ETHEREUM BASIC COURSE 002

By: Mr. Chainblockz

On: 28 July 2018

Goals

- After finishing the course, you can
  - *apply for Ethereum blockchain developer positions*
  - *build your own blockchain application with Ethereum*

Course Roadmap

- Basic Course
  - *Day 1 Ethereum and Smart Contract*
  - *Day 2 Key Concepts revisit and Compiling + Testing + Deployment*
  - *Day 3 Your own framework vs Truffle framework*
  - *Day 4 A complicated block-chain solution for a real problem*
- Advanced Course
  - *Day 5 ICO and Token*
  - *Day 6 ICO and Token (continued) & IPFS*
  - *Day 7 Oraclize & Private Network*
  - *Day 8 Security Awareness & Some Design Patterns*

Day 1 Outline

- Metamask installation
- Our first contract demo – Inbox
- Why is Ethereum?
- What is Ethereum?
- A few preliminary concepts
- Our second contract demo – Lottery
- More fun expected
- Caveat
- Recap

Day 2 Outline

- Let's go over it again
  - *External Account vs Contract Account*
  - *Bytecode vs ABI*
  - *Inbox Revisit*
  - *Common Function Types*
  - *External Account to External Account Transaction*
  - *External to Create Contract Transaction*
  - *Calling a function vs Sending a Transaction to a function*
  - *Ether vs Wei vs other units*
- Demo - Inbox project
  - *Compiling*
  - *Testing*
  - *Deployment*
- Recap

Day 3 Outline

- Web App Traditional Architecture
- Web App Ethereum Architecture
- Lottery Prototype
- Injected web3
- Demo - Lottery with React
- Truffle introduction
- DIY - Pet Shop tutorial
- Recap

Day 4 Outline

- A look at Kickstarter
- Kickstarter’s problems
- A blockchain-based solution
- Coding time
- Recap

Day 5 Outline

- What is ICO?
- What is Token?
- What are popular ICOs?
- Demo – Create own token and ICO
- Recap

Day 6 Outline

- ICO and Token (continued)
- What is IPFS?
- Why is IPFS well-suited to Ethereum world?
- Demo - Upload file to IPFS and inform Ethereum user
- Recap

Day 7 Outline

- Oraclize
  - *How does it work?*
  - *Examples*
  - *Let's code*
- A private network setup
- Recap

Day 8 Outline

- Security Awareness
  - *Re-Entrancy*
  - *Arithmetic Over/underflows*
  - *and more*
- Some Design Patterns
  - *Withdrawal from Contracts*
  - *Restricting Access*
  - *State Machine*
  - *Multisig Wallet (https://github.com/ConsenSys/MultiSigWallet/blob/master/MultiSigWalletWithDailyLimit.sol)*
  - *Upgradable Smart Contract*

