Writing Smart Contracts
01 Introduction

Peter H. Gruber

Supported by the Algorand Foundation

Introduction

“To understand the power of blockchain systems, [. . .] it is important to distinguish between three things that are commonly muddled up, namely

1. the bitcoin currency,
2. the specific blockchain that underpins it and
3. the idea of blockchains in general.”

“The Trust Machine”, THE ECONOMIST, Oct. 31, 2015

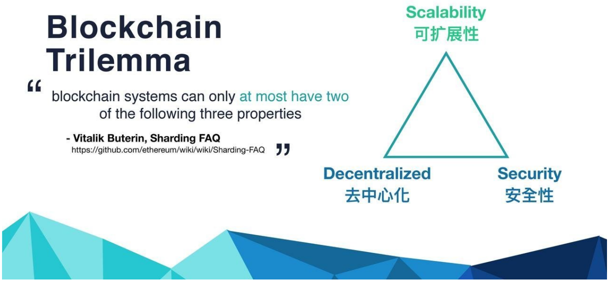
A digital ledger

1. **In the beginning**, Alice had 100 coins and Bob 50
2. Next, Alice paid 10 coins to Bob for bread
3. Then, Bob asked Alice to repair his house for 30 coins
4. Then, Alice went to Charlie's and bought coffee for 1 coin
5. . . .

COINS: _____ Alice _____ Bob _____ Charlie

Challenges

- Secure
- Decentralized
- Scalable



Blockchain Trilemma

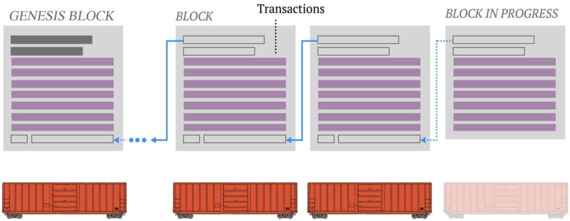
“blockchain systems can only at most have two of the following three properties

- Vitalik Buterin, Sharding FAQ
https://github.com/ethereum/wiki/wiki/Sharding-FAQ”

Security

Goal: Make it impossible to ”rewrite history”

- Concatenate *all(!)* transactions
- Apply 1-way cryptographic Hashing Algorithm (last slide)
- Start from *genesis block*
- Make it *costly* for a new block to get accepted



Security (2)

How do we make proposing a new block costly?
→ link to valuable/limited resource

Physical proofs

– proof of work (BTC, ETH 1.0)
– proof of elapsed time (use Intel's trused execution environment)
– proof of (disk) space (or retrievability, data possession; Chia)
– proof of space-time (similar, but over some amount of time)
– proof of capactiy (Signum)

Economic proofs

– proof of stake (ETH 2.0, . . .)
– pure proof of stake (Algorand)
– proof of authority (Lugano's triple-A blockchain)
– proof of burn

Algorand's consensus algorithm

Pure proof of stake

- Starting point: Bitcoin and ETH are energy hungry = dirty
- Goal: avoid malicious attacks
- Question: How can we do this without asking for costly energy burning?

The idea

- The Byzantine General's problem:
  Whom can I trust? Who has been bribed?
- If 51% of nodes are compromised, a majority vote would confirm fake transactions.
- So don't do a pure majority vote!
  - Randomly choose nodes that participate in a majority vote
  - An attacker does not know whom to bribe
  - Threshold requirement for compromised nodes increases

Consensus algorithms – discussion

Desirable properties of consensus algorithms

- Robustness against attacks
- Minimize waste (minimize signaling)
- Provide a competition-friendly framework for participants
- Incentivize participation in network (network effects)
- Cost efficient incentivisation to provide common goods
  - Provision of infrastructure (work/capacity/connectivity)
  - Participation in consensus
  - Participation in governance

Language

- **Blockchain:** a digital ledger or growing list of records/blocks, that are linked together using cryptography.
  Properties: decentralized, distributed, often public.
- **Key pair:** Two keys (public–private) in public key cryptography.
- **Address:** Public key, encoded for better readability.
- **Wallet:** Collection of several (public/private) keys.
- **Hash function:** Injective function that is difficult to invert.
- **Digital Signature function:** Injective. Verifiable cryptographic signature. Sign with private key, verify with public key.
- **Token:** Class of entries in a blockchain that represents an absolute claim, often ownership.
- **Layer 1:** Base or infrastructure layer of a blockchain, e.g. Bitcoin, Ether, Algorand.
- **Smart Signature:** Logic that can approve (or not) a proposed transaction.
- **Smart Contract:** Logic that can interact (read/write) with the blockchain.

Official terms and definitions: `https://www.federalregister.gov/d/2022-05471/p-58`

A brief history of Algorand

- 2017 work started; goal to improve over Bitcoin's inefficiencies
- 2017 company founded by Silvio Micali (MIT, Turing price)
- 2018-Feb 4M USD seed funding from Pillar, Union Sq. Ventures
- 2018-July Launch of testnet
- 2018-Oct 62M USD venture capital funding
- 2019-May launch of Algorand University program
- 2019-June auction of ALGO token
- 2019-July launch of mainnet
- 2020-Feb first version of PyTEAL
- 2021 First carbon negative blockchain

See also
`https://arxiv.org/abs/1607.01341`
`https://dl.acm.org/doi/10.1145/3132747.3132757` (first video)
`https://www.algorand.com/about/our-history`
`https://www.algorand.com/about/sustainability`
`https://github.com/algorand/pyteal/releases`

Algorand and USI

Global University Program
MIT
Massachusetts Institute of Technology
Stony Brook University
University of Waterloo
Università degli Studi di Salerno
Sapienza Università di Roma
Tel Aviv University
USI
Università della Svizzera italiana
北京大學
Peking University
Berkeley
University of California
清華大學
Tsinghua University

- USI joined the Algorand Global University Program in May 2019
- Algorand supports the USI foundation
- USI runs a validation node
- USI collaborates on research and teaching

Basic Cryptography

Hashing

- Ensure immutability of blockchain
- Proof of knowledge or existence without publication

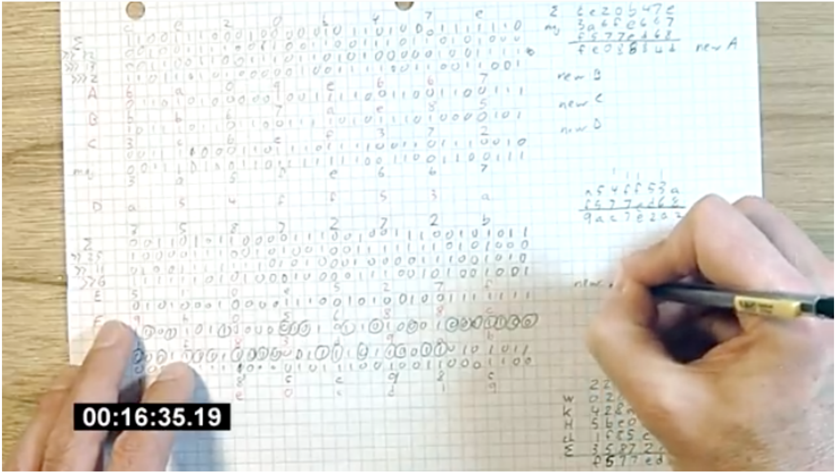
Signing

- Ensure Authority of sender of a message/trasaction

Encrypting

- Keep contents of a document secret, even if transported over public channel
- Usually not used in Blockchain

SHA-256 Hashing Algorithm



How to calcualte an SHA-256 hash by hand in 16 minutes

`https://www.youtube.com/watch?v=y3dqhixzGVo`