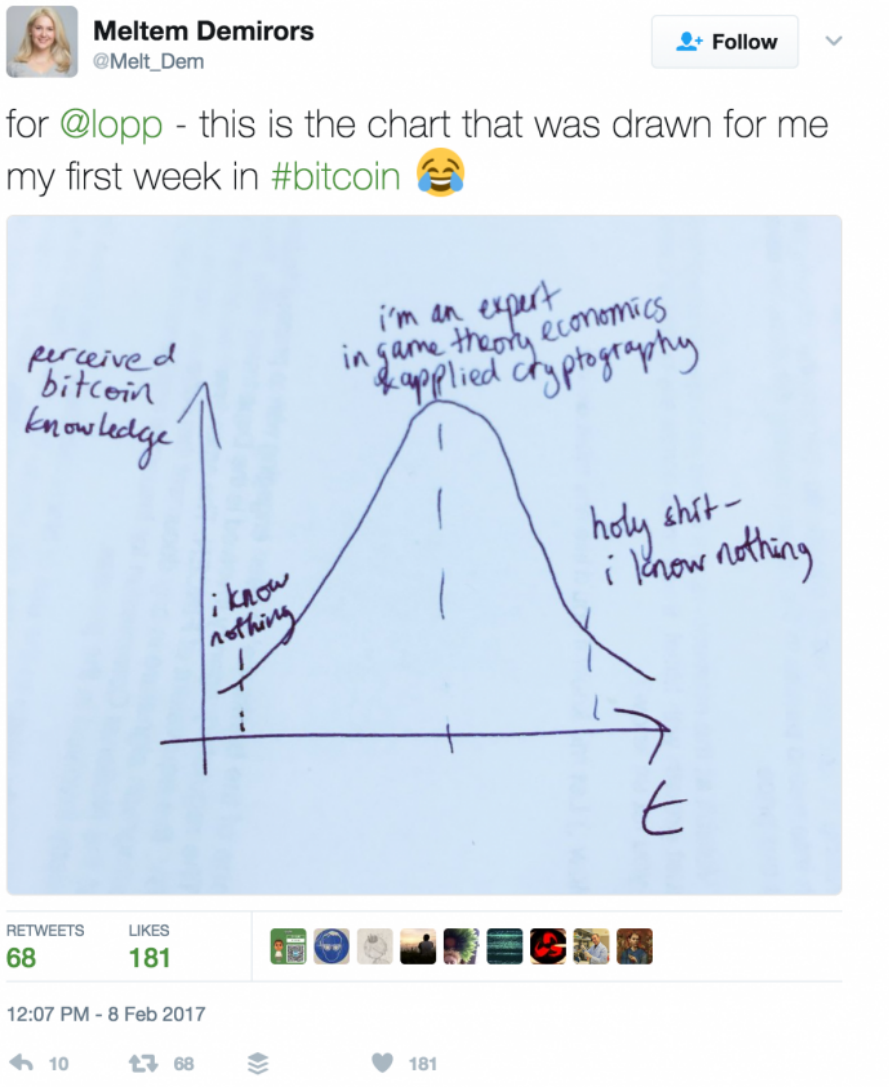
Bitcoin, Blockchain and Cryptoassets

Bitcoin Primer

Prof. Dr. Fabian Schär
University of Basel

Release Ver.: (Local Release)
Version Hash: (None)
Version Date: (None)

Let's Begin


Meltem Demirors
@Melt_Dem
Follow
for @lopp - this is the chart that was drawn for me my first week in #bitcoin 😂
perceived bitcoin knowledge
i'm an expert in game theory economics & applied cryptography
holy shit - i know nothing
i know nothing
t
RETWEETS
68
LIKES
181
12:07 PM - 8 Feb 2017
10
68
181

