The Blockchain Technology

Mooly Sagiv

Tel Aviv University

http://www.cs.tau.ac.il/~msagiv/courses/blockchain.html
msagiv@acm.org

Advisory Board

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

vmware

Shelly Grossman

Noam Rinetzky

Ittai Abraham

Guy Golan-Gueta

Yan Michalevsky

Orr Tamir

Eran Tromer

Ittay Eyal

Benny Pinkas

אוניברסיטת בר-אילן

Outline

- Formalities
  - Prerequisites
  - Course Goals
  - Course Requirements
  - Tentative Schedule
- *A gentle introduction*
  - *A better one next week by Ittay Eyal (Tehnion)*
- *Guides to presentation (short)*

Prerequisites

- Computational Models
- One of the following
  - Logics in Computer Science
  - Cryptography

Tentative Schedule

- March 4: Overview and Introduction
- March 11: Ittay Eyal, Technion: Basics of mining and incentives
- April 4: Ittai Abraham, Vmware and Hebrew University: The Bitcoin Blockchain and Nakamoto Consensus
- April 22: Yonathan Sompolisky, Hebrew University: TBD
- Presentations by Students

Seminar Goals

- Learn how to read a scientific article in computer science
  - Not necessarily practical for Blockchain
  - Not self contained
  - Critical thinking
  - >100 hours
- Learn how to prepare a high quality presentation
  - Help from Instructor
  - A lot of good advise in the Internet
  - > 150 hours
- Read introductory material
- Meet the instructor twice (at least)
- Participate in 11 lectures

Traditional Online Transactions

Trusted third party

Yup! He sent the money

$10,000

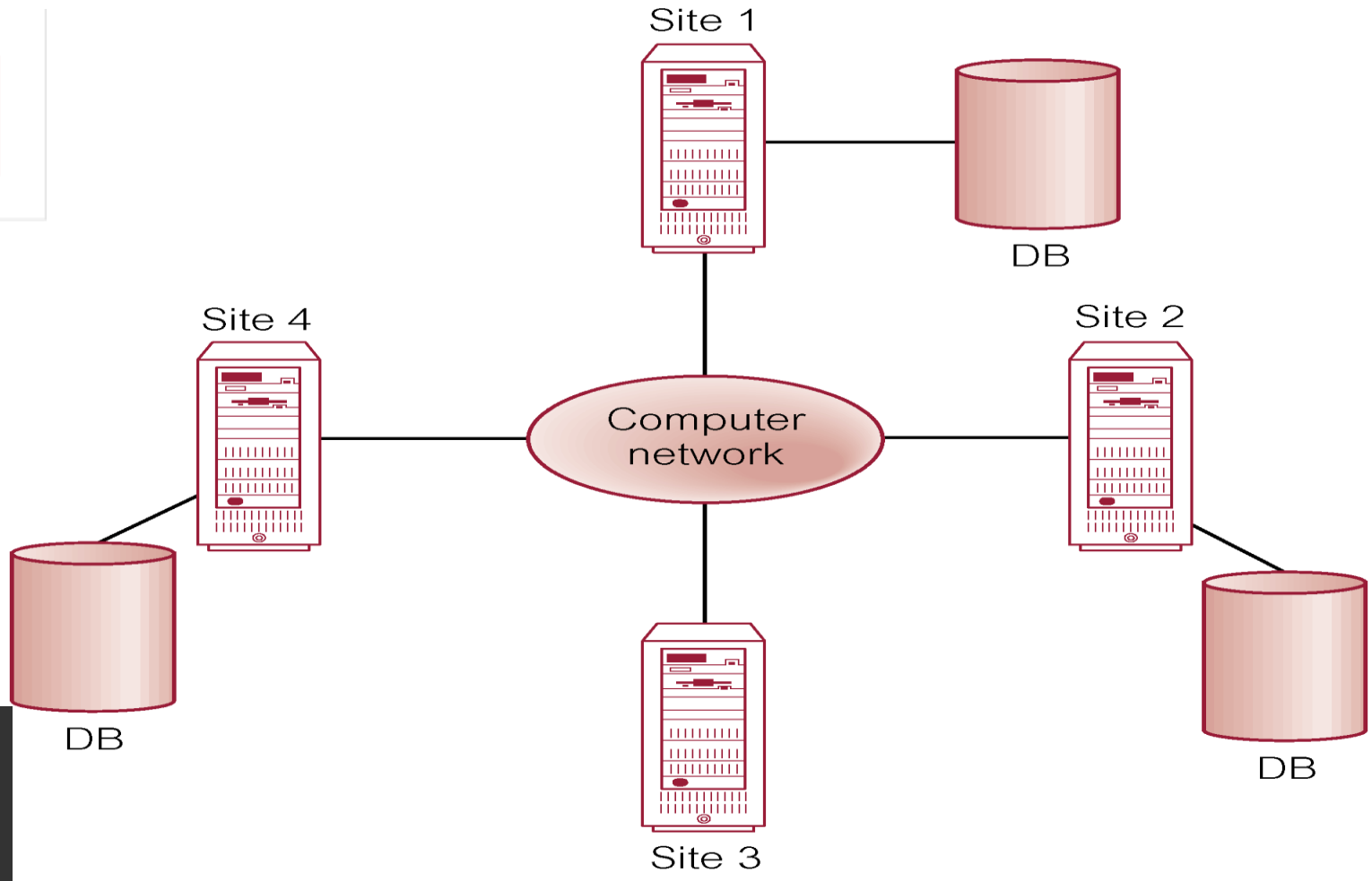
1. Validate entries
2. Safeguard entries
3. Preserve historic records

