Intro to Blockchain

CubCon

Nadir Akhtar
Ronen Kirsh

AGENDA

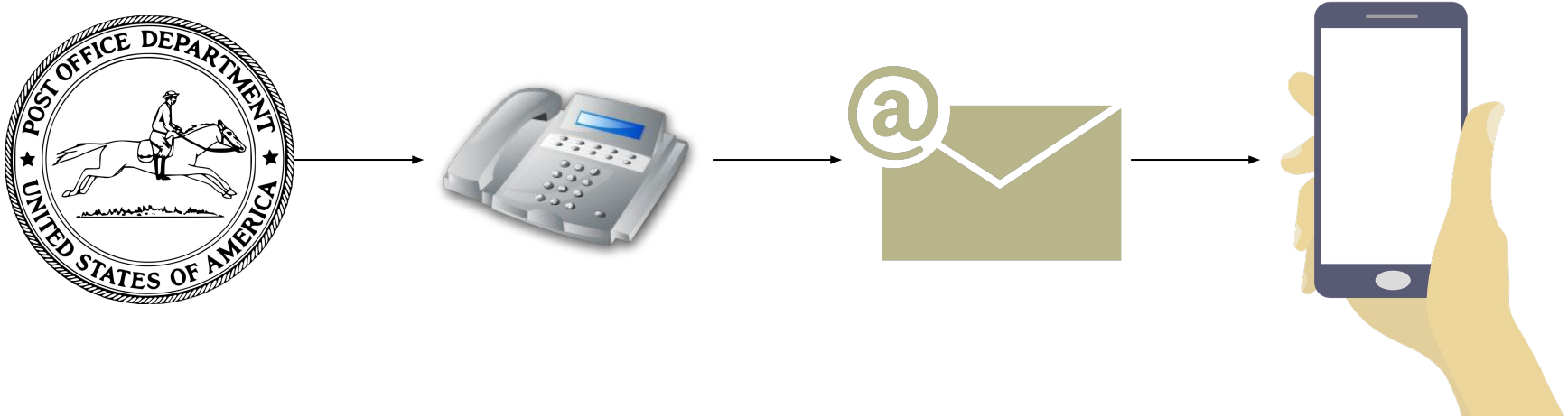
INTRO TO BLOCKCHAIN

1. Why Should You Care?
2. Understanding Bitcoin and Consensus
3. Blockchain Types and Platforms
4. Use Cases and Application
5. Blockchain at Berkeley
6. Earn your first Bitcoin

1 WHY SHOULD YOU CARE?

DIGITIZATION

MACRO TRENDS



BankAccount
owner : String balance : Dollars = 0
deposit (amount : Dollars) withdrawal (amount : Dollars)

DECENTRALIZATION

MACRO TRENDS

UBER

MARRIOTT

airbnb

EXPONENTIAL GROWTH

	EXPLOITING THE TECHNOLOGY INTENSIFICATION, SEQUENCING	WASTING THE TECHNOLOGY PROLIFERATION, PARALLELIZING
COMPUTATION MOORE'S LAW	MAINFRAMES SUPERCOMPUTERS	PC'S CLOUD COMPUTING
COMMUNICATION BUTTERS' LAW	BELL SYSTEM	INTERNET
MEMORY/STORAGE KRYDER'S LAW	BIG DATA	BLOCKCHAIN
NETWORK AND POWER		
BENEFIT	STATIC EFFICIENCY	ADAPTABILITY, ROBUSTNESS, UPTIME
STRATEGY	TYPICALLY SUSTAINING	TYPICALLY DISRUPTIVE

https://www.bcg.com/blockchain/thinking-outside-the-blocks.html

THE REVOLUTION OF VALUE

THE FUTURE

Internet is for sharing **information** instantly as Blockchain is for sharing **value** instantly.

LIVE EXAMPLE

DON'T BE SHY

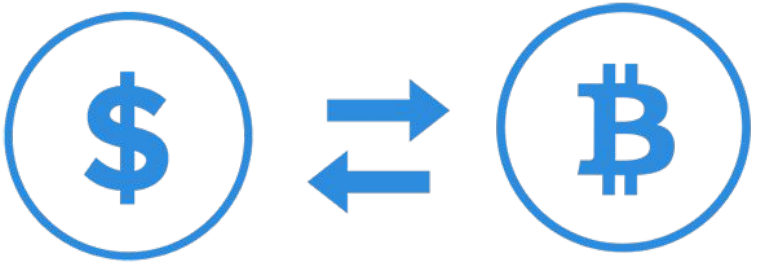
Volunteers?

2 BITCOIN AND CONSENSUS

WHAT IS BITCOIN?