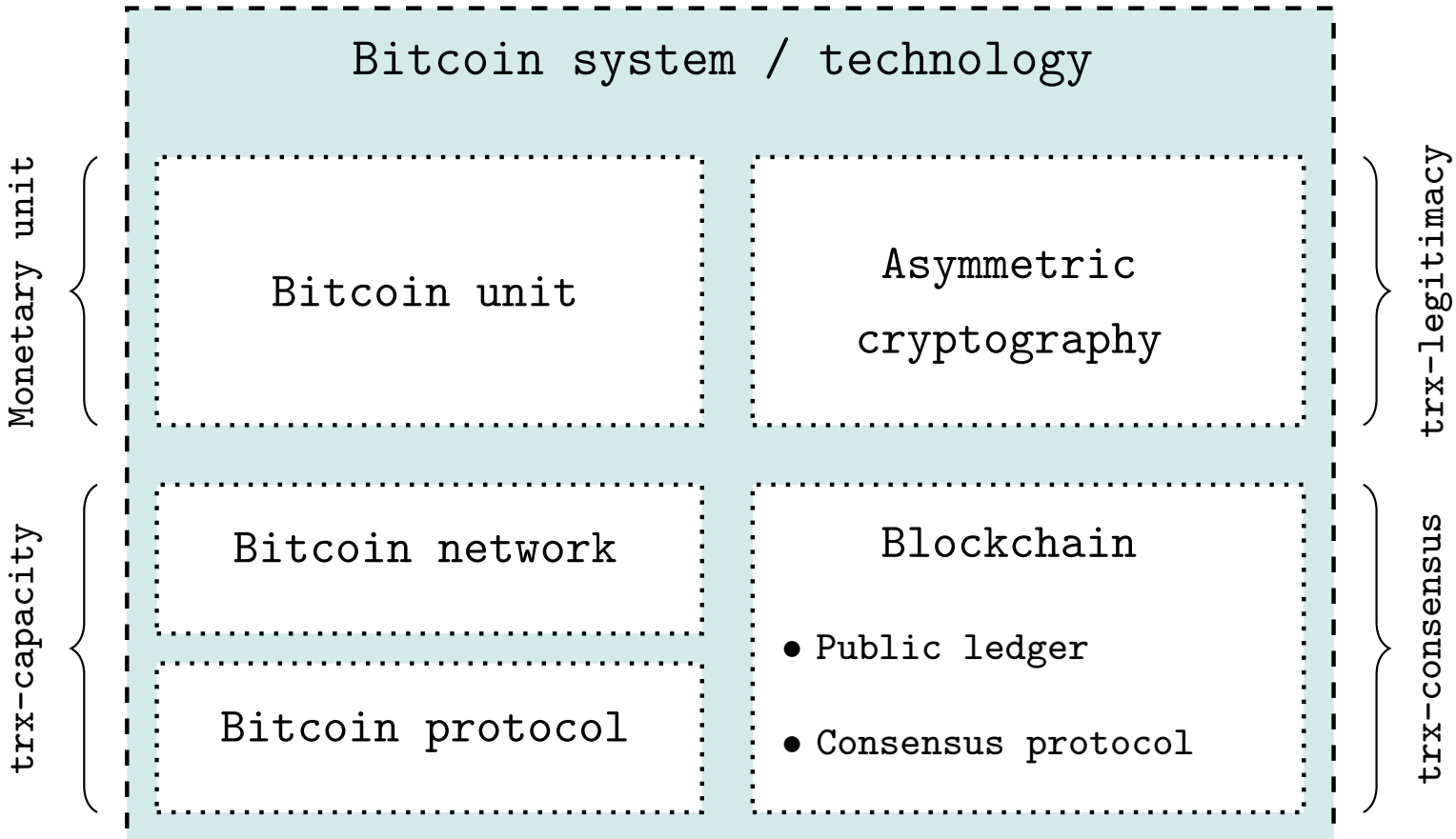
What We Already Know...

Bitcoin key characteristics:

1. Competitive creation
2. Virtual representation
3. Decentralized management
   - Transaction capacity
   - Transaction legitimacy
   - Transaction consensus