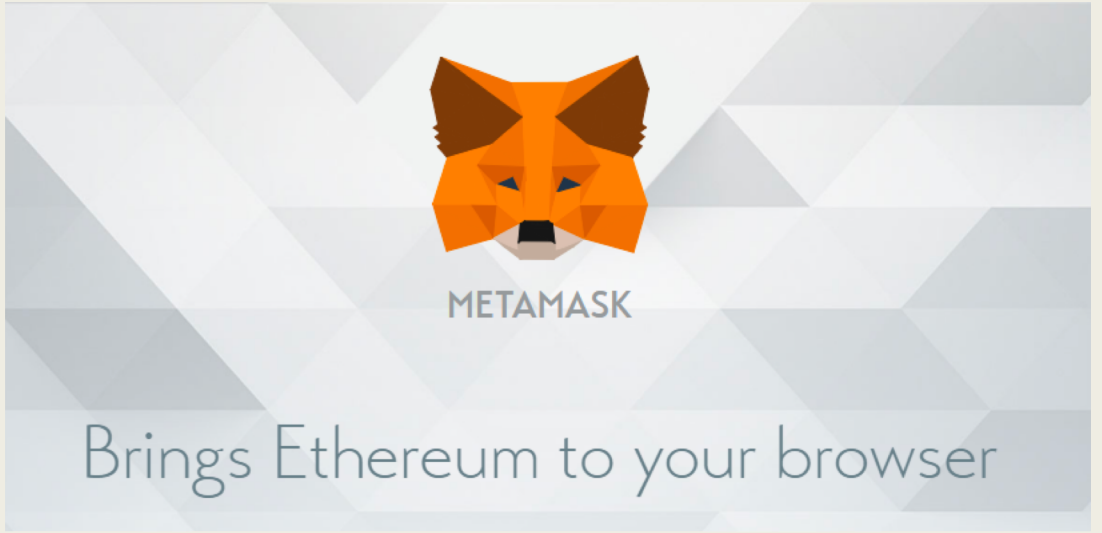
GET TO KNOW EACH OTHER

Day 1 Outline

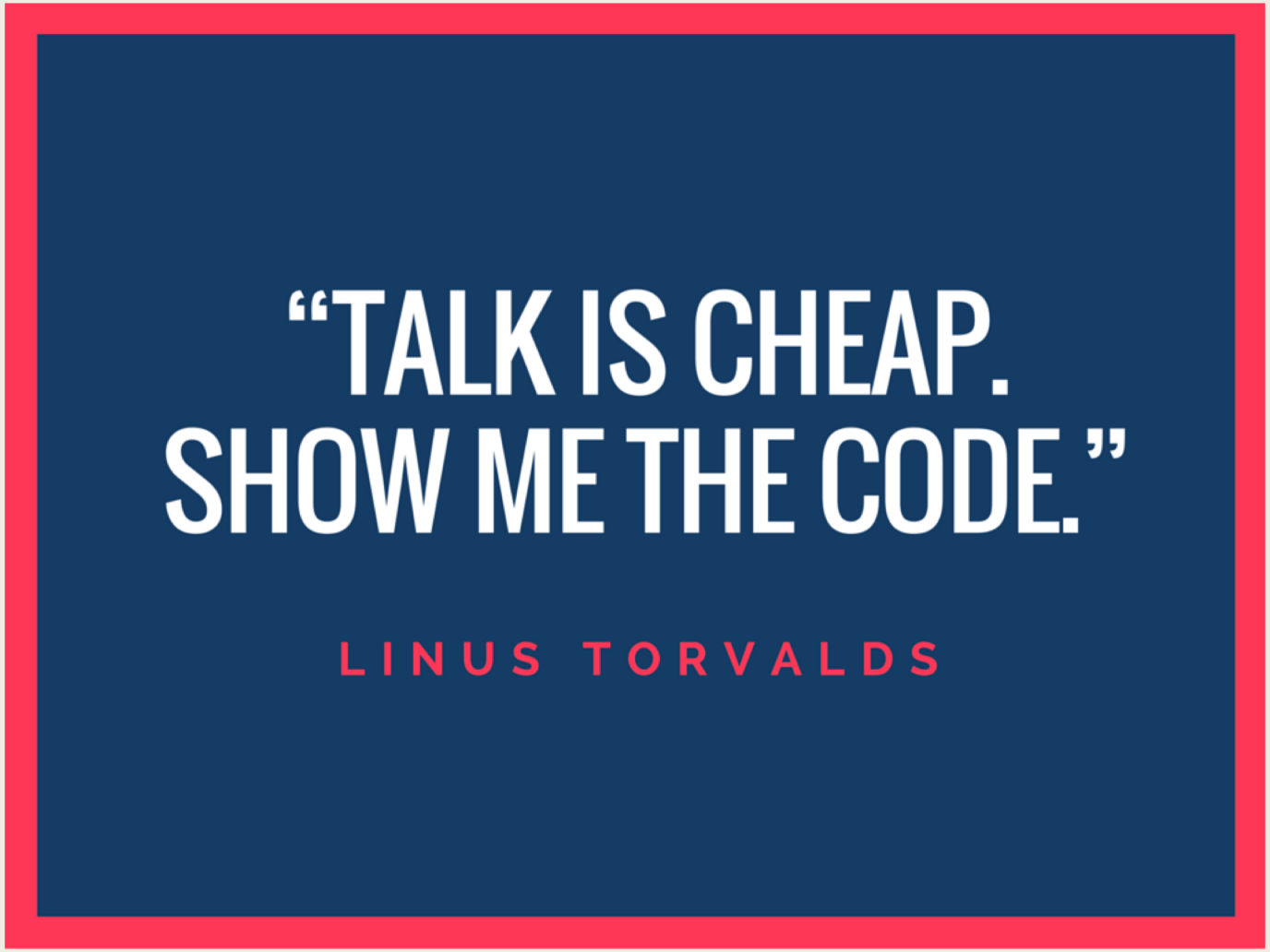
- Metamask installation
- Our first contract demo – Inbox
- Why is Ethereum?
- What is Ethereum?
- A few preliminary concepts
- Our second contract demo – Lottery
- More fun expected
- Caveat
- Recap