- Expensive
- Slow
- Subjects to frauds

Questions

- Can we permanently store assets globally with trust?
- Single ownerships
- Identity management
- Easy transfer of assets
- Create the illusion of a single global computer

Distributed DBMS



Limitations of Distributed Databases

- Centralized
- Complexity & Costs
- Trust the database company

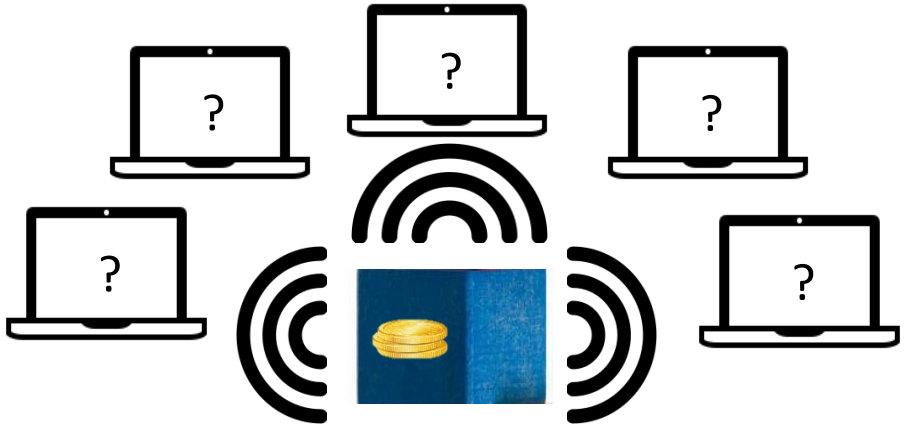
How Blockchain works?