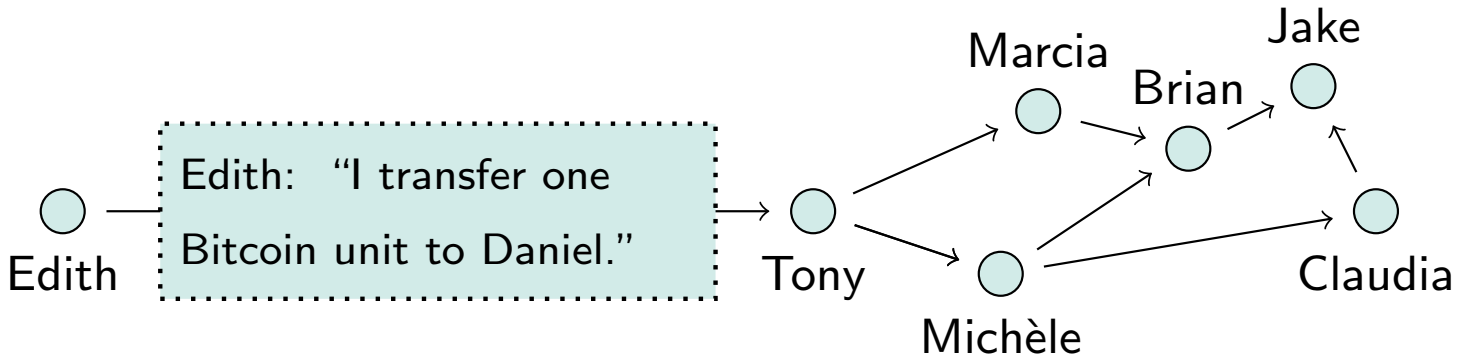
Key Idea:
Bitcoin is a decentralized data structure. The system is maintained by its participants and works in the absence of centralized third parties.

Bitcoin Building Blocks



Transaction Capacity

Goal: Ensure that each participant can reliably initiate a transaction without having to fear censorship.