Metamask

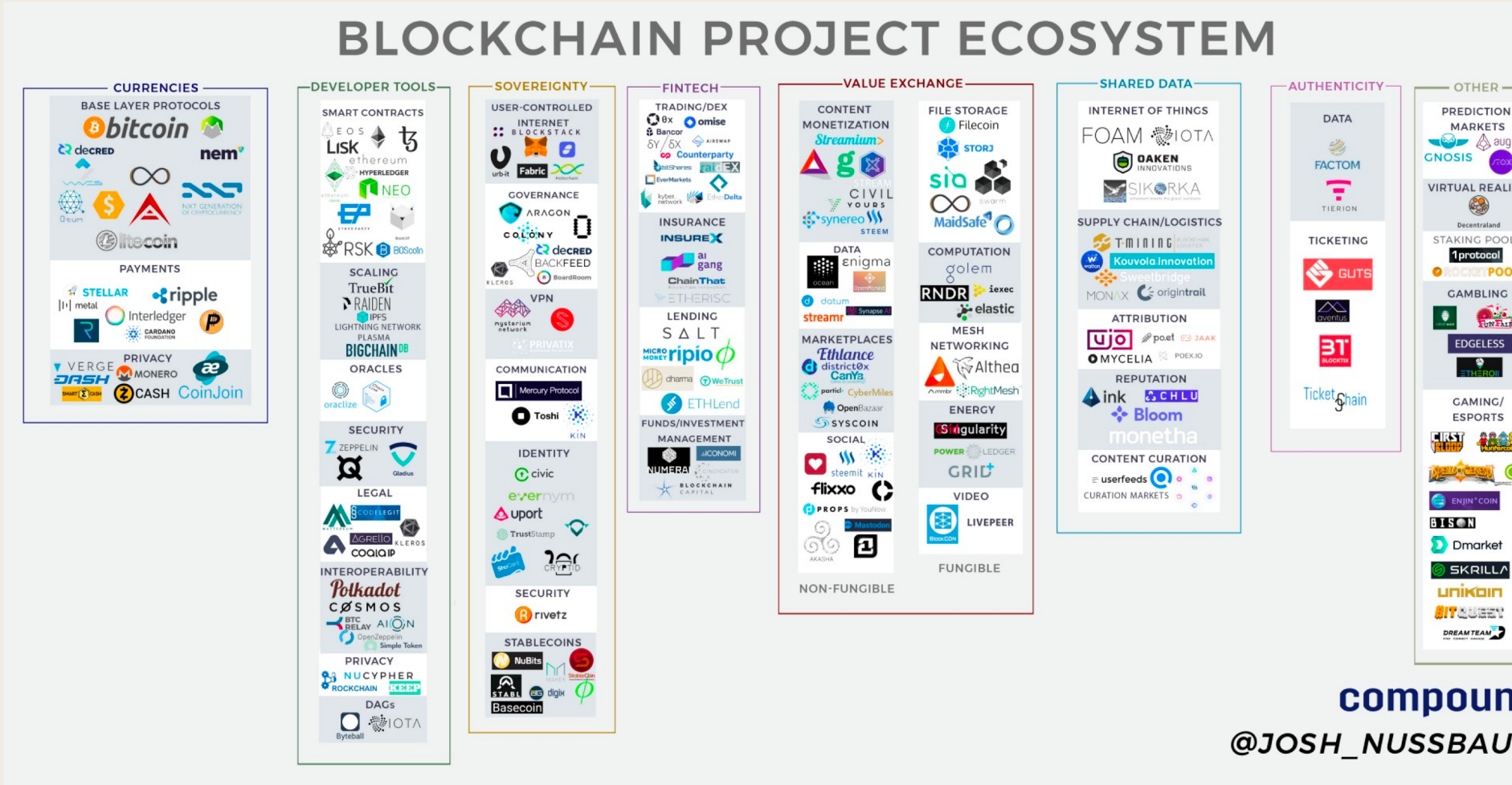
- Hot wallet ~ internet-enabled wallet
- Installation
- Get some ethers
- Play around



Inbox



Why is Ethereum?



Why is Ethereum?

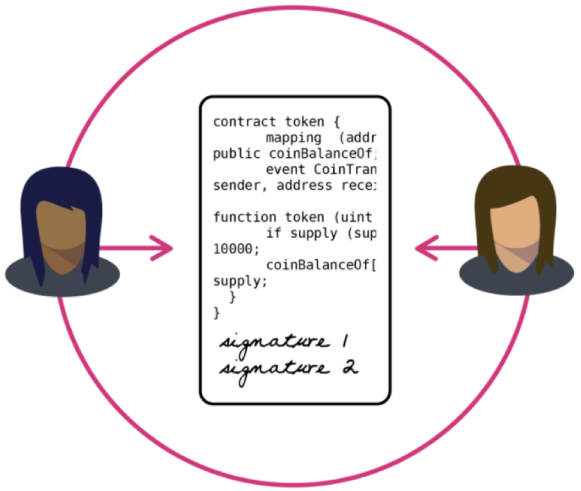
- You can start building your Đapp quickly
- You can apply up to 80% of job posts on the market
- ICO is damn easy

What is Ethereum in a few words?