A wants to send money to B

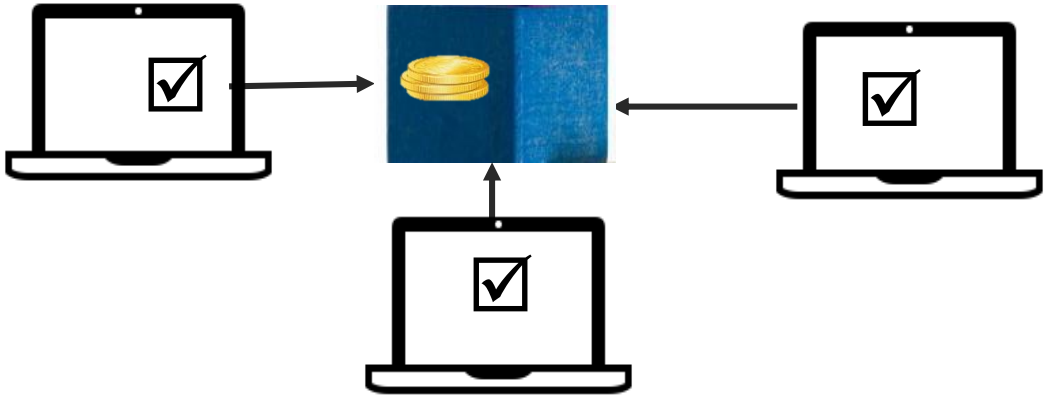
A

The transaction is represented as block

The block is broadcast to every node in the network

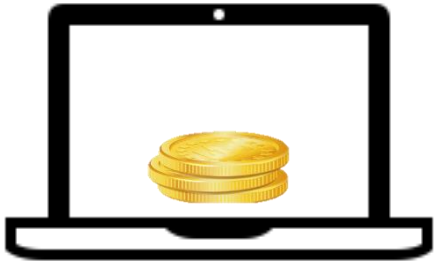


Sufficient miners approve the transaction



The transaction is added to Blockchain

B receives the money



B

Public vs. Private Blockchains

Public blockchains

- Anyone can participate

Private blockchains

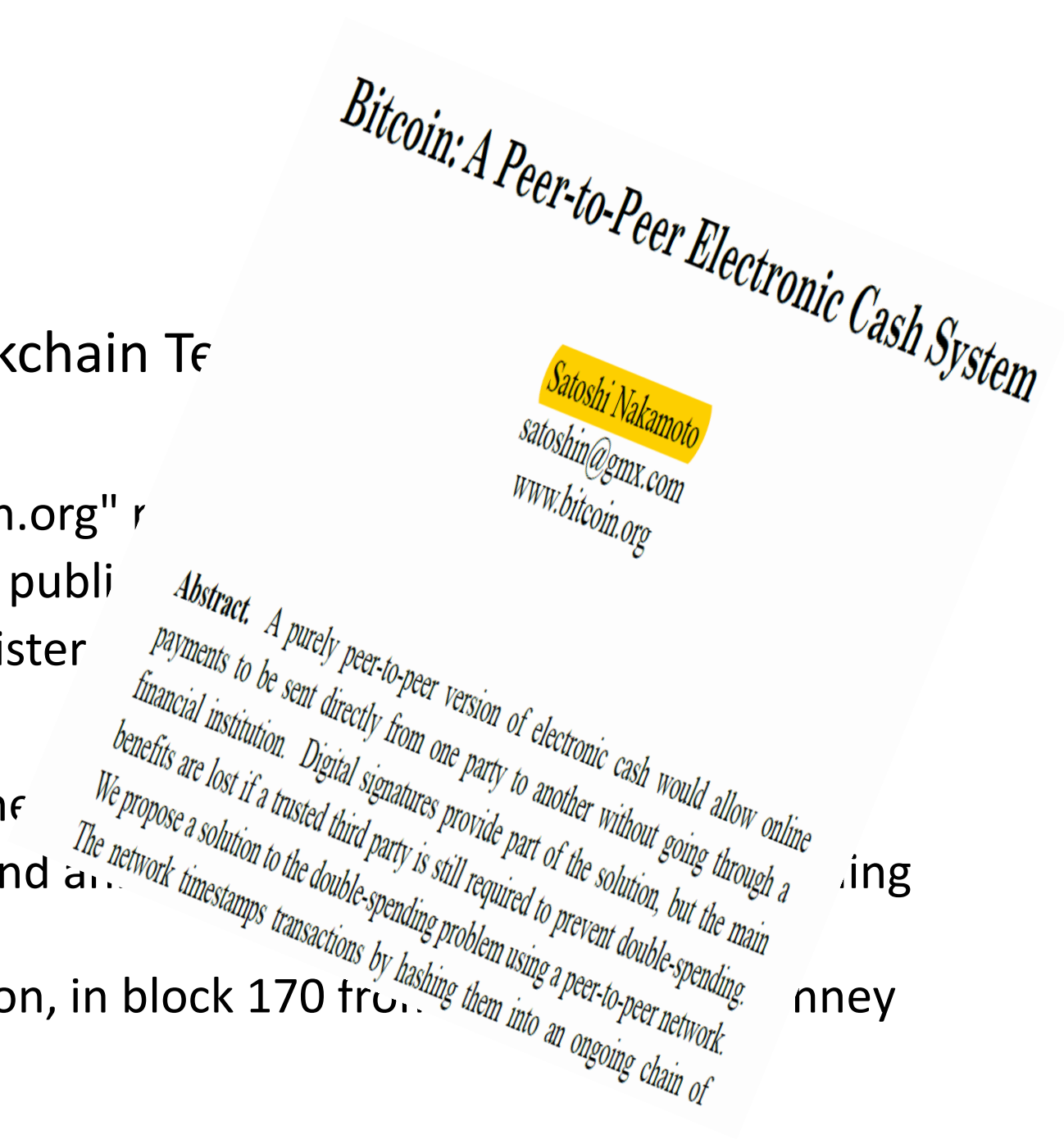
- Participants are known and trusted
  - An industry group, or a group of companies owned by an umbrella company
  - Many of the mechanisms aren't needed – or rather they are replaced with legal contracts

ethereum

The Bitcoin Blockchain

Bitcoin

- The first realization of the Blockchain Te
- 2008
  - **August 18** Domain name "bitcoin.org" r
  - **October 31** Bitcoin design paper publi
  - **November 09** Bitcoin project register
- 2009
  - **January 3** Genesis block establishe
  - **January 9** Bitcoin v0.1 released and a ing list
  - **January 12** First Bitcoin transaction, in block 170 fro nney



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

The essence of bitcoin

- A **protocol** that supports decentralized anonymous peer-to-peer digital currency
- A **publicly** disclosed **ledger** of transactions
- A **reward** driven system for achieving **consensus** (mining) based on
  - "Longest chain for consensus”
  - “Proofs of Work” for helping to secure the network
- A “scare token” economy with an eventual cap of about 21M bitcoins