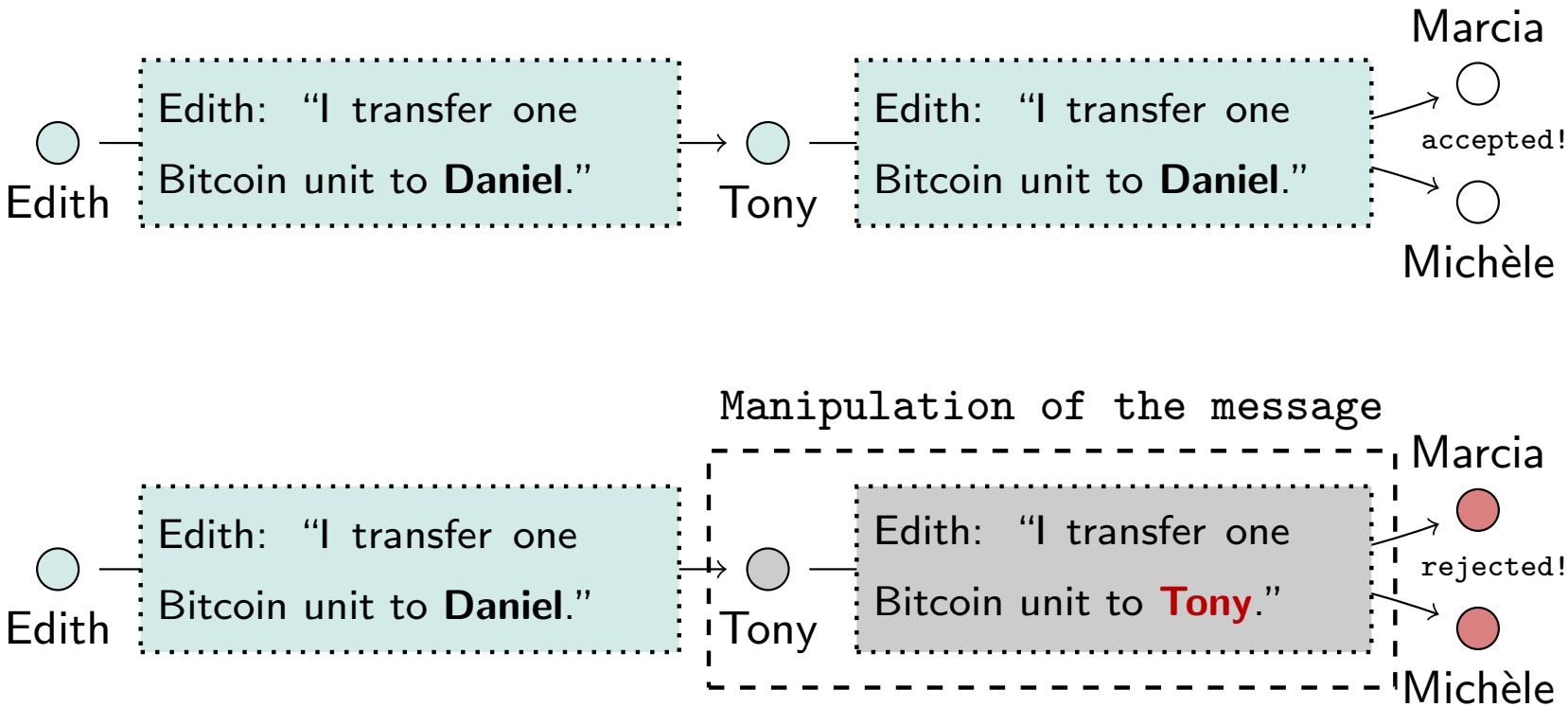


Peer-to-Peer Network:

- Permissionless
- Censorship-resistant
- No special privileges

Transaction Legitimacy

Goal: Ensure transaction authenticity and integrity, i.e., ensure that the transaction was initiated by its owner of the funds and has not been changed.



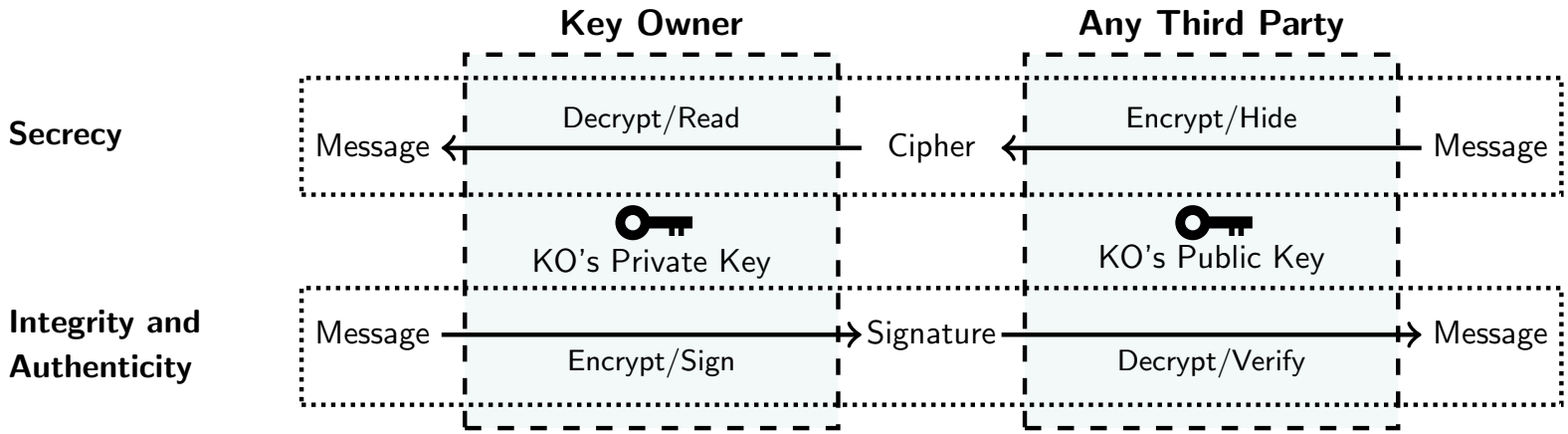
Public/Private Key Pair

Two key principles:

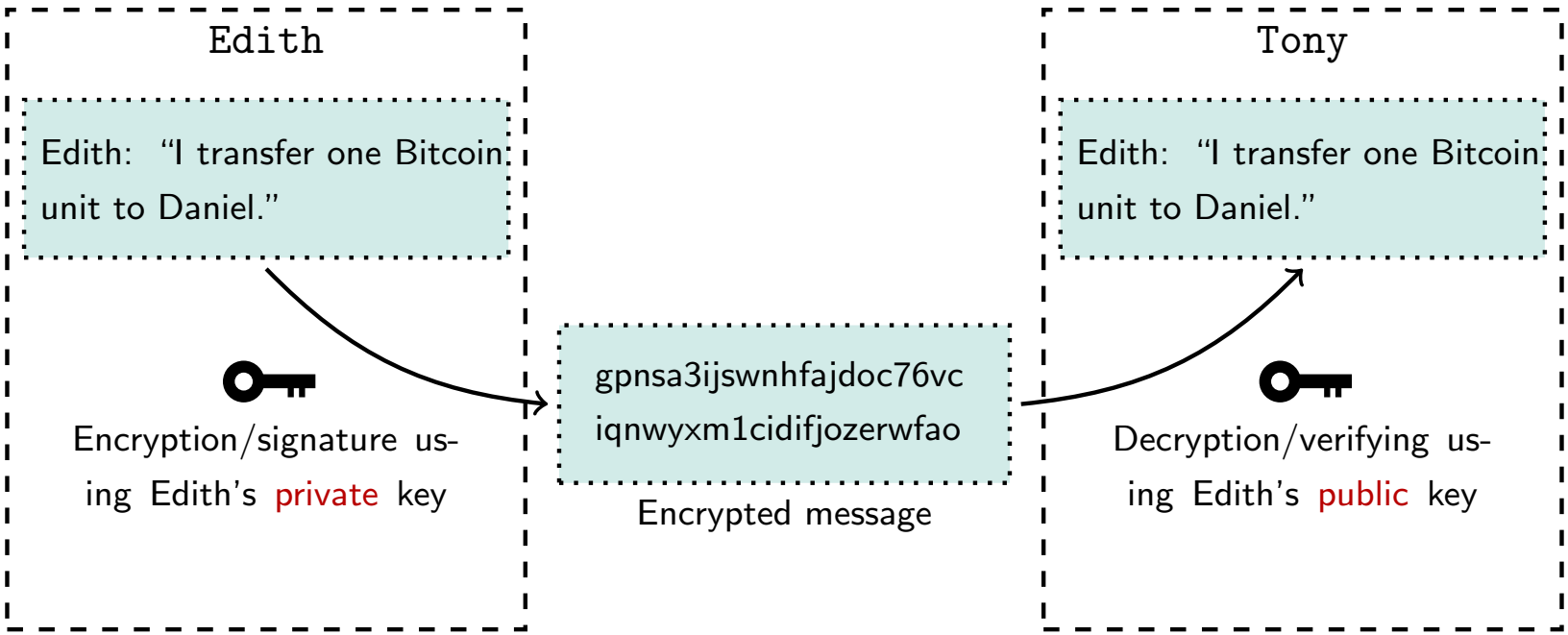
1. Private key is created (chosen) without the help of an intermediary, and can be used to derive public key.
2. If information is encrypted with one key, it can only be decrypted with the other key.

Key assumption:
Asymmetric cryptography and its applications assume that you are willing and able to keep your private key secret.

