

Intro to Blockchain DATA-X



Nadir Akhtar



BLOCKCHAIN
AT BERKELEY



AGENDA

INTRO TO BLOCKCHAIN

2

1



Why Should You Care?

2



Understanding Bitcoin and Consensus

3



Blockchain Types and Platforms

4



Use Cases and Application

5



Blockchain at Berkeley



BLOCKCHAIN
AT BERKELEY



1

WHY SHOULD YOU CARE?

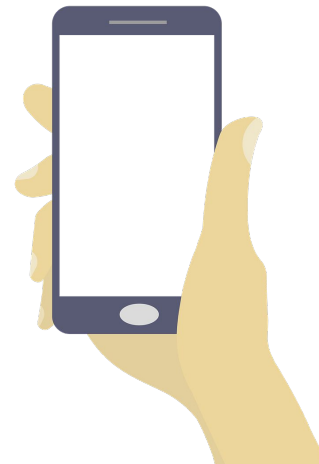




DIGITIZATION

MACRO TRENDS

4



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



BLOCKCHAIN
AT BERKELEY



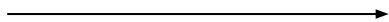
DECENTRALIZATION

MACRO TRENDS

5



UBER



airbnb

MARRIOTT



BLOCKCHAIN
AT BERKELEY



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



BLOCKCHAIN
AT BERKELEY



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

8

Volunteers?



BLOCKCHAIN
AT BERKELEY



2

BITCOIN AND CONSENSUS

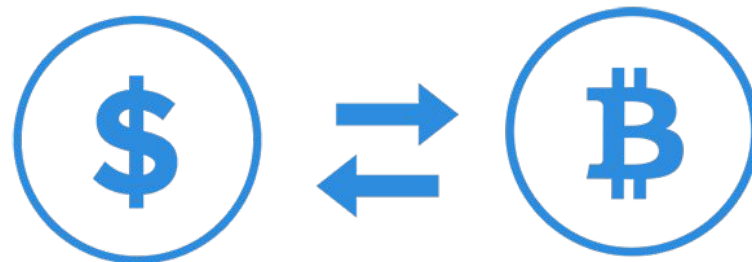




WHAT IS BITCOIN?

FIRST CRYPTOCURRENCY

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



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



BLOCKCHAIN
AT BERKELEY



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

Send Funds

Recipient



Email or bitcoin address

Amount

0.00

BTC ▾



My Wallet

0.8635703 BTC ↕

Note

Write an optional message

Send Funds



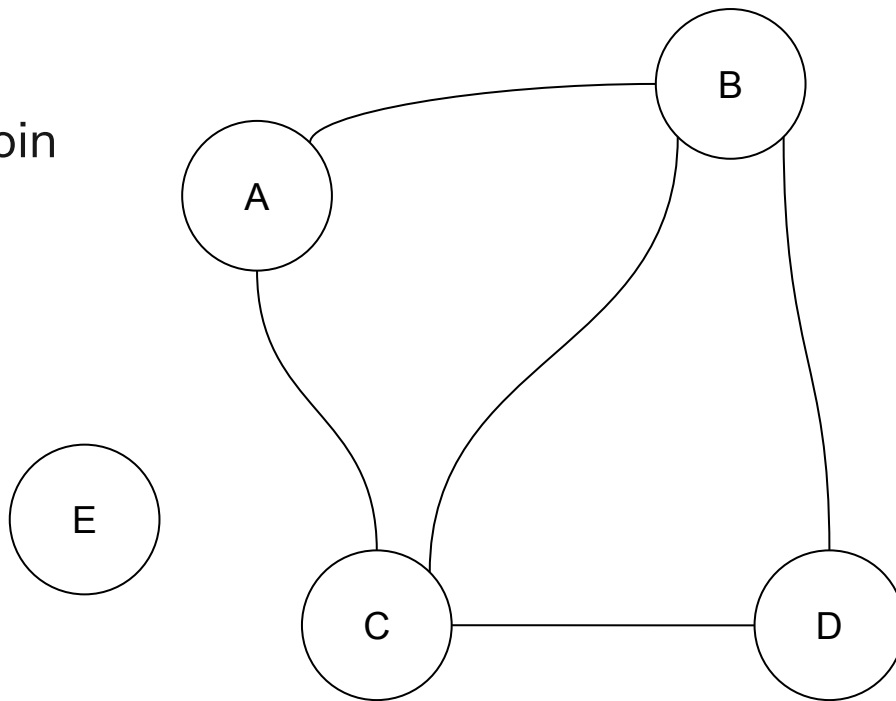


WHO REGULATES BITCOIN?