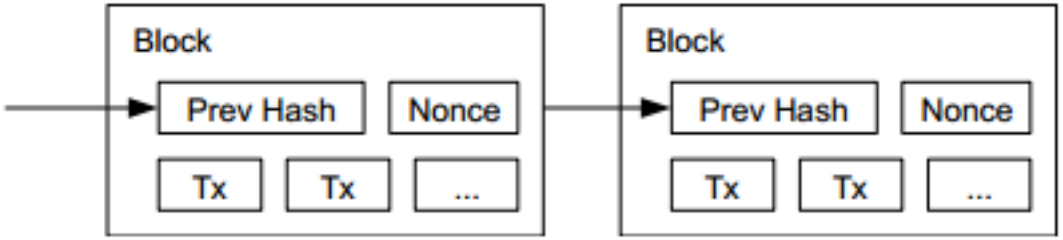
The Bitcoin Blockchain

The header of the block contains unique hash

Refer to prev blocks

Bitcoin Blockchain

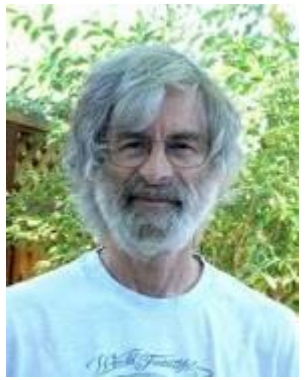
- Every *viable* transaction is stored in a public ledger
- Transactions are placed in blocks, which are linked by SHA256 hashes
- https://blockchain.info



Proof of Work [Naor&Dwork 92]

- Make it harder for dishonest miners to create blocks
- Make sure that miners solve computationally hard problems when a block is created
  - But validation is easy
  - A guessing game where block-makers need to guess a number, which when crunched with the rest of the block data contents, results in a hash / fingerprint that is smaller than a certain number

The Consensus Problem[Lamport]



- How to reach an agreement in a distributed system?
- Every node votes on a value
- The nodes exchanges messages until they reach consensus
- Correctness properties
  - Non-triviality: Only proposed values can be learned
  - Safety: At most one value can be learned
    - two different learners cannot learn different values
  - Liveness: If value C has been proposed, then eventually learner L will learn some value
    - if sufficient processors remain non-faulty

The FLP Theorem 1985

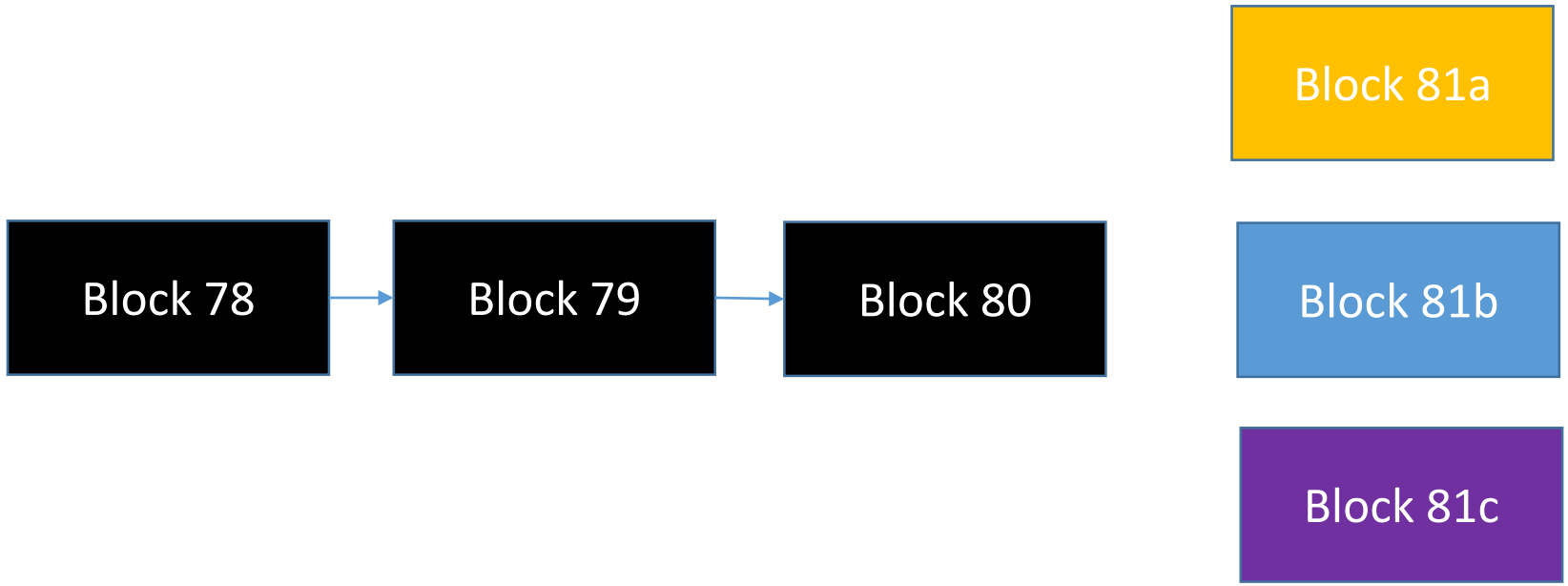
- In the asynchronous setting no live consensus exists