Two Distinct Applications



Transaction Legitimacy

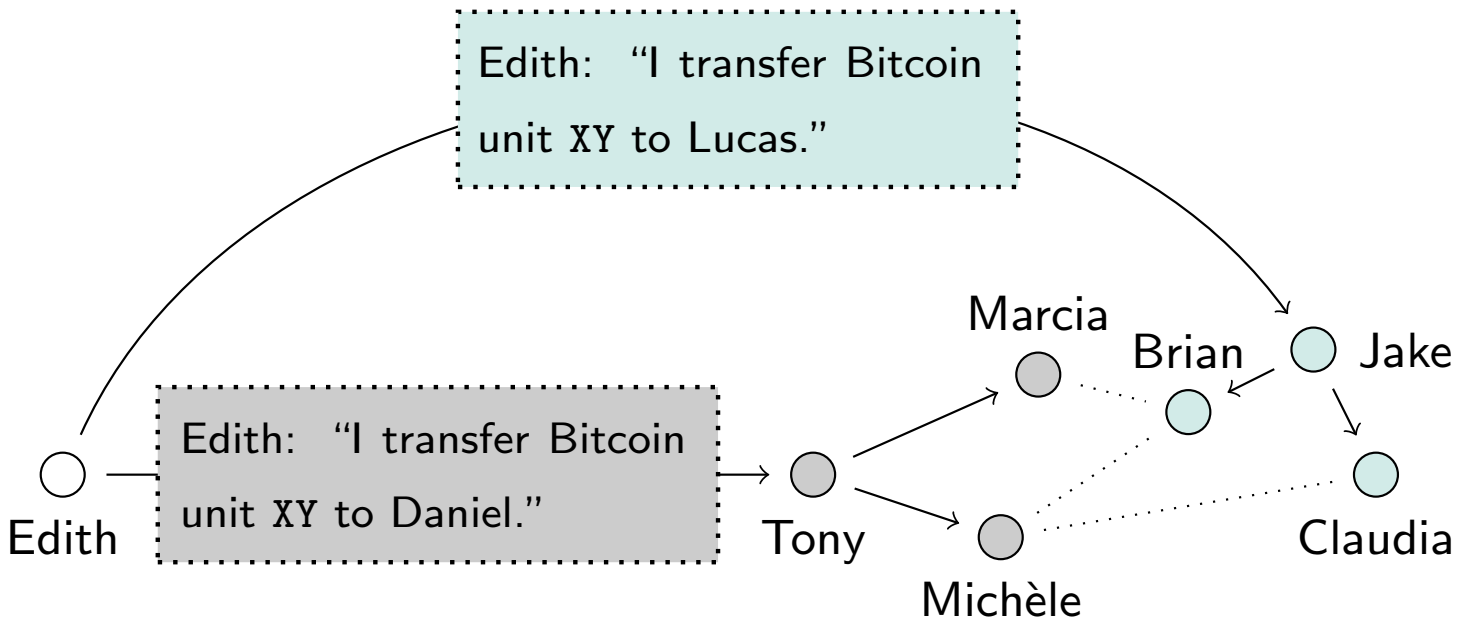


Encryption and decryption of the transaction message

Transaction Consensus

Goal: Deciding which (legitimate) transactions are valid.

Potential Problem: Assume both transactions have valid signatures, but spend the same Bitcoin units. What now?



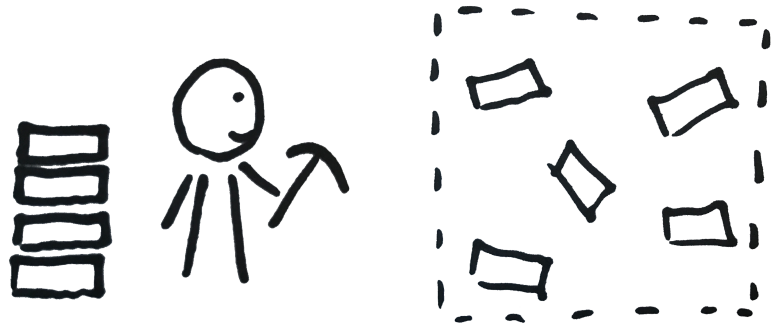
Blocks and the Blockchain

Transactions are bundled into blocks.