FIRST CRYPTOCURRENCY

- Inspiration for the blockchain
- “Cryptocurrency”
- Secured with cryptography
- Value based on speculation



https://www.coinbase.com/buy-bitcoin

THE BIRTH OF BITCOIN

GENESIS BLOCK

Bitcoin was created by Satoshi Nakamoto in 2009

- First ever decentralized, trustless system for transactions
- Prices rose sharply, fell, then rose back again
  - Notorious for volatile value
- Inspired creation of other cryptocurrencies
  - Ethereum, Litecoin, Dogecoin...

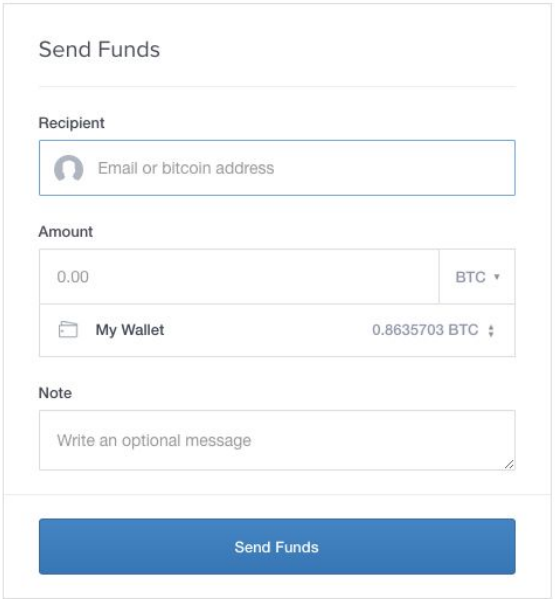
Dorian Satoshi Nakamoto
(not actually Satoshi Nakamoto)

BITCOIN WALLETS

STORING BITCOIN

- Software to hold Bitcoin with a unique address
- Private and Public Keys
  - Think Password and Email address
- Transaction components:
  - Sender
  - Receiver
  - Amount
- “Miners” check for:
  - Signature
  - Balance
  - Duplicates

1LNnJDNTUXYUfmbiVcngKGg52N8TKNPw6J



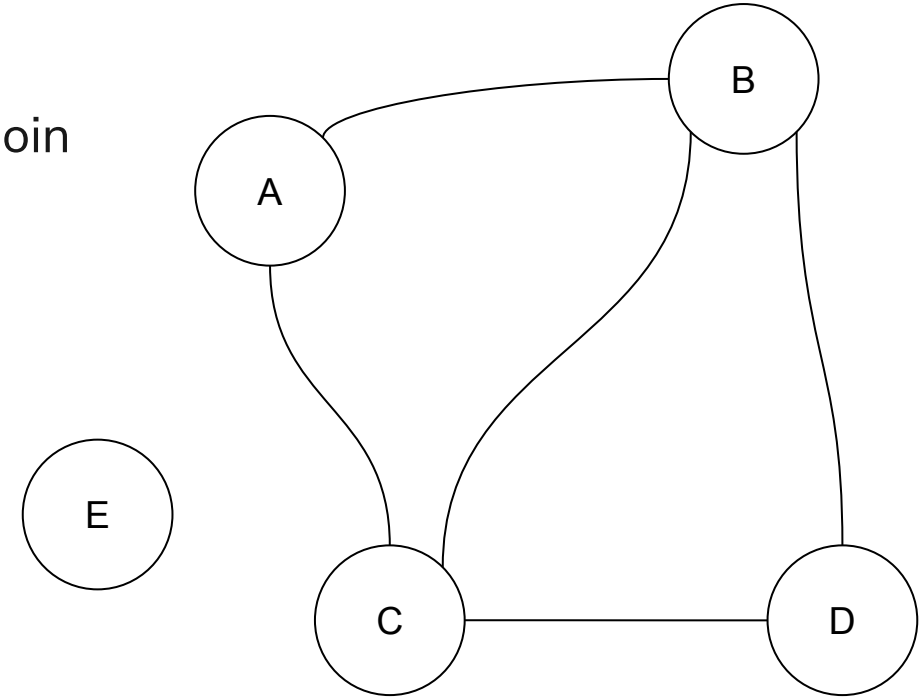
Coinbase interface

WHO REGULATES BITCOIN?