INTRO TO BLOCKCHAIN

No central authority; anyone can join

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



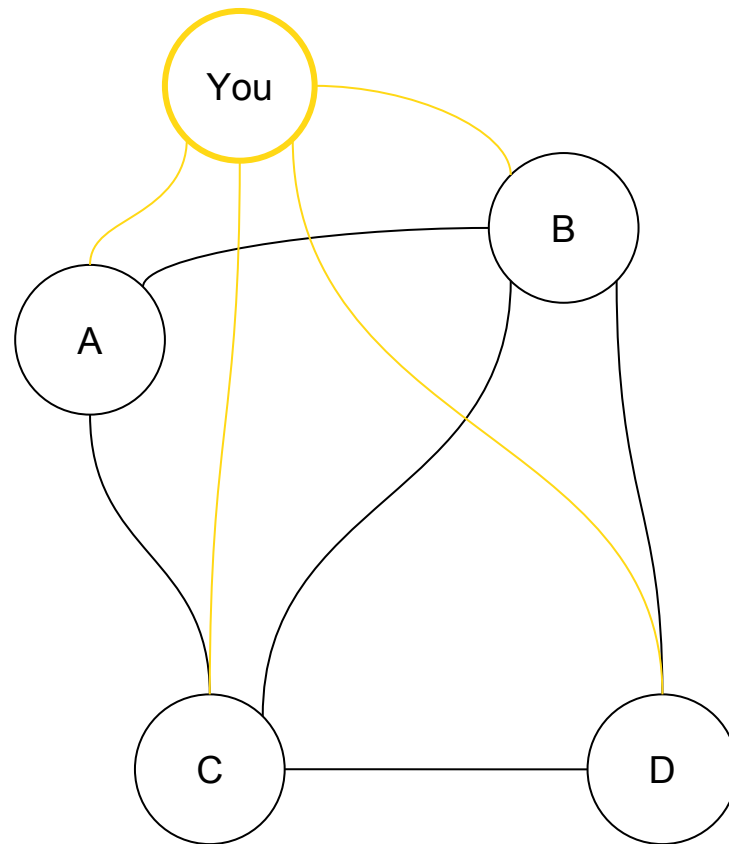


CAN I JOIN?

INTRO TO BLOCKCHAIN

Of course!