Blocks are sequentially linked $\rightarrow$ Blockchain

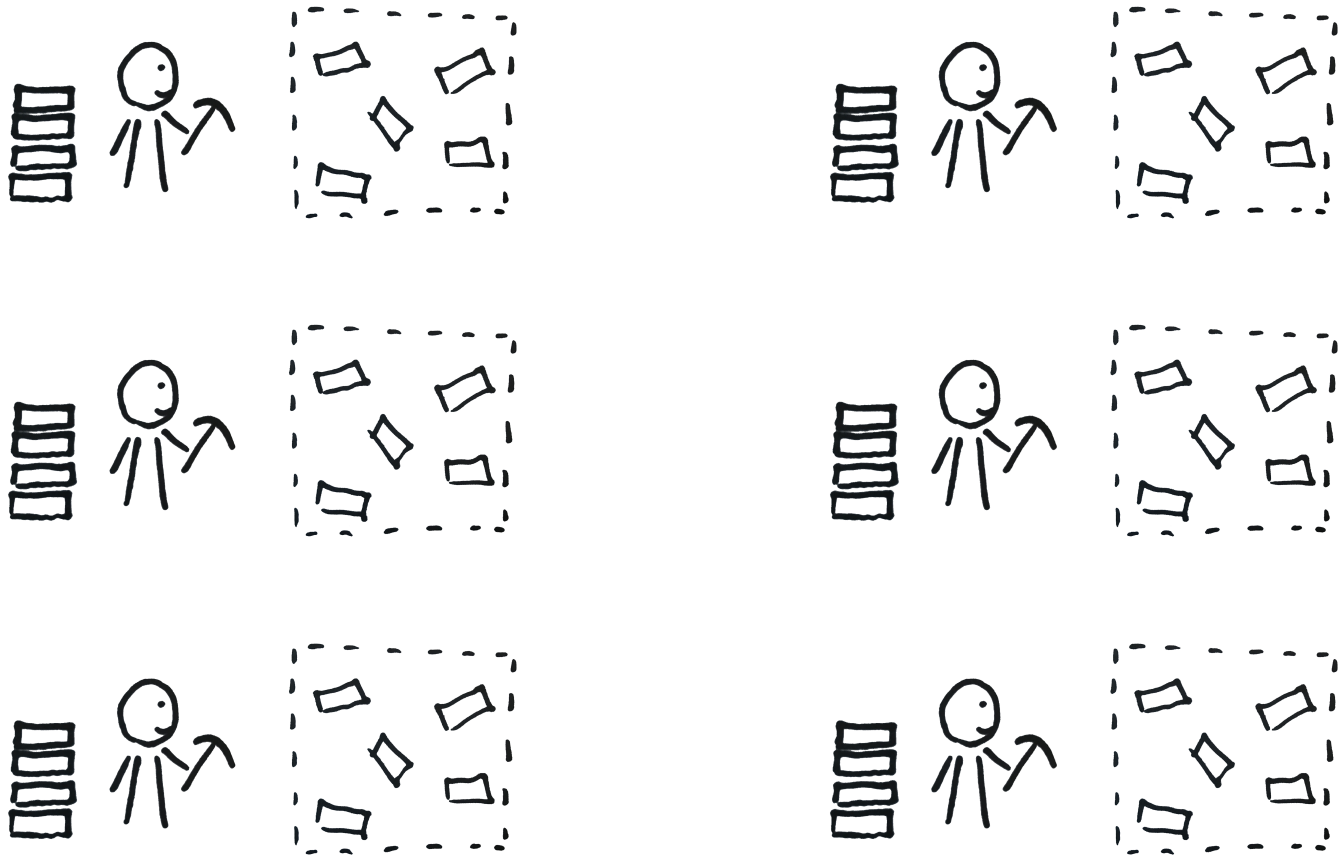
Bitcoin Mining

Network participants, who assemble candidate blocks are usually referred to as Bitcoin Miners.

