Foundations of Blockchain Systems

Lecture 2: Bitcoin

Course: EE 595, Autumn 2020.

Instructor: Sreeram Kannan

University of Washington Seattle

ELECTRICAL & COMPUTER ENGINEERING

What is a blockchain

Mechanism to coordinate between multiple parties without a trusted intermediary.

Core properties

- Immutable: Append-only ledger
- Fault tolerant: Functional despite some fraction of nodes being faulty / malicious

Application-level properties

- Censorship resistant
- Transparency: Each object's history is traceable on the ledger
- Truly permissionless operation
- Privacy

When not to use a blockchain

1. There is a high trust intermediary
   - Run a server

2. There are physical aspects to coordination
   - Cannot be assured by the blockchain

3. Certifying physical provenance
   - Cannot ensure *correct* data entered into blockchain

4. Efficiency is the primary determinant
   - No decentralized system can be more efficient than a centralized system

Applications of Blockchain: Cryptocurrencies


Opinion
The New York Times

Bitcoin Has Saved My Family

"Borderless money" is more than a buzzword when you live in a collapsing economy and a collapsing dictatorship.

By Carlos Hernández
Mr. Hernández is a Venezuelan economist.

Feb. 23, 2019

Permissionless

Total Market Cap: 500 Billion USD

Central Bank
Digital Currency

Real Time
Gross Settlement

Permissioned

Today's Applications beyond Currencies

StableCoins

Lending

Exchange

Decentralized Finance

Cryptokitties

NBA Collectible

Gaming Assets

Digital Collectibles

Projected Applications

1 Static registry

- Distributed database for storing reference data

Example

- Land title
- Food safety and origin
- Patent

2 Identity

- Distributed database with identity-related information
- Particular case of static registry treated as a separate group of use cases due to extensive set of identity-specific use cases

Example

- Identity fraud
- Civil-registry and identity records
- Voting

3 Smart contracts

- Set of conditions recorded on a blockchain triggering automated, self-executing actions when these predefined conditions are met

Example

- Insurance-claim payout
- Cash-equity trading
- New-music release

4 Dynamic registry

- Dynamic distributed database that updates as assets are exchanged on the digital platform

Example

- Fractional investing
- Drug supply chain

5 Payments infrastructure

- Dynamic distributed database that updates as cash or cryptocurrency payments are made among participants