Consensus in Bitcoin

- Not aiming for fully correct consensus
- No need for message exchange
- Several mechanisms used to ensure well behaved programs under certain assumptions
  - Longest chain

Longest Chain

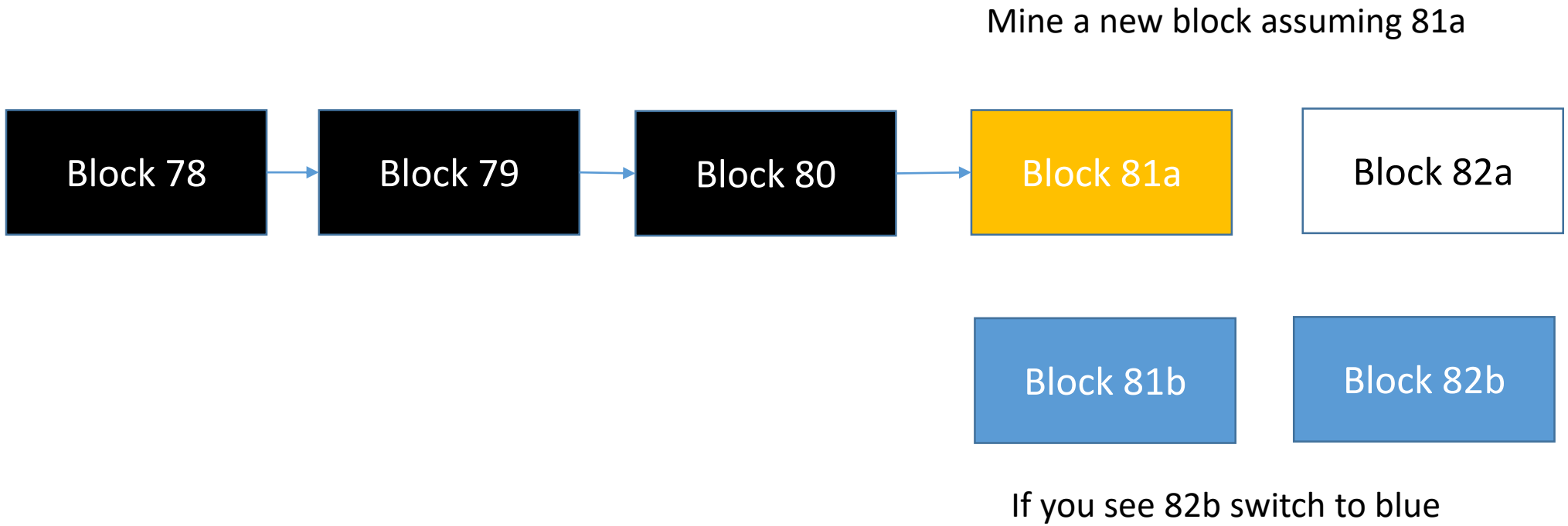


Which one should be used?

They contain different transactions

They contain different rewards

Longest Chain



The effects of the longest chain rule

- Consensus with high probability
  - Because creating blocks is hard
- The number of miners does not effect the results
- Transactions can be revoked

Bitcoin Main Features

Question	Bitcoin	Other ways
How should data be stored?	Blockchain	Distributed database
How should new data be distributed?	Peer-to-Peer	Client-Server hierarchical
Resolving conflicts (Consensus)	Longest chain rule	Other consensus protocols
Adding/Changing rules	BIP for writing rules Vote for hashing power	Centralized updates Contextual obligations
Who can submit transactions?	Open anonymous	Trusted pre-vetted
Who can validate transactions	Open anonymous	Trusted pre-vetted
Who can add blocks?	Open anonymous	Trusted pre-vetted
Preventing bad behaviors	Proof of work	Poof of Stake or trusted
Incentivize block makers	Coins	3rd party

The Ethereum Blockchain

Smart Contracts

- Transactions in bitcoin are limited
  - Transfer ‘X’ bitcoins from ‘Y’ to ‘Z’
- More powerful transactions
  - Exchange
  - Auction
  - Games
  - Bets
  - Legal agreements
- Solution
  - Store smart contracts on the blockchain
  - Computer programs implement transactions
  - Immutability guarantees persistence