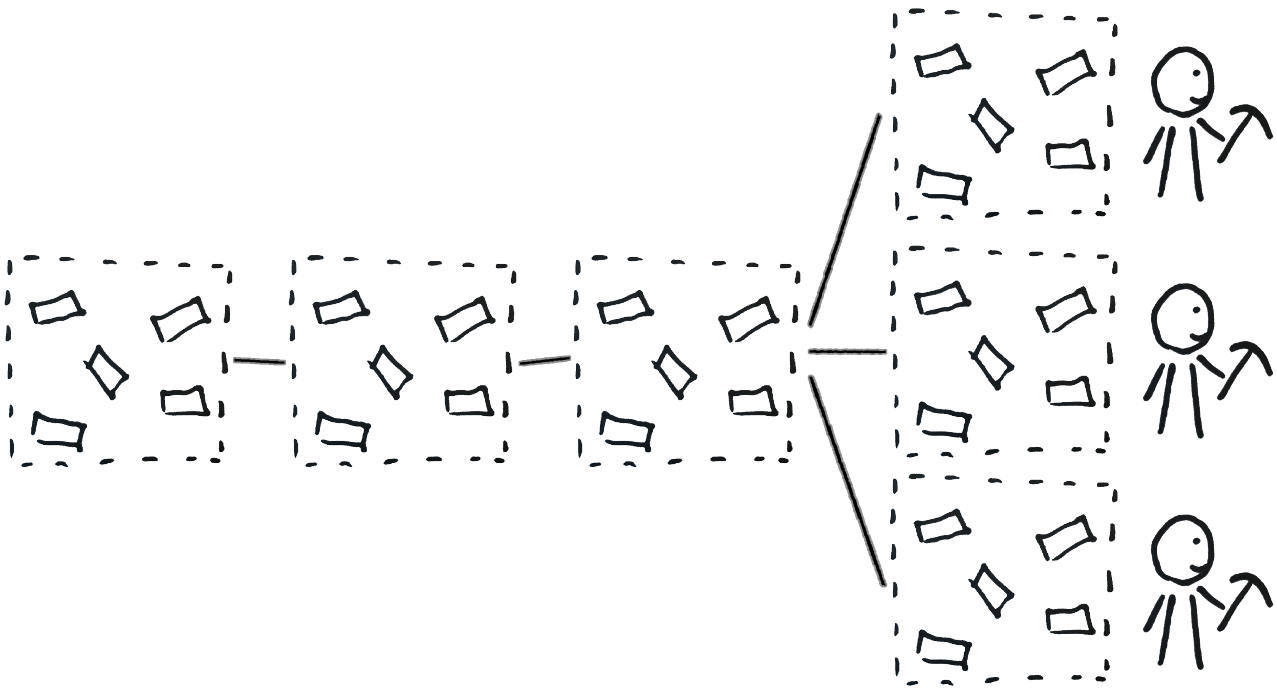


- Miner chooses the status quo on which to base its block. (Most recent version of Blockchain)
- Miner chooses a subset of the transactions from its queue (mempool) to create a block, as long as they...
  - ...are legimitate.
  - ...do not conflict with other transactions.
  - ...do not exceed block size limitation.

Bitcoin Miner



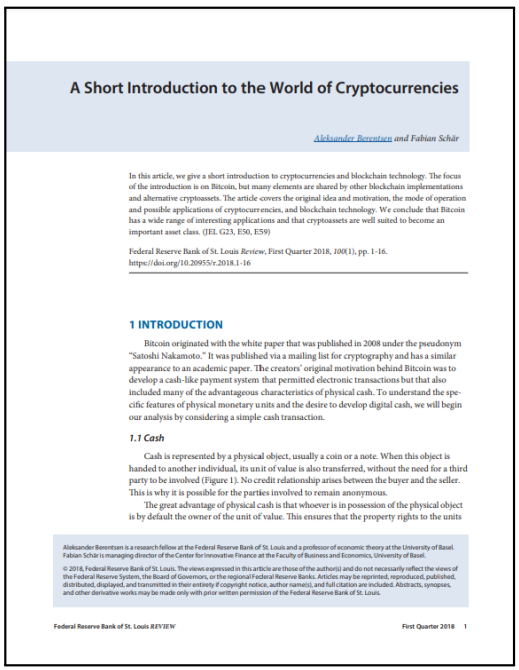
Transaction Consensus



How to reach consensus?:

- Centralized decision (Proof-of-Authority)
- Decentralized lottery (Proof-of-Work)

Recommended Reading



A Short Introduction to the World of Cryptocurrencies

Aleksander Berentsen and Fabian Schär

In this article, we give a short introduction to cryptocurrencies and blockchain technology. The focus of the introduction is on Bitcoin, but many elements are shared by other blockchain implementations and alternative cryptoassets. The article covers the original idea and motivation, the mode of operation and possible applications of cryptocurrencies, and blockchain technology. We conclude that Bitcoin has a wide range of interesting applications and that cryptoassets are well suited to become an important asset class. (JEL G23, E50, E59)

Federal Reserve Bank of St. Louis *Review*, First Quarter 2018, *100*(1), pp. 1-16.
https://doi.org/10.20955/r.2018.1-16

1 INTRODUCTION

Bitcoin originated with the white paper that was published in 2008 under the pseudonym "Satoshi Nakamoto." It was published via a mailing list for cryptography and has a similar appearance to an academic paper. The creators' original motivation behind Bitcoin was to develop a cash-like payment system that permitted electronic transactions but that also included many of the advantageous characteristics of physical cash. To understand the specific features of physical monetary units and the desire to develop digital cash, we will begin our analysis by considering a simple cash transaction.

1.1 Cash

Cash is represented by a physical object, usually a coin or a note. When this object is handed to another individual, its unit of value is also transferred, without the need for a third party to be involved (Figure 1). No credit relationship arises between the buyer and the seller. This is why it is possible for the parties involved to remain anonymous.

The great advantage of physical cash is that whoever is in possession of the physical object is by default the owner of the unit of value. This ensures that the property rights to the units

Aleksander Berentsen is a research fellow at the Federal Reserve Bank of St. Louis and a professor of economic theory at the University of Basel. Fabian Schär is managing director of the Center for Innovative Finance at the Faculty of Business and Economics, University of Basel.

A Short Introduction to the World of Cryptocurrencies

Aleksander Berentsen and Fabian Schär

External link Online PDF