INTRO TO BLOCKCHAIN

No central authority; anyone can join

- Just requires a computer
- All peers are created equal*
- All peers connected

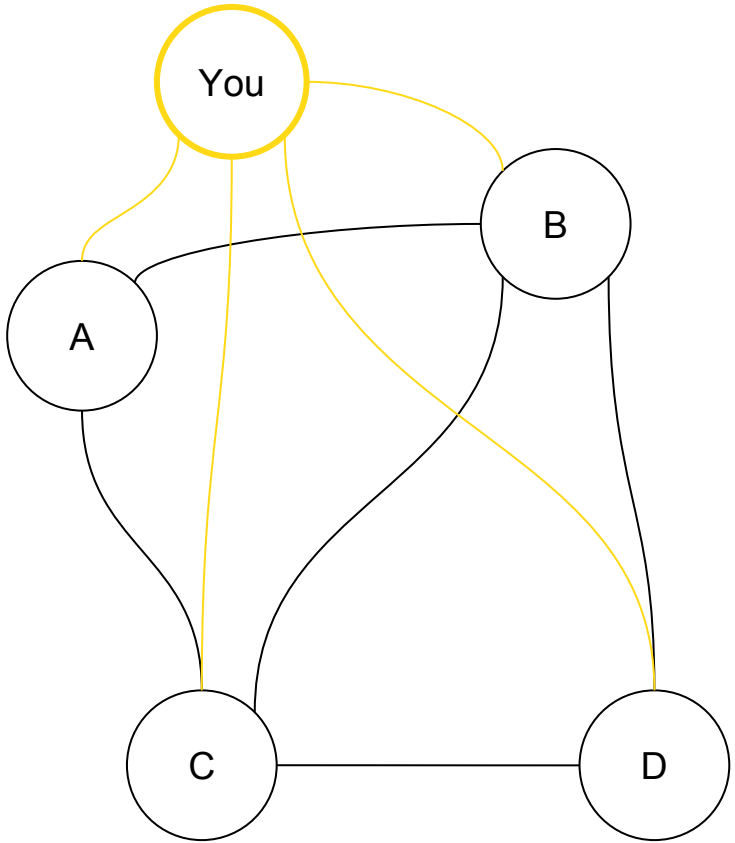


CAN I JOIN?

INTRO TO BLOCKCHAIN

Of course!

- No formal registration process
- Generate public and private key
- Secure access to funds

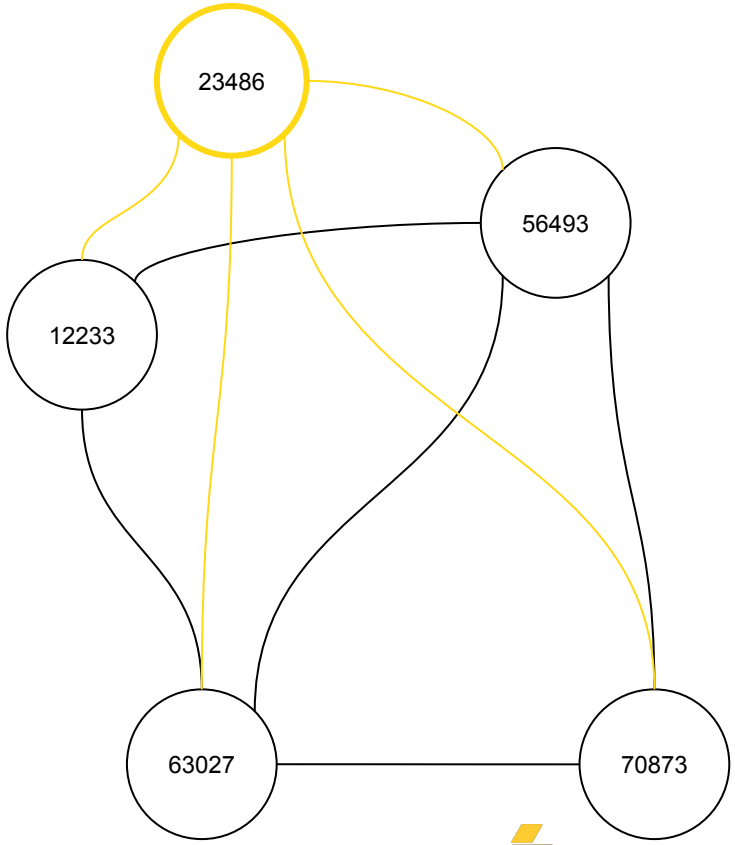


WHAT DO PEOPLE KNOW ABOUT ME?

EVERYONE'S A STRANGER

Not much....