Ethereum

- A decentralized platform that runs smart contracts
- Proposed in late 2013 by Vitalik Buterin
- Released 2015
- Supports Turning complete smart contracts (Solidity)
- A virtual machine for cryptocurrency (Ethereum Virtual Machine)
  - Creating new currencies
  - Guaranteeing certain currency consistency
- But has all bad features of computer programs (DAO, Parity, …)

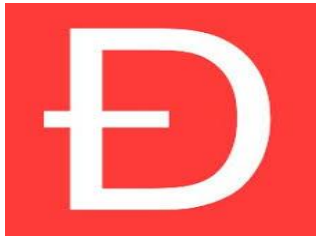
How to steal $50M – the DAO bug

```
DAO::withdraw(to) {
 if shares[to] > 0 {
  transferTo(to, shares[to]);
  shares[to] = 0;
 }
}
```

coins[Thief]=7

shares[Thief]=100

How to steal $50M – the DAO bug

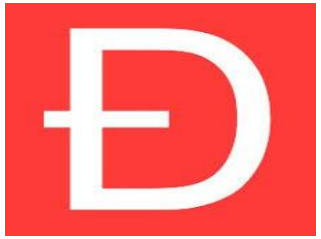


```
DAO::withdraw(to) {
  if shares[to] > 0 {
    transferTo(to, shares[to]);
    shares[to] = 0;
  }
}
```

coins[Thief]=7

shares[Thief]=100

How to steal $50M – the DAO bug



```
DAO::withdraw(to) {
 if shares[to] > 0 {
  transferTo(to, shares[to]);
  shares[to] = 0;
 }
}
```

```
Thief::uponTransfer(a) {
 DAO::withdraw(Thief)
}
```

coins[Thief]=107

shares[Thief]=100

How to steal $50M – the DAO bug

```
DAO::withdraw(to) {
  if shares[to] > 0 {
   transferTo(to, shares[to]);
   shares[to] = 0;
  }
}

Thief::uponTransfer(a) {
 DAO::withdraw(Thief)
}
```

coins[Thief]=107

shares[Thief]=100

How to steal $50M – the DAO bug

```
DAO::withdraw(to) {
  if shares[to] > 0 {
   transferTo(to, shares[to]);
    shares[to] = 0;
  }
}


Thief::uponTransfer(a) {
 DAO::withdraw(Thief)
}
```