Example

- Cross-border peer-to-peer payment
- Insurance claim

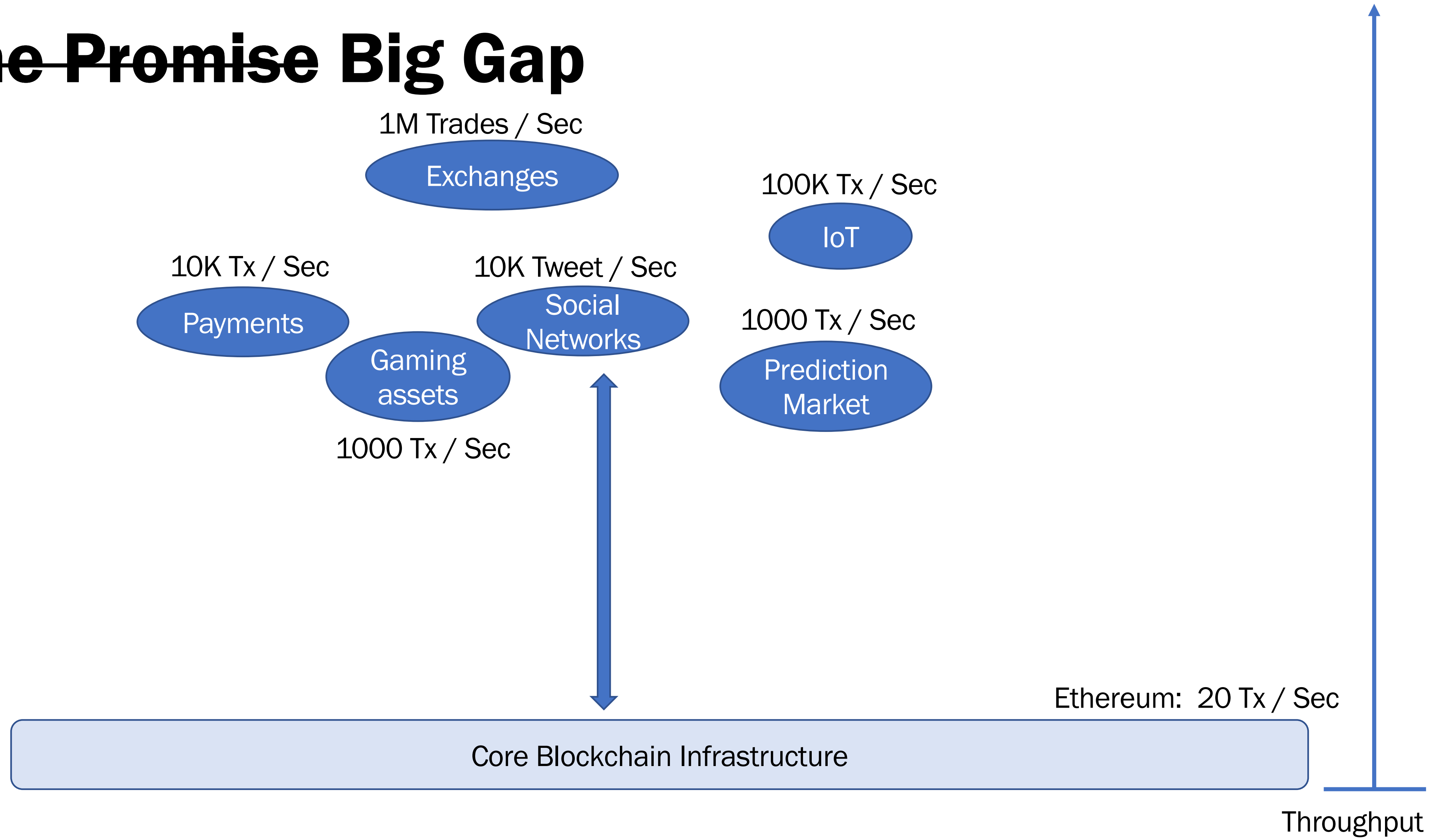
6 Other

- Use case composed of several of the previous groups
- Standalone use case not fitting any of the previous categories

Example

- Initial coin offering
- Blockchain as a service

~~The Promise~~ Big Gap



Bitcoin: Case Study

Bitcoin: A Peer-to-Peer Electronic Cash System

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

BITCOIN IS A CRYPTOCURRENCY

LAUNCHED IN JANUARY 2009

VERY SECURE: SAFETY AND LIVENESS

Cryptography background: Hash & Digital Signatures

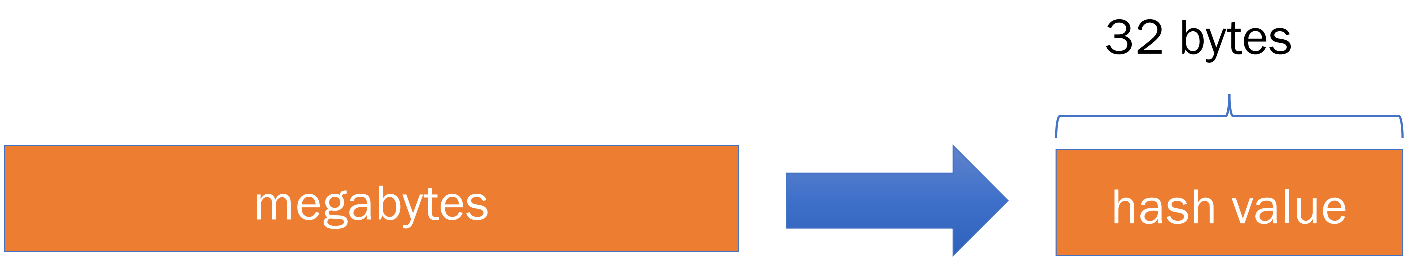
Adapted from Stanford CS 251 slides [Dan Boneh]

