TECHNION Israel Institute of Technology

ANDREW AND ERNA VITERBI FACULTY OF ELECTRICAL ENGINEERING

Smart Contracts for Cryptocurrencies

May, 22 2018

TECHNION
Israel Institute of Technology

ANDREW AND ERNA VITERBI
FACULTY OF ELECTRICAL ENGINEERING

Shoval Loolian

David Strouk

Oded Naor
Supervisor


BITCOIN DIGITAL • DECENTRALIZED • PEER TO PEER
MJB MONETARY METALS
1 TROY OZ 999 FINE COPPER

Background

Bitcoin

- First decentralized digital currency, introduced in January 2009. Bitcoins are digital coins you can send through the Internet.

- No institution controls it. Bitcoins are produced by people using software that solves mathematical problems (mining).

- Bitcoin transactions are processed and validated by the Bitcoin network, no centralized party is involved.

- Transfer of Bitcoins consists not of physically moving an object from A to B, but simply of adding a new, publicly accepted transaction to the blockchain.

Identities

Private Key

- Randomly generated string (numbers and letters)
- Required to control your funds

`5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF`

Public Key (“Address”)

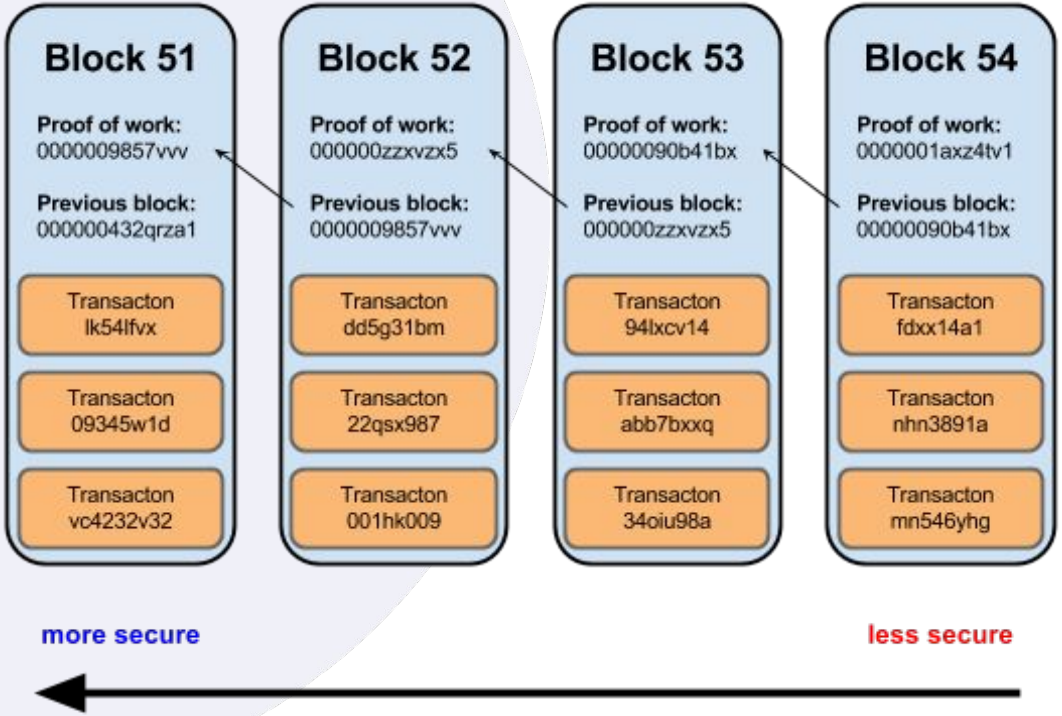
- The Address is derived from the private key by hash function
- Represents a possible destination for payment

`1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2`

Blockchain

- Growing general public ledger of cryptographically-signed transactions.
- All transactions are public, but are not tied to anyone’s real identity.
- We can see that address A sent a message to address B, but we can’t know which entity is A or B, unless he declares it himself.
- Secured by collective compute power of miners.

Blockchain



Blocks are “more secure” as you go further back in the chain

Mining

- Miners are awarded newly-minted Bitcoins or transaction fees for successfully finding blocks.

- The distributed algorithm ensures that bounty of new bitcoins will asymptotically approach 21M, and the reward for mining will then become transaction fees only.

- The distributed algorithm dynamically adjusts how much computing power it takes to find a valid block, limiting block creation to around 1 block every 10 minutes for Bitcoin (for Ethereum it is 1 block every 12 seconds).

Background

Ethereum

- Decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.

- *“The core idea was simple: a blockchain with a built-in Turing-complete programming language, allowing users to build any kind of applications on top.”* - Vitalik Buterin

Smart Contracts

Bitcoin VS Ethereum

Bitcoin VS Ethereum

	Bitcoin	Ethereum
Founder	Satoshi Nakamoto	Vitalik Buterin
Release Date	9 Jan 2009	30 July 2015
Blockchain	Proof of Work	proof of work (Planning for PoS)
Utility	Digital currency	Smart contracts Digital currency
Cryptocurrency used	Bitcoin	Ether
Supply cap	21 million in total	18 million every year
Price	Around 8500$	Around 730$
Blocks Time	10 Minutes	12-14 seconds

Bitcoin VS Ethereum

- Ethereum is more general, not just a currency (Ether).
- Each node has a virtual machine forming a planetary scale computer.
- The virtual machines run “smart contracts”.
- Users can call functions on the contract = transactions.


K-of-N Multisig

The Problem

- N-of-N Multisig: what if someone can’t access his personal key?
- Funds will be inaccessible because there are only N-1 available keys.
- We want to allow (N-1)-of-N Multisig under special circumstances.

Our Smart Contract

- If the group suspects that one of the members lost his access to its private key, it can publish a challenge to the suspicious user.
- The user have a predefined period of time to respond the challenge.
- If he didn’t send any response, then the common account becomes a (N-1)-of-N Multisig.

Related problems

- Blockchain is an asynchronous system and because of that we can't measure time.
  In the blockchain, we can "measure time" by counting blockchain height.

- Members of the group can exploit this mechanism for malicious purposes, by publishing unnecessary challenges.
  In case of an answered challenge, publishers will be charged a fee.

- All members need to be always connected to the blockchain so they can respond to eventual challenges.
  Users can be alerted of a challenge by other ways, yet they need to be "online".

Project Goals

1. Get familiar with concepts of blockchain, Bitcoin, Ethereum, smart contracts, …
2. Install a work environment for building and running smart contracts on Ethereum blockchain.
3. Learn how to write in Solidity / Vyper and choose one language.
4. Designing and programming the code of our smart contract.
5. Search and solve security breaches and issues in our code.
6. Run our contract on a Test Network.

Project Tools

Work Environment

- Linux Ubuntu Server

Programming languages

- Solidity - mainly used
- Vyper (Python-like)

Other tools

- GitHub
- Remix IDE
- Metamask


THANK YOU