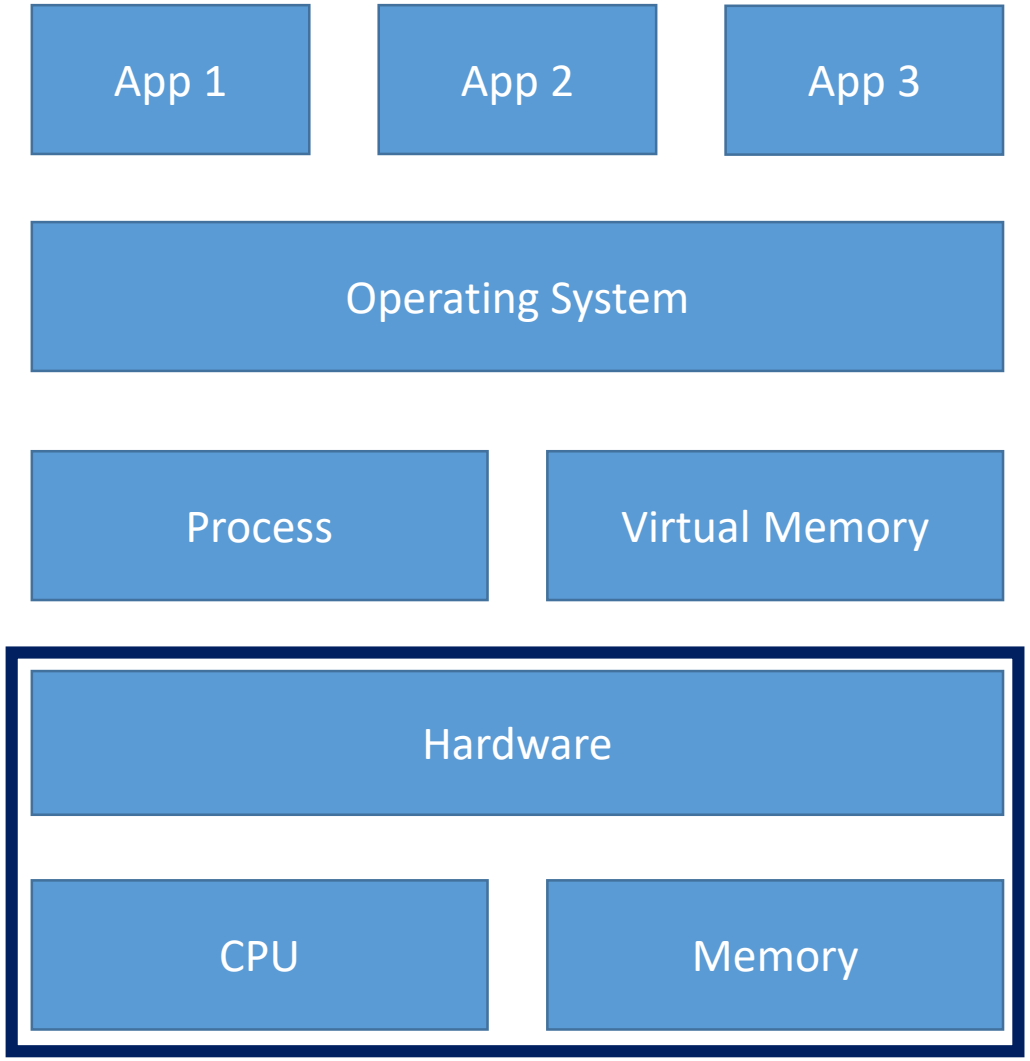
coins[Thief]=207

shares[Thief]=100

Final Comments

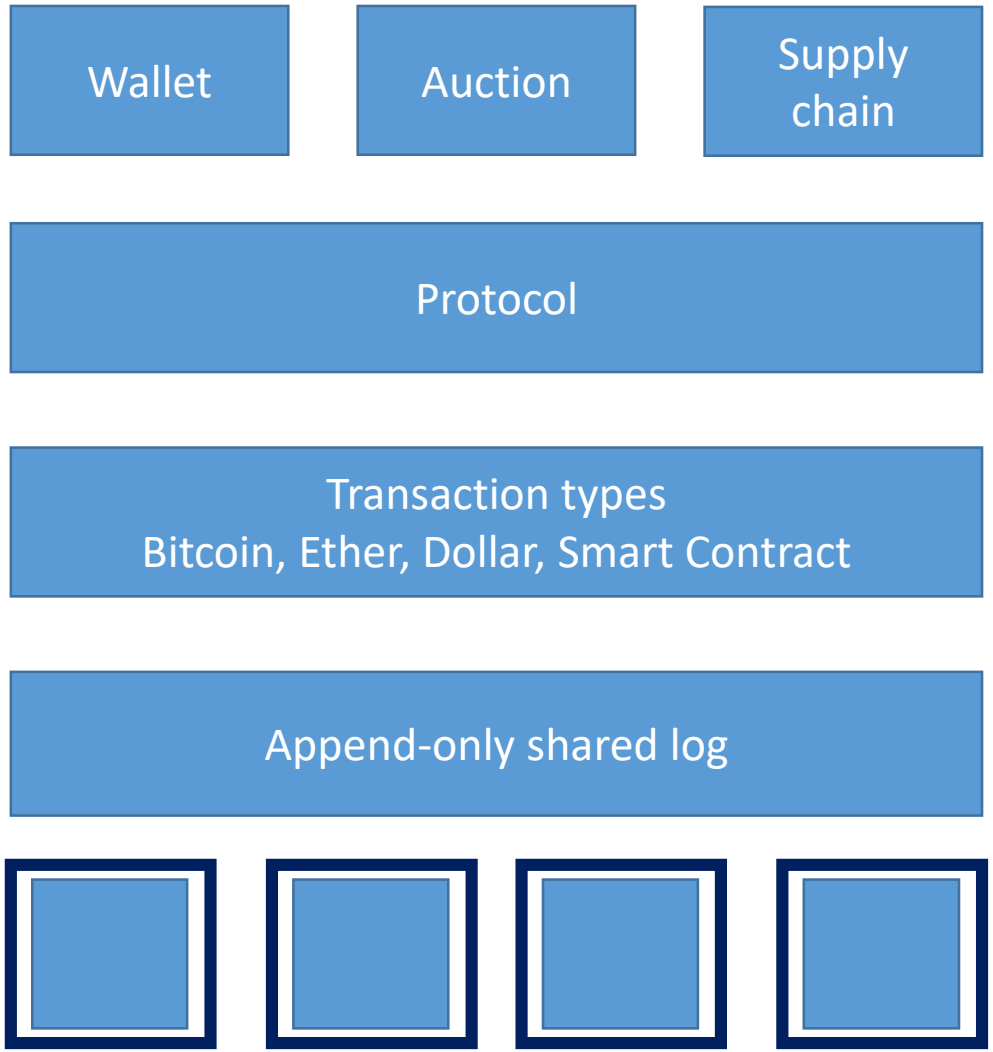
Something Completely Different OS

Guaranteed semantic isolation



Blockchain

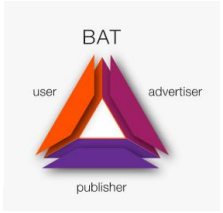
Guaranteed global view for isolated users