- No central regulation
  - Just don't share public key
- Difficult to trace activity
  - But not impossible

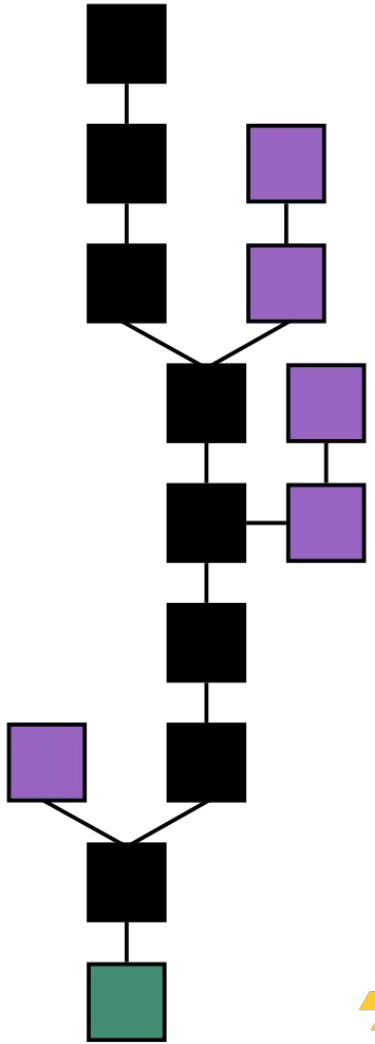


3 BLOCKCHAIN TYPES AND PLATFORMS

WHAT IS BLOCKCHAIN?

INTRO TO BLOCKCHAIN

- The technology underlying Bitcoin
- Data management infrastructure
- Enabler of distributed consensus
- An unbreakable chain of truth



https://upload.wikimedia.org/wikipedia/commons/thumb/9/98/Blockchain.svg/385px-Blockchain.svg.png

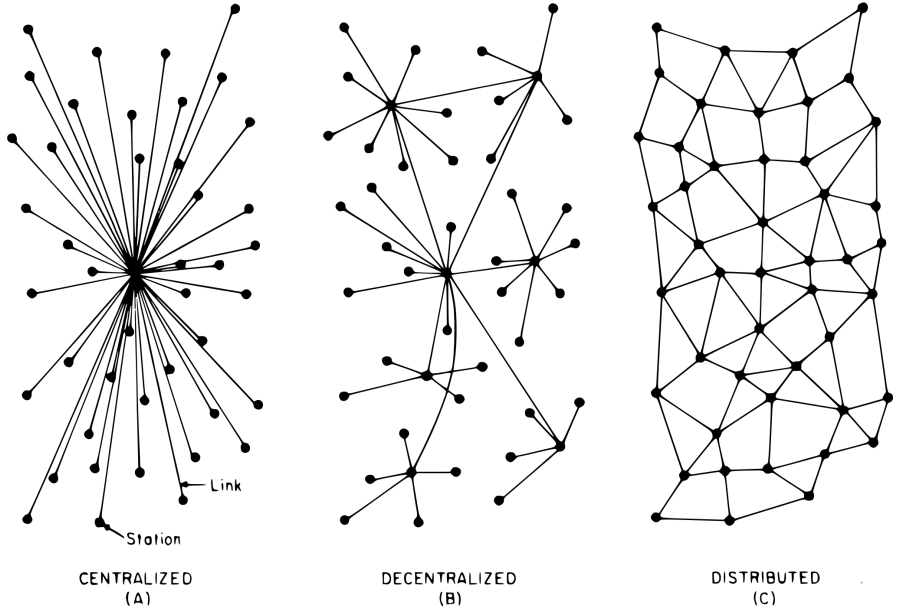
TYPES OF BLOCKCHAINS

INTRO TO BLOCKCHAIN

Fully Private Blockchain - write permissions are kept centralized to one organization.

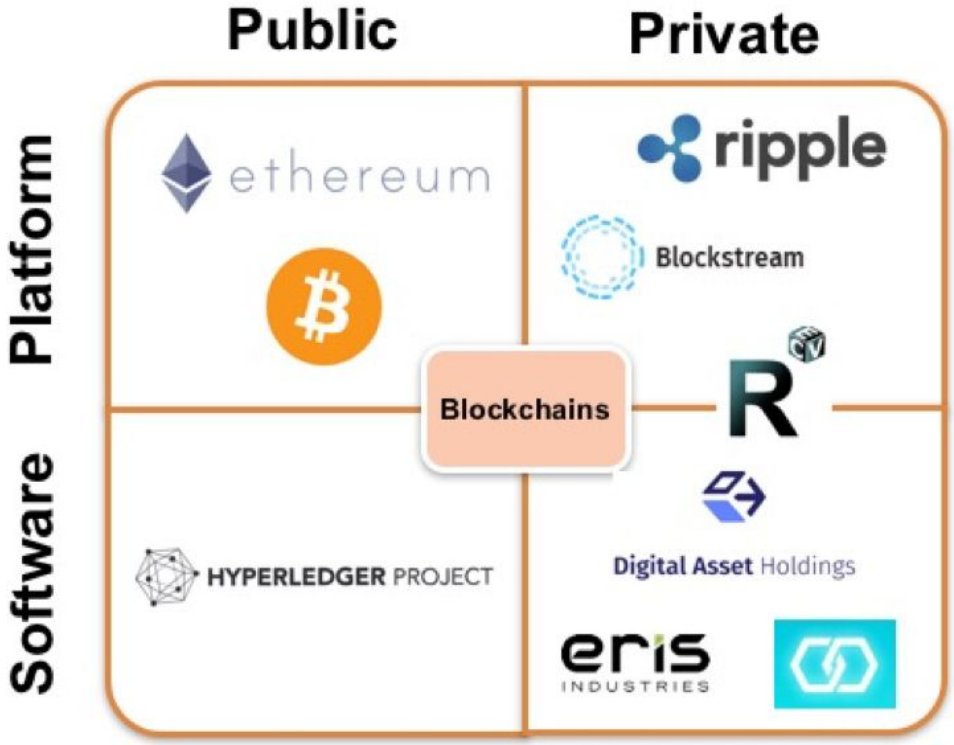
Consortium Blockchain - the consensus process is controlled by a preselected set of participants