- A world computer
- A platform so that Đapp can be build on top
- Cannot fail, be stopped or be censored

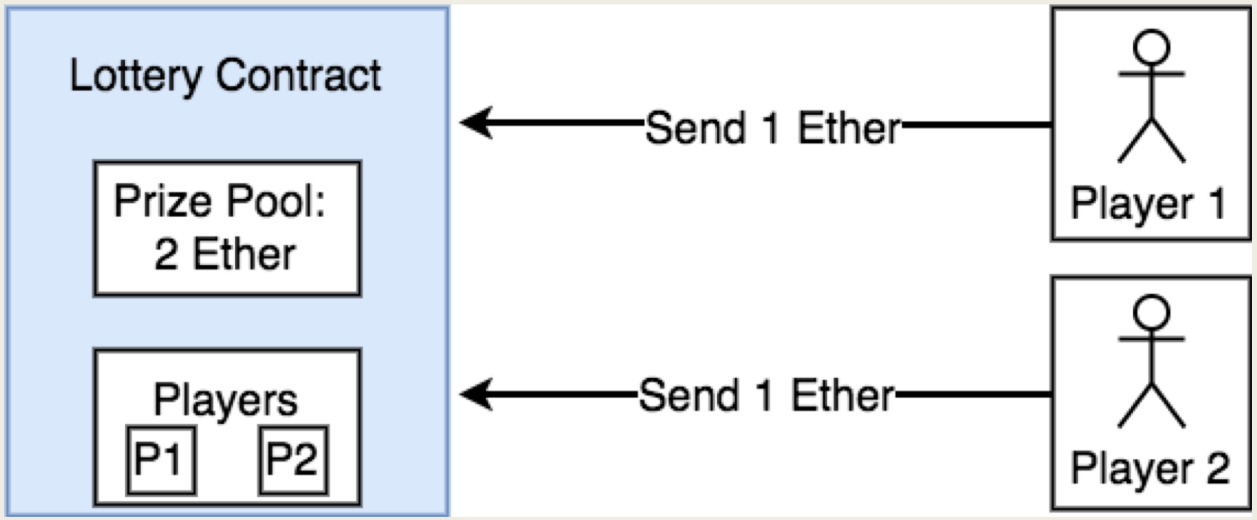
A few preliminary concepts

- Smart contract
- Ether
- Transaction
- Gas
- Wallet

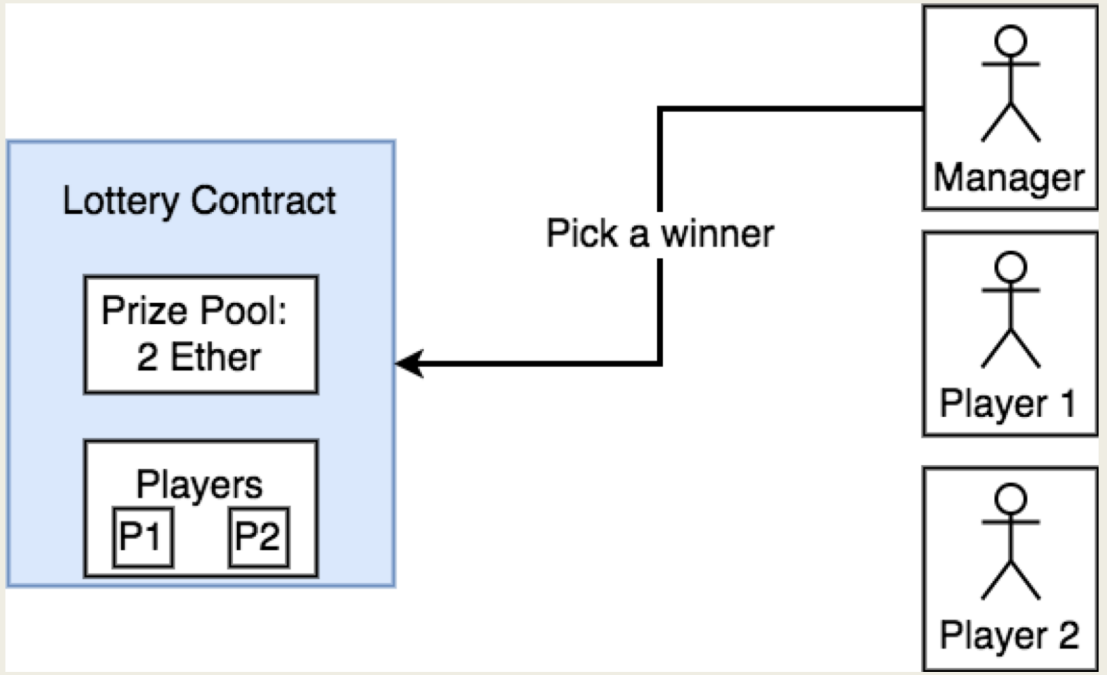


	Gas consumed by operation	Gas remaining
Start of transaction		150
STORE 31	45	105
ADD 2 numbers	10	95
STORE sum	45	50
End of transaction	The number 31 and the sum is stored and written to the blockchain.	