Some Early Applications of Blockchain

- Banking services for those who are not eligible for bank accounts in their country

- Music sales
- Smarter web advertisements protecting user anonymity



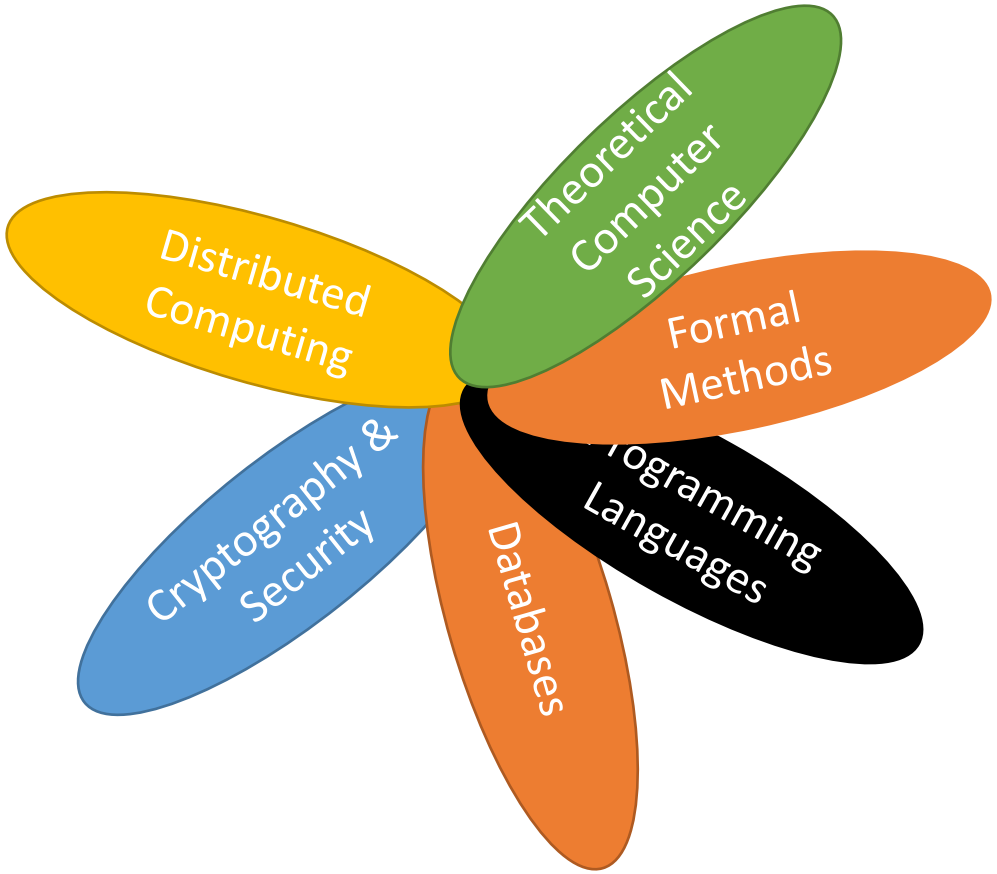
- UN’s World Food Programm uses blockchain to eliminate costs related to fair distribution of food and supplies to Syrian refugees
- Applications of private blockchains to replace databases

Challenges

- How does the sender prevent others to receive the money?
- Who guarantees that the sender has the money and prevents double spending due to network delays?
- How can new money created?
- What are the exchange rules?

- Cryptography checks
- The miners
- Rewards for mining
- Determined by smart contracts

Blockchain is interdisciplinary



Foundational Work

- 1977 RSA: Mention currency an early proposed application
- 1978 Lamport: Consensus
- 1982 Chaum: Anonymous cryptocurrency introduced
- 1993 Dwork and Naor: Proofs of work introduced (w/o the name)
- 1996 Rivest and Shamir: proof-of-work-based cryptocurrency
- 2002: Vivek Vishnumurthy, Sangeeth Chandrakumar and Emin Gun Sirer: P2P Currency

What do you have to do if you are registered?

- Attend the 2nd lecture on presentations (short)
- Select three articles from the web by March 11 and email titles to instructor
- Read chapters 1 & 2 of “Bitcoin and Cryptocurrency Technologies” by March 18t
- Receive topic and date
- Meet the instructor twice before the lecture

Acknowledgments

- The noun project
- David V Duccini
- Antony Lewis
- http://scet.berkeley.edu/blockchain-lab/
- The IC3 project Cornell

For more information

- http://www.cs.tau.ac.il/~msagiv/courses/blockchain.html
- https://crypto.stanford.edu/cs251/