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



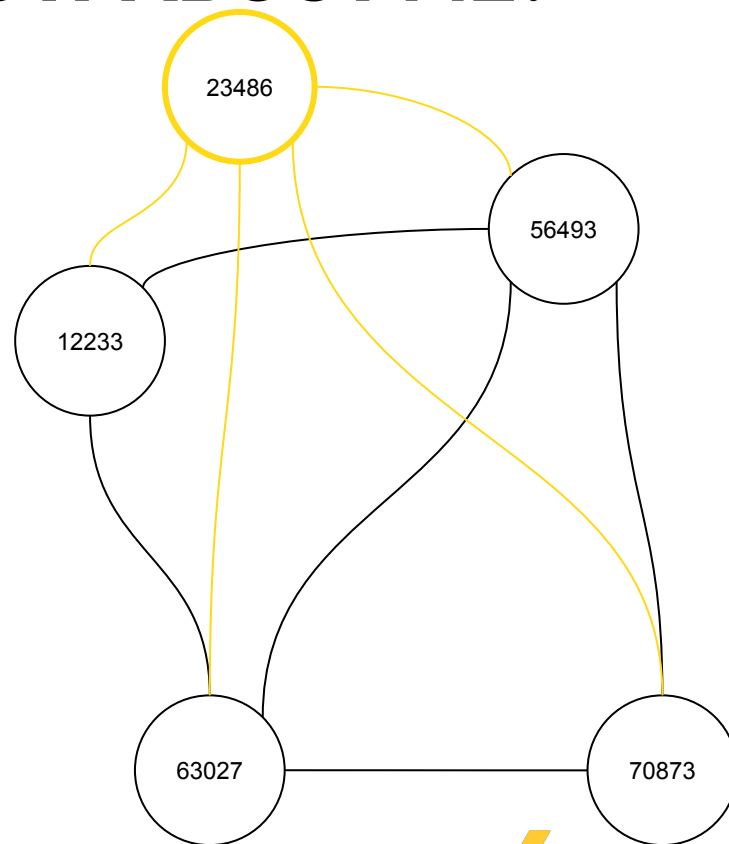


WHAT DO PEOPLE KNOW ABOUT ME?

EVERYONE'S A STRANGER

Not much....

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





3

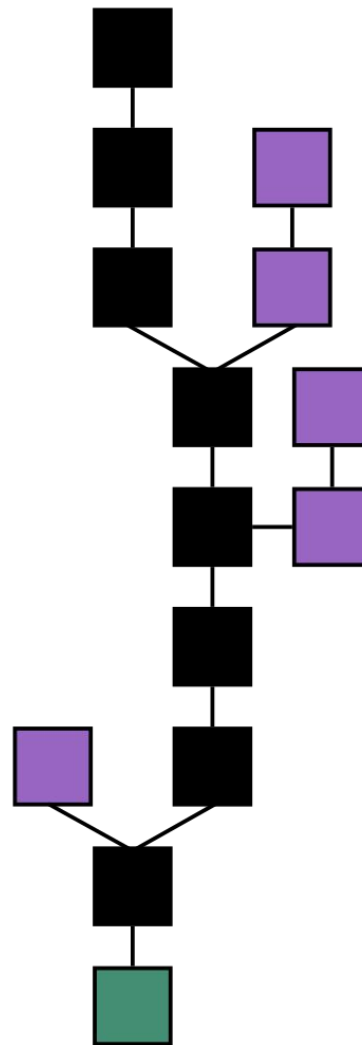
BLOCKCHAIN TYPES AND PLATFORMS



WHAT IS BLOCKCHAIN?

INTRO TO BLOCKCHAIN

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





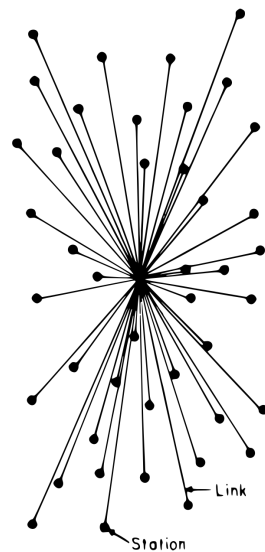
TYPES OF BLOCKCHAINS

INTRO TO BLOCKCHAIN

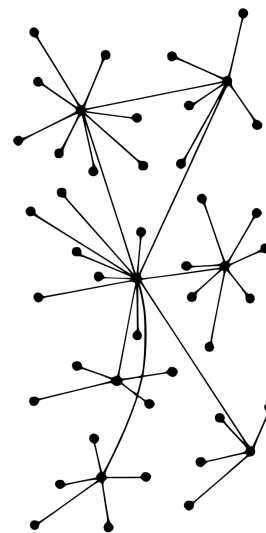
Fully Private Blockchain - write permissions are kept centralized to one organization.

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

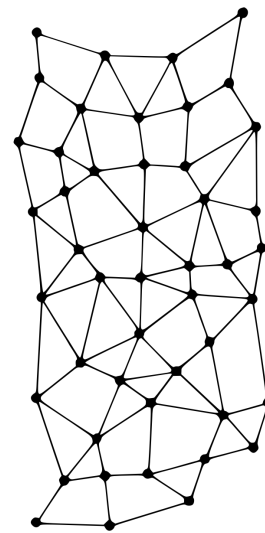
Public Blockchain - anyone in the world can participate in the consensus process.