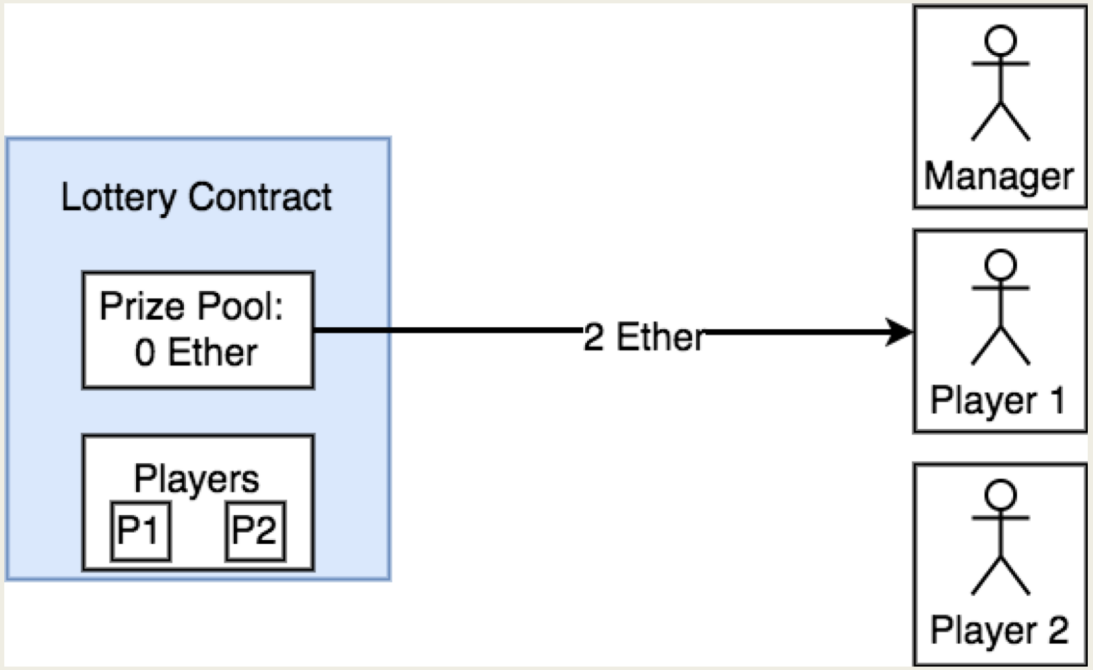
Lottery illustration



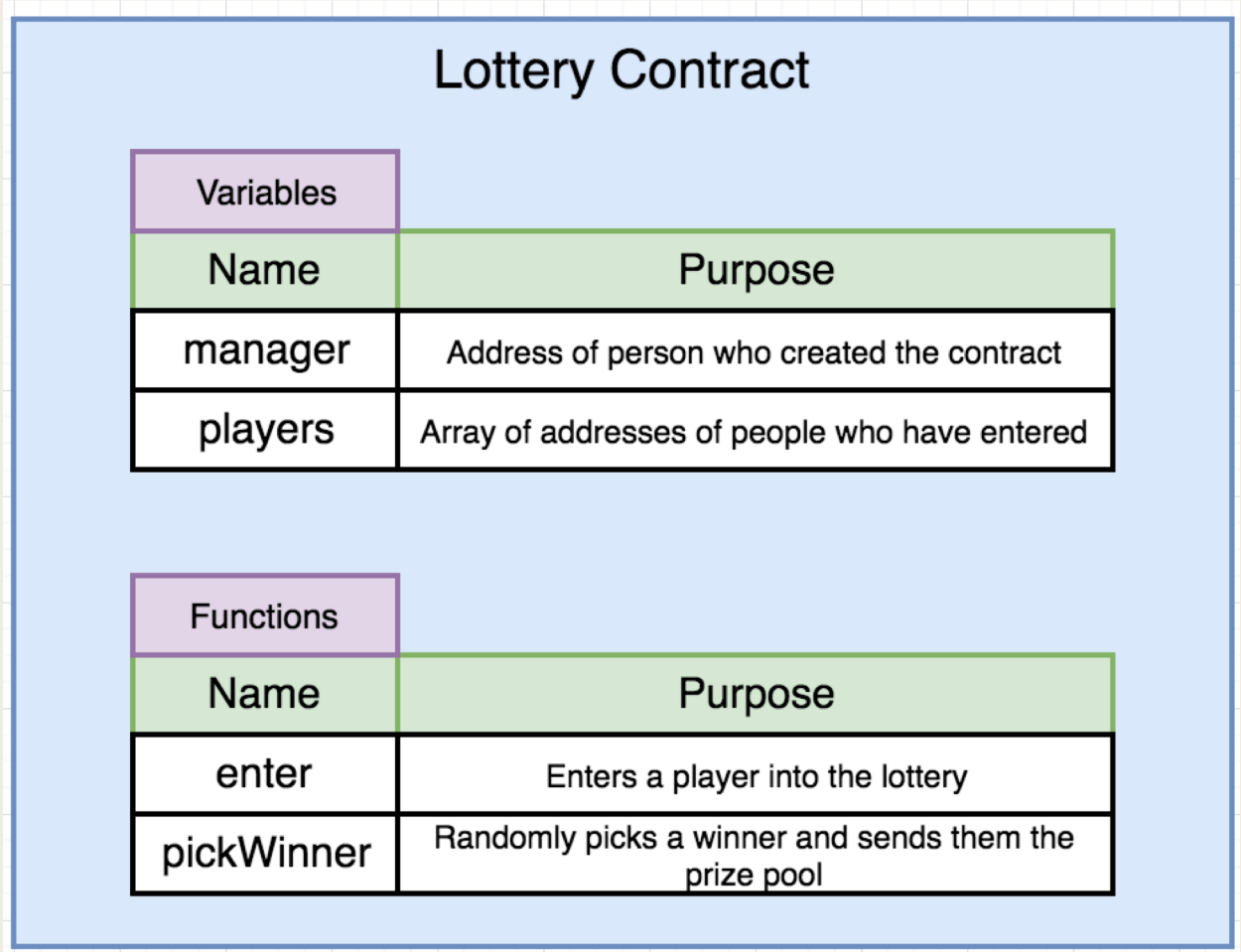
Lottery illustration



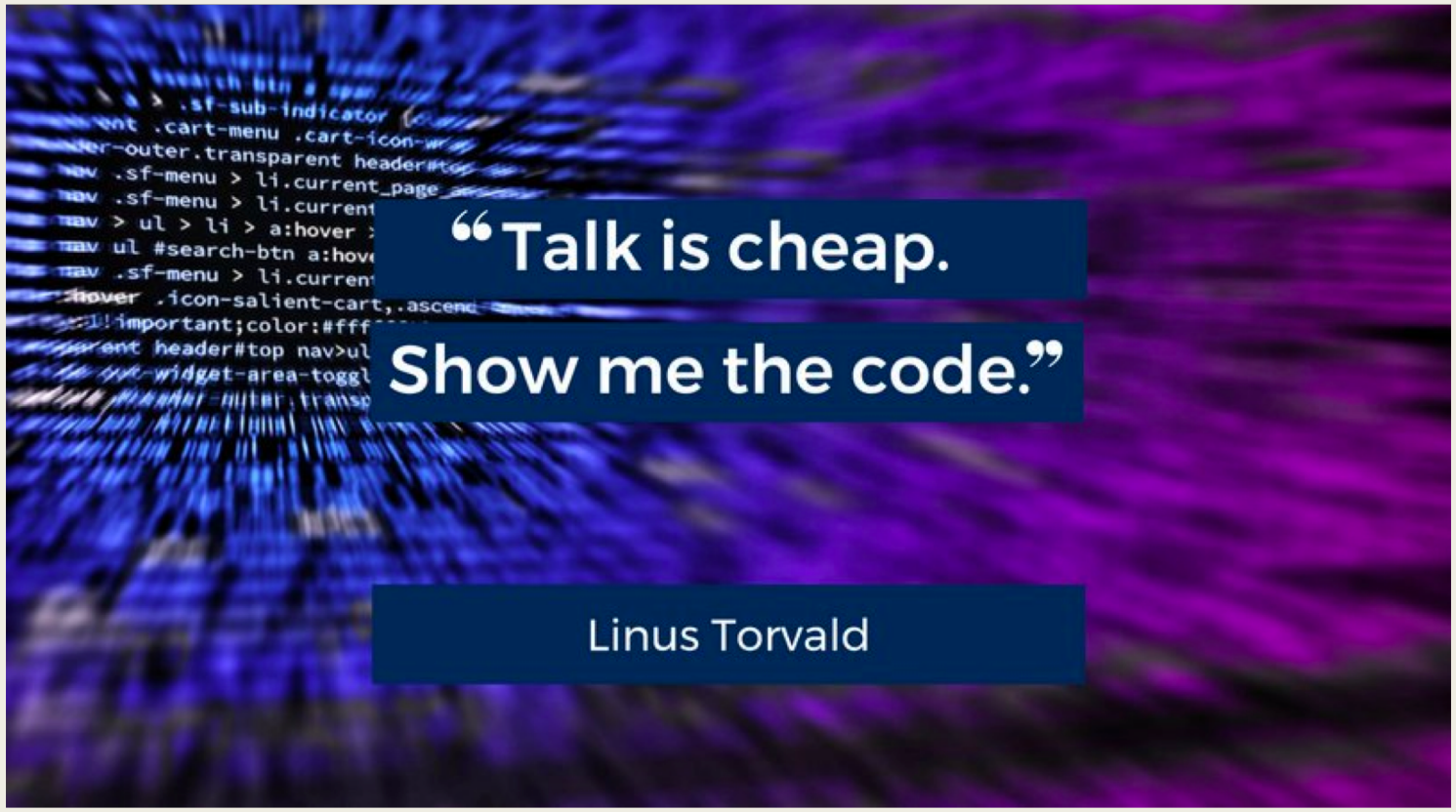
Lottery illustration



Lottery


Lottery Contract
Variables
Name
Purpose
manager
Address of person who created the contract
players
Array of addresses of people who have entered
Functions
Name
Purpose
enter
Enters a player into the lottery
pickWinner
Randomly picks a winner and sends them the prize pool