Public Blockchain - anyone in the world can participate in the consensus process.



(From Vitalik Buterin: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/)

TYPES OF BLOCKCHAINS

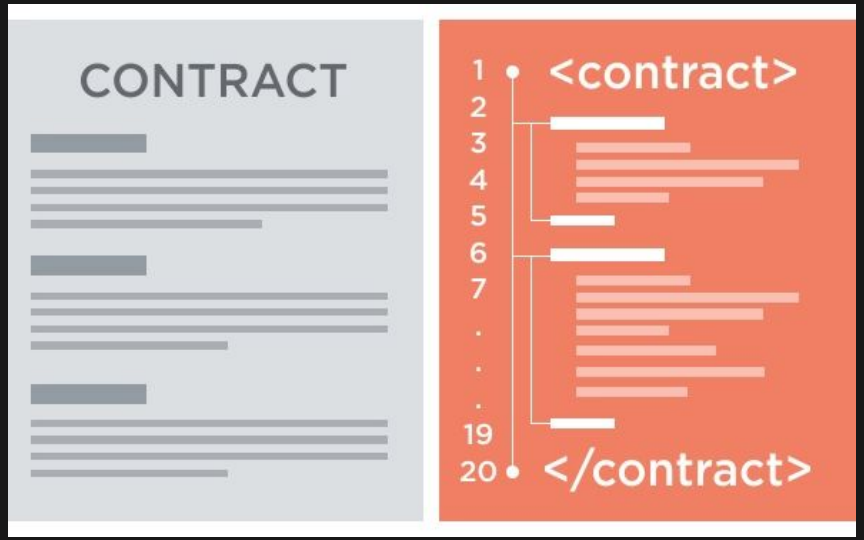


http://www.coindesk.com/state-of-blockchain-q1-2016/

WHAT IS ETHEREUM?

AUTOMATING THE BLOCKCHAIN

- **Ethereum:** Smart Contract Platform
  - Complex and feature-rich
- **Bitcoin:** Decentralized Asset
  - Simple and robust



https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/

WHAT IS A SMART CONTRACT?

ONLY AS SMART AS YOU MAKE IT

con·tract

(noun) /ˈkäntrakt/

1. a written or spoken agreement ... that is intended to be enforceable by law.

smart con·tract

(noun) /smärt ˈkäntrakt/

1. code that facilitates, verifies, or enforces the negotiation or execution of a digital contract.
    a. Trusted entity must run this code

```
contract token {
    mapping (address => uint) public coinBalanceOf;
    event CoinTransfer(address sender, address receiver, uint amount);

  /* Initializes contract with initial supply tokens to the creator of the contract */
  function token(uint supply) {
        if (supply == 0) supply = 10000;
        coinBalanceOf[msg.sender] = supply;
    }

  /* Very simple trade function */
    function sendCoin(address receiver, uint amount) returns(bool sufficient) {
        if (coinBalanceOf[msg.sender] < amount) return false;
        coinBalanceOf[msg.sender] -= amount;
        coinBalanceOf[receiver] += amount;
        CoinTransfer(msg.sender, receiver, amount);
        return true;
    }
}
```

4 USE CASES

DECENTRALIZED PREDICTION MARKETS

INCENTIVES FOR HONESTY

Prediction markets draws on the wisdom of the crowd to **forecast the future**

INITIAL COIN OFFERINGS (ICOs)