CENTRALIZED
(A)



DECENTRALIZED
(B)



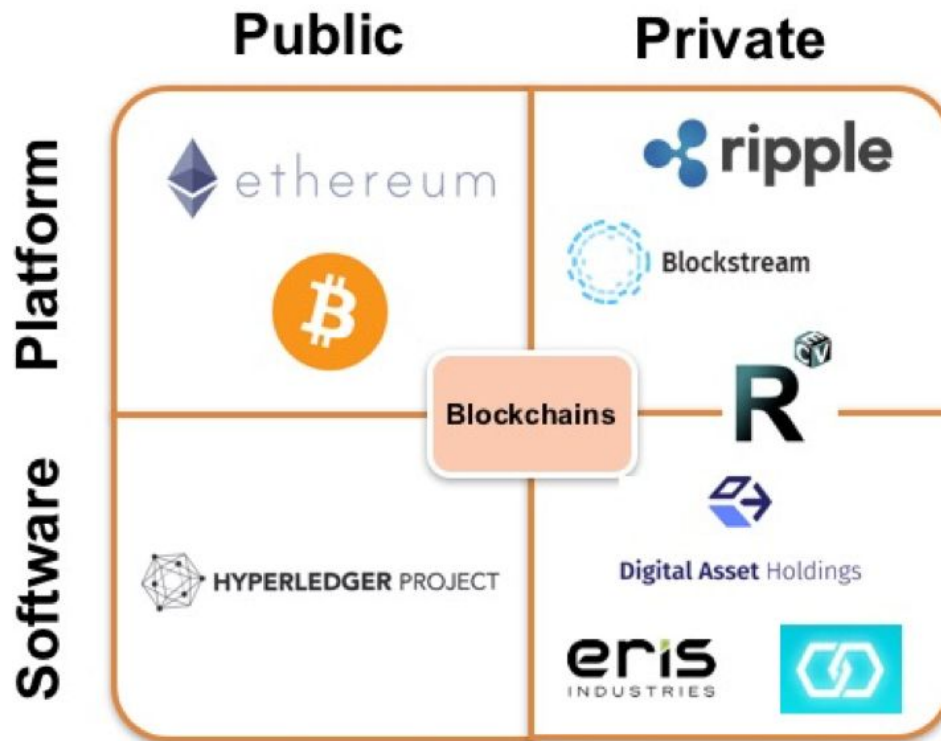
DISTRIBUTED
(C)

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





TYPES OF BLOCKCHAINS

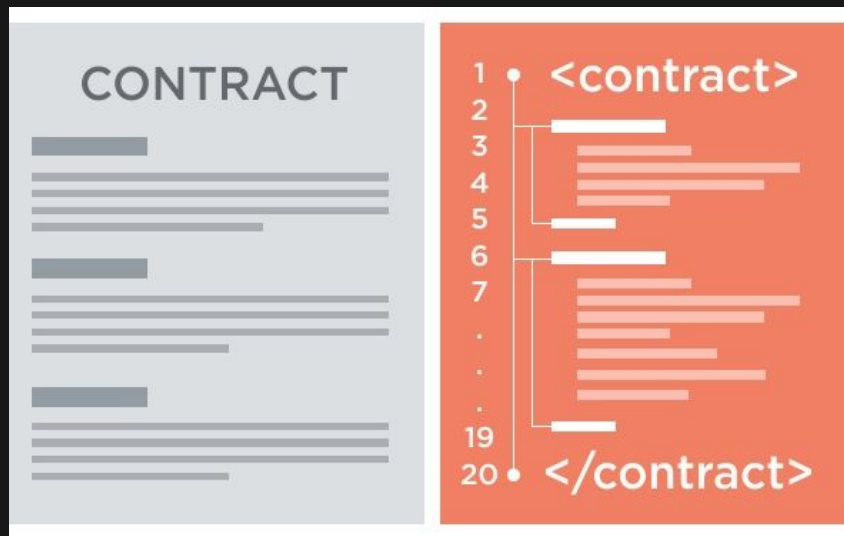




WHAT IS ETHEREUM?

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) / kən·trakt/

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

smart con·tract

(noun) /smärt kən·trakt/

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;
    }

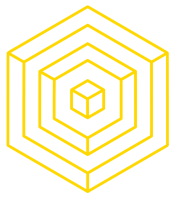
    /* Very simple trade function */
    function sendCoin(address receiver, uint amount) returns(bool sufficient) {
        if (coinBalanceOf[msg.sender] < amount) return false;
        coinBalanceOf[msg.