Lottery



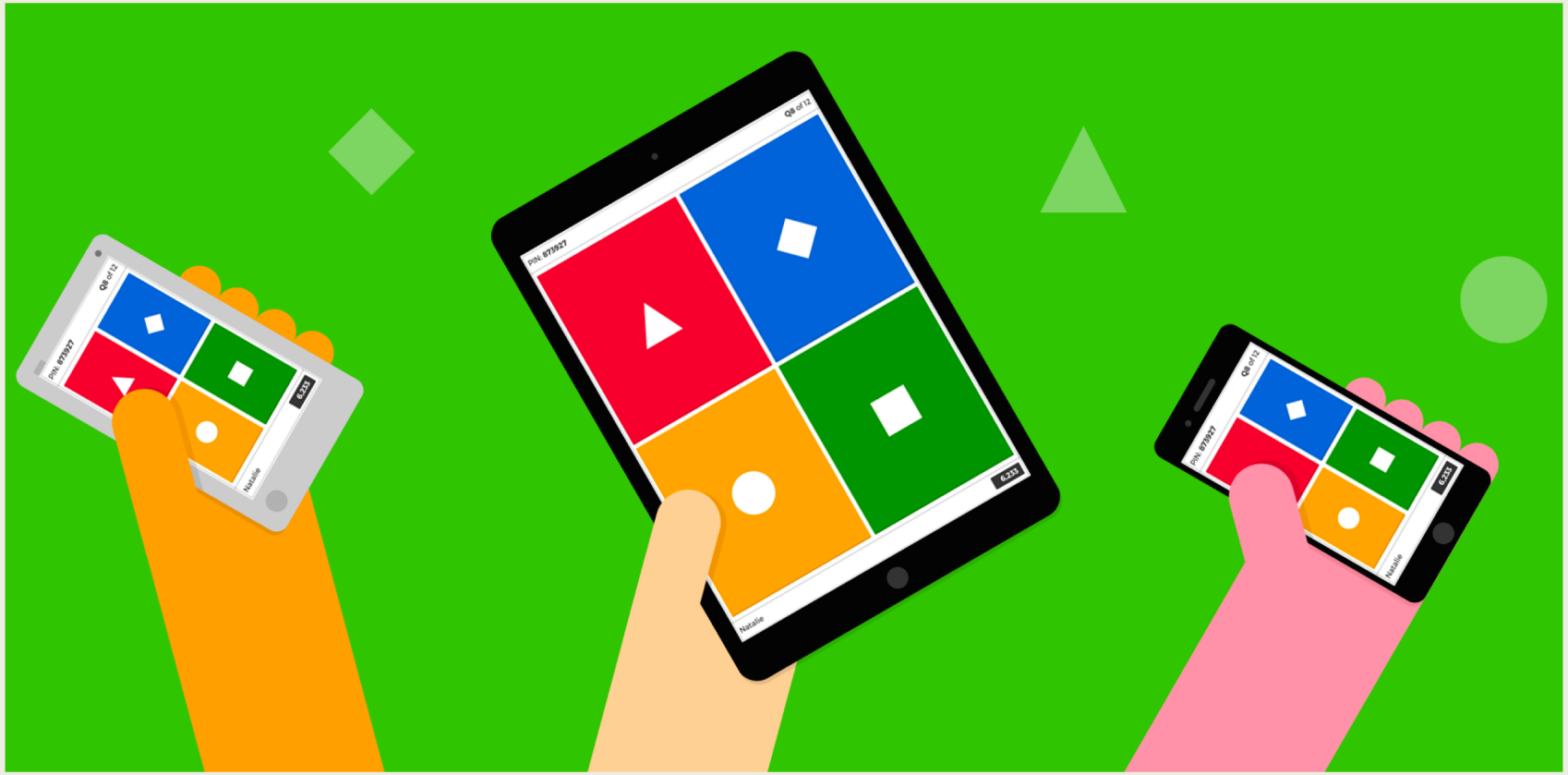
Fun stuff

Fun stuff

Fun stuff

- https://www.stateofthedapps.com/
- https://dappradar.com/

Fun stuff



Caveat

- Ethereum scaling issue
- Ethereum is costly
- No more Agile
- Read more
  - https://medium.com/@jimmysong/why-blockchain-is-hard-60416ea4c5c
  - https://hackernoon.com/ether-purchase-power-df40a38c5a2f
  - https://hackernoon.com/costs-of-a-real-world-ethereum-contract-2033511b3214

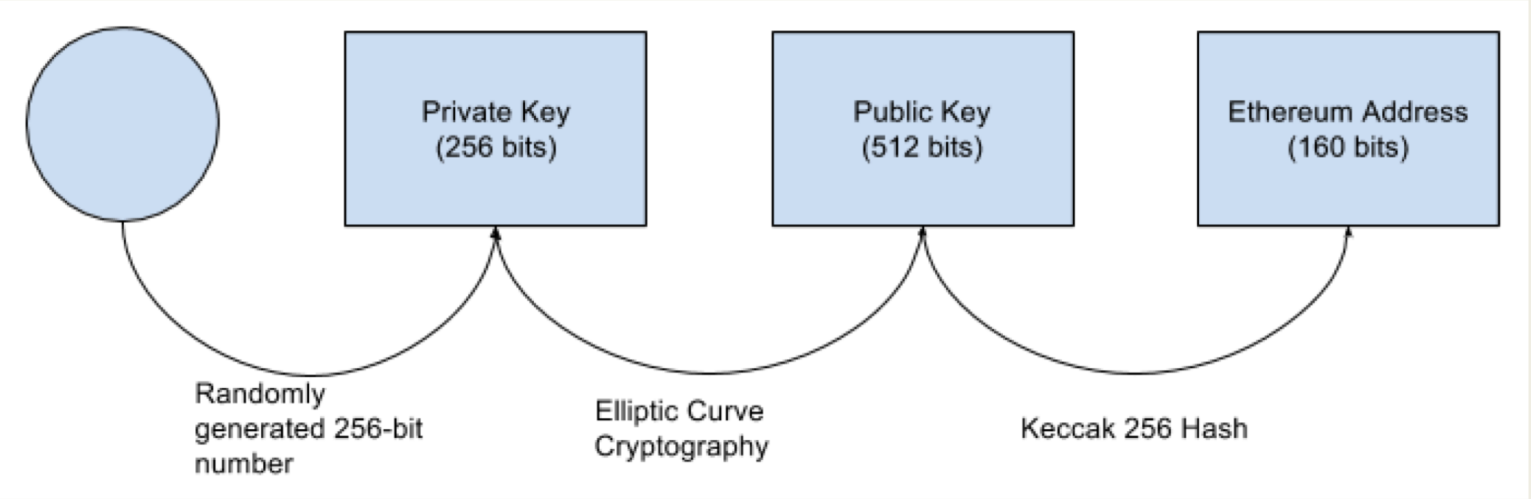
Recap

- Ethereum or all kind of blockchain technologies is simple to pickup
- However, Ethereum / blockchain is not mature yet
- Yet, Ethereum / blockchain has a huge potential ahead

LAST SESSION'S Q&A

How to generate an Ethereum address?

- Step 1: Create a random private key (64 hex characters / 256 bits / 32 bytes)
- Step 2: Derive the public key from this private key (128 hex characters / 512 bits / 64 bytes)
- Step 3: Derive the address from public key by taking the last 40 hex characters / 160 bits / 20 bytes



The chance that 2 Ethereum addresses are duplicate

- One Ethereum address has 40 hex characters, each has 16 possibilities
- Hence, the total possibility addresses are 16 ^ 40 = 1461501637330902918203684832716283019655932542976
- Assume we have 6 billion Ethereum users and each user has 10 addresses, the chance that 2 addresses are duplicate is
  - *(10 * 6 000 000 000) / (16 ^ 40) * 100 %* = **0.00000000000000000000000000000041053665947 %**

How to find solidity code for a contract address

- No, you can’t unless the smart contract developers choose to reveal it.

Remix At Address

- You have to have ABI