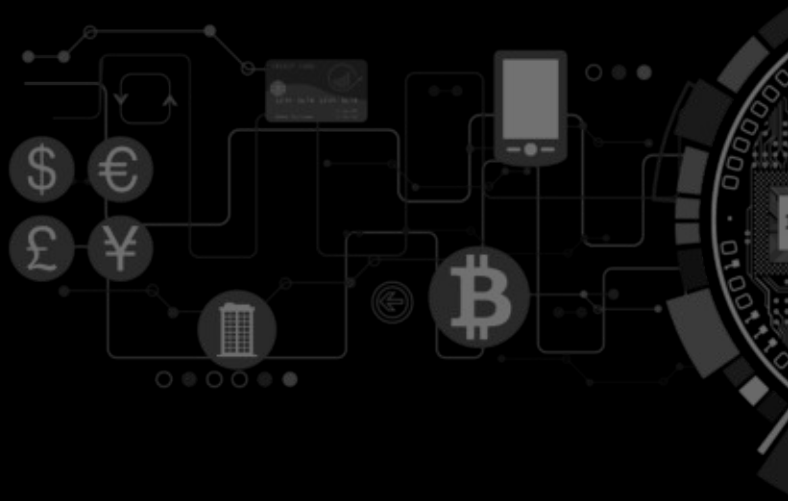
INVESTING REIMAGINED

Cryptographic Token

24/7 Trading

Equity Token vs. AppCoin

Capitalism for Open-Source



DECENTRALIZED ESCROW

BUY A HOUSE IN AN HOUR

Definition:
"...*Money held by a third-party on behalf of transacting parties. It kept in the custody of a third party and taking effect only when a specified condition has been fulfilled*"

Example use cases:

- Buying a house
- Business Deals (If-this-then-that)
  - Redundant, logical, task-related
- Peer-to-Peer community crowdfunding
  - Gofundme with lower the fees (8% → 0.1-1%)