Hash Function

(1) cryptographic hash functions

An efficiently computable function $H\colon M \rightarrow T$
where $|M| \gg |T|$

Given H(x) “hard” to find x



$T = \{0,1\}256$

Collision resistance

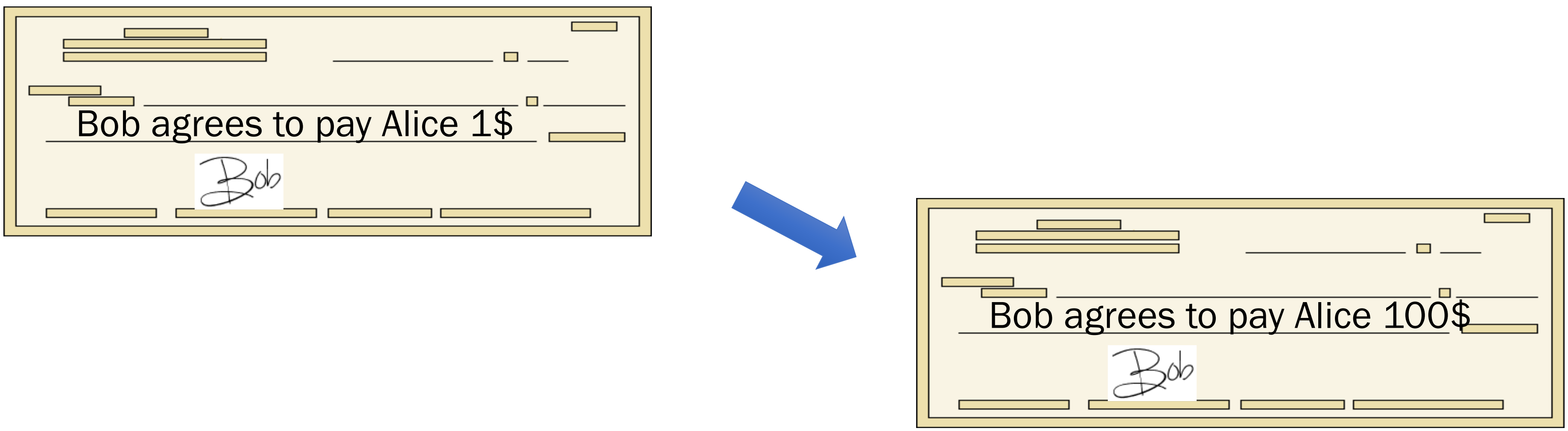
<u>Def</u>: a **<u>collision</u>** for $H: M \to T$ is pair $x \neq y \in M$ s.t. $H(x) = H(y)$

$|M| \gg |T|$ implies that <u>many</u> collisions exist

<u>Def</u>: a function $H: M \to T$ is **<u>collision resistant</u>** if it is "hard" to find even a single collision for H

Signatures

Physical signatures: bind transaction to author

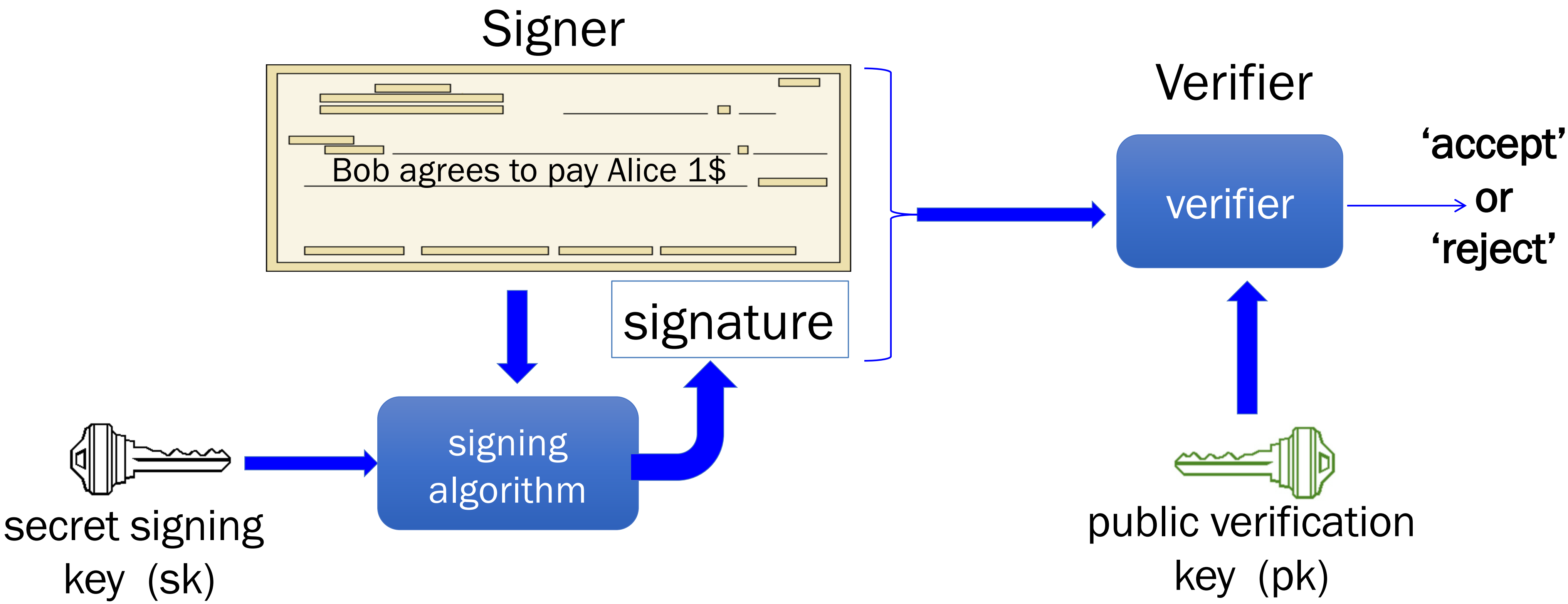


Problem in the digital world:

anyone can copy Bob’s signature from one doc to another

Digital signatures

Solution: make signature depend on document



Digital signatures: syntax

Def: a signature scheme is a triple of algorithms:

- **Gen**(): outputs a key pair (pk, sk)
- **Sign**(sk, msg) outputs sig. σ
- **Verify**(pk, msg, σ) outputs 'accept' or 'reject'

Secure signatures: (informal)

Adversary who sees signatures on many messages of his choice, cannot forge a signature on a new message.

Families of signature schemes

1. RSA signatures (old … not used in blockchains):
   - long sigs and public keys (≥256 bytes),   fast to verify

2. Discrete-log signatures: Schnorr and ECDSA
   - short sigs (48 or 64 bytes) and public key (32 bytes)

     (Bitcoin, Ethereum)

3. BLS signatures: 48 bytes,   aggregatable,   easy threshold

   (Ethereum 2.0, Chia, Dfinity)

4. Post-quantum signatures: long (≥768 bytes)

Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System

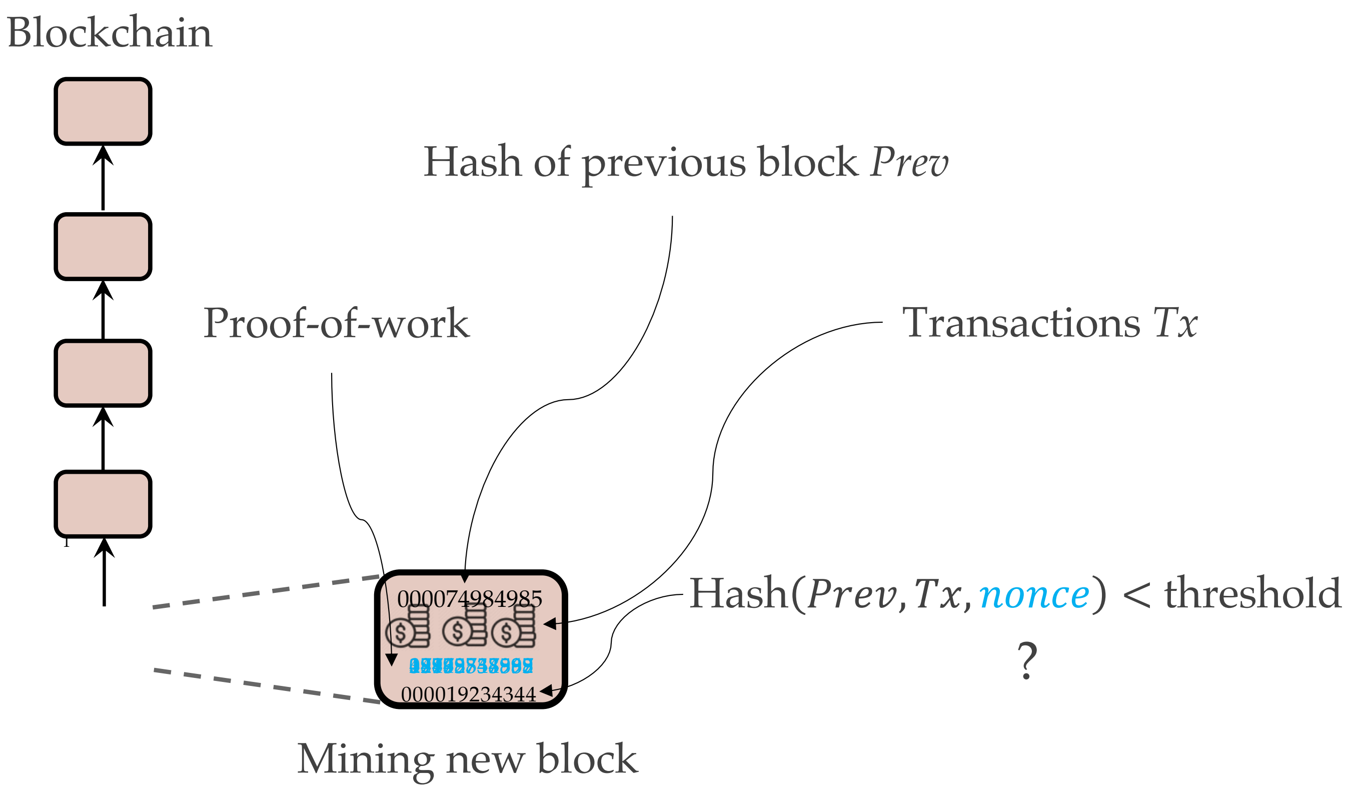
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

BITCOIN IS A CRYPTOCURRENCY

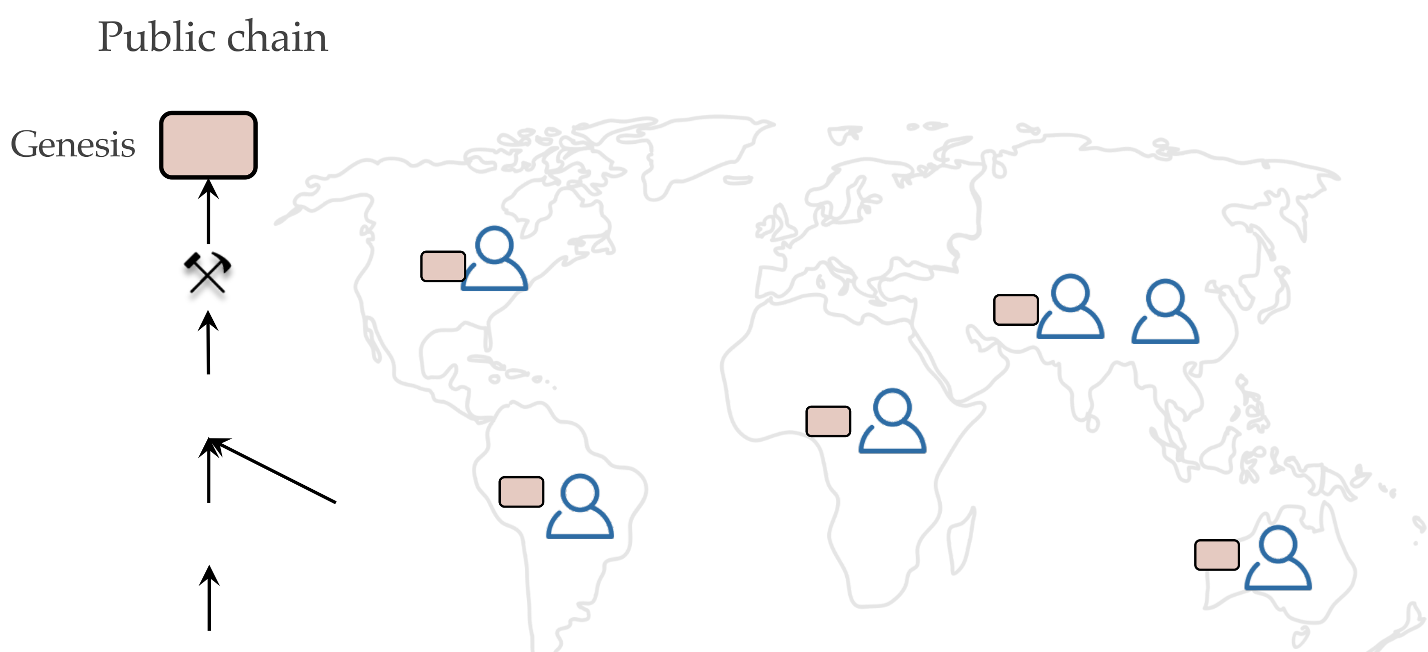
LAUNCHED IN JANUARY 2009

VERY SECURE: SAFETY AND LIVENESS

Bitcoin Primer - Mining



Bitcoin Primer – Distributed Mining



- Poisson process
- longest chain protocol