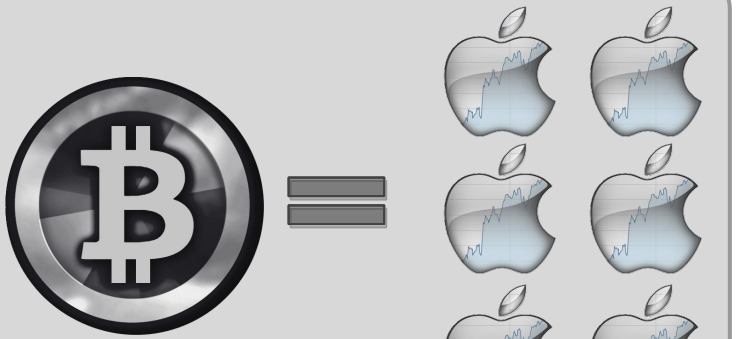
https://en.wikipedia.org/wiki/Escrow

COLORED COINS

OPEN ASSETS PROTOCOL

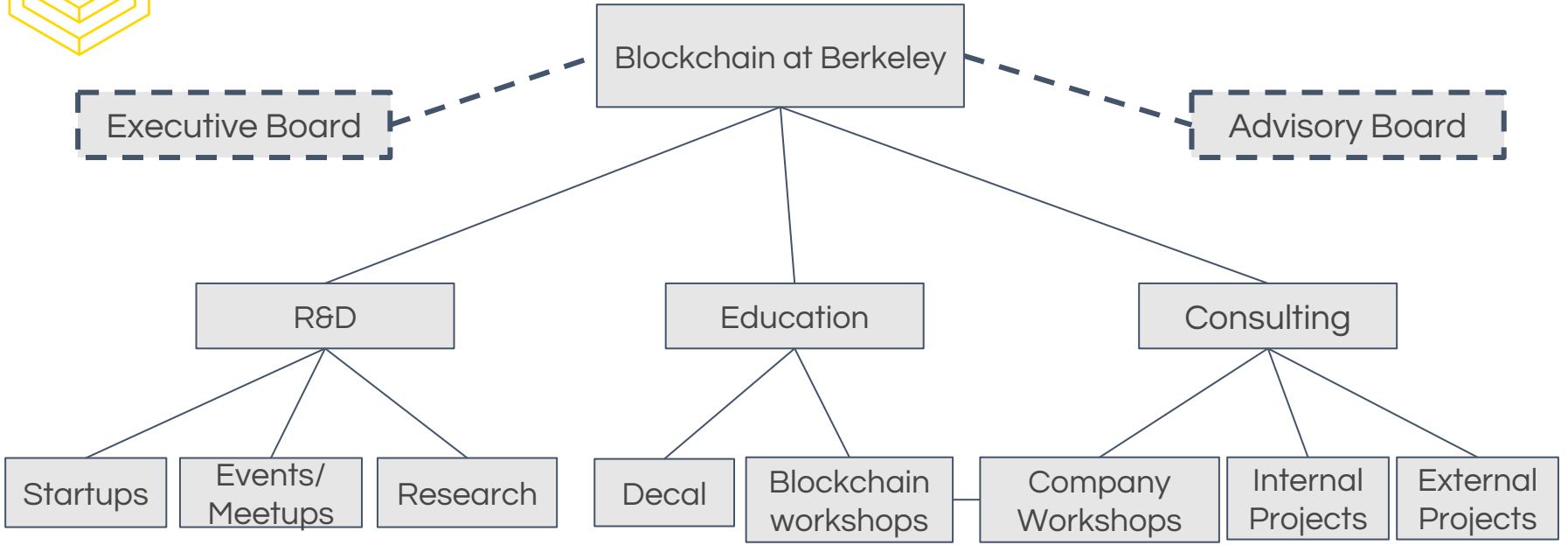
Nasdaq

$1BTC = $1USD



$1BTC = 10 APPL

5 Blockchain at Berkeley


Blockchain at Berkeley
Executive Board
Advisory Board
R&D
Education
Consulting
Startups
Events/ Meetups
Research
Decal
Blockchain workshops
Company Workshops
Internal Projects
External Projects

JOBS! JOBS! JOBS!

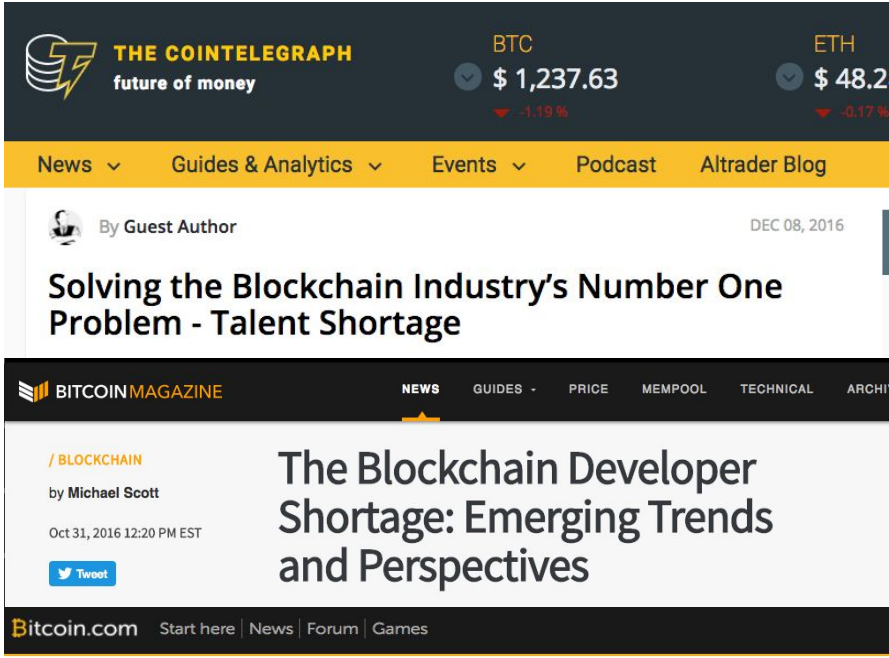
ExxonMobil

SAP Deloitte.

AIRBUS

adidas

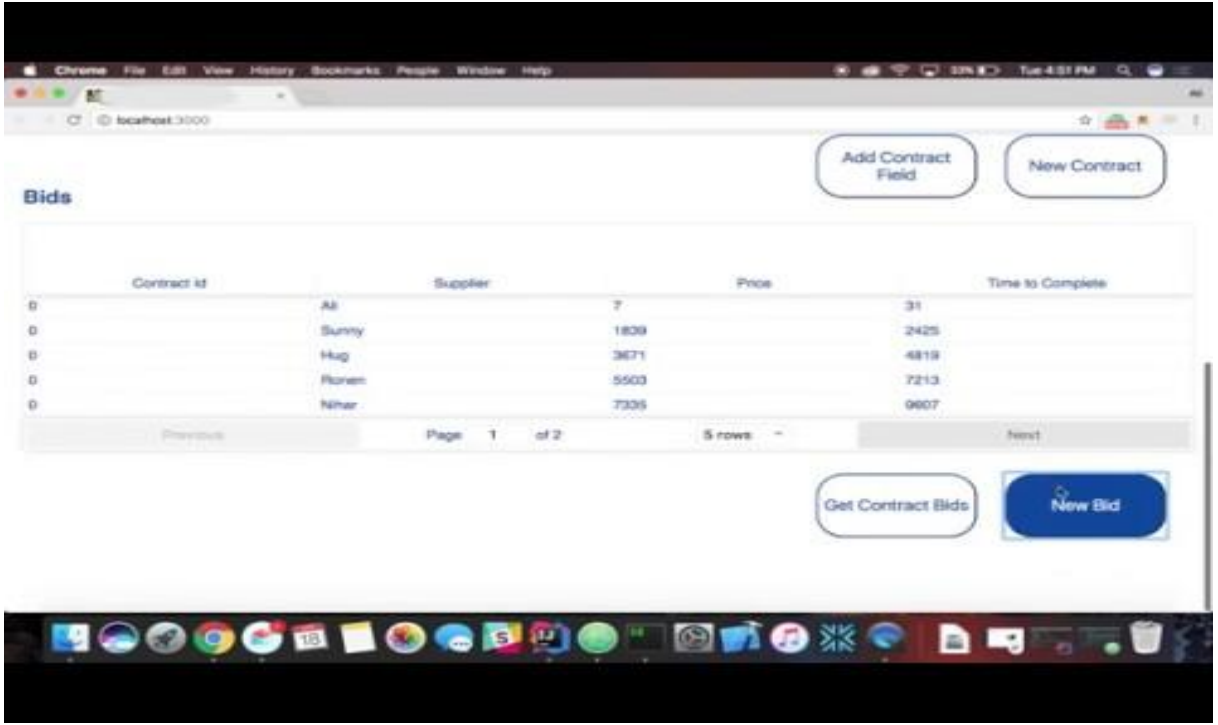
QUALCOMM



BLOCKCHAIN AT BERKELEY

AIRBUS

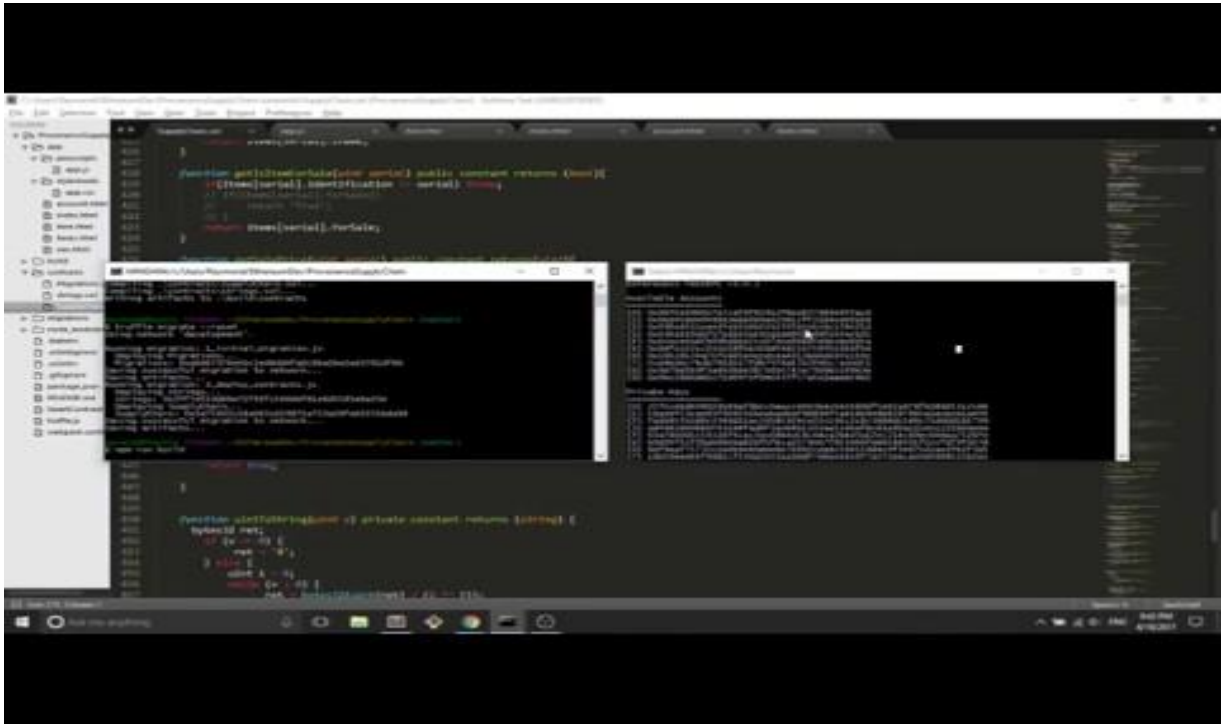
Decentralized Auction Bidding & Smart Contract Modularity



BLOCKCHAIN AT BERKELEY

PHARMACEUTICALS TRACEABILITY

Immutable Audit Trail for Traceability of Physical Goods



Get Your Bitcoin & Join B@B

Get Your Bitcoin

1. Download Bitcoin Wallet from: https://airbitz.co/bitcoin-wallet/
2. Press SCAN at the bottom of the screen
3. Scan QR code and press Import
4. You are a Bitcoin Owner now

Join Us & Stay Tuned for future applications

LIKE OUR PAGE
FB.com/BerkeleyBlockchain

SIGN UP FOR NEWSLEETER
https://Blockchain.Berkeley.Edu

SPONSORED BY airBitz

BLOCKCHAIN AT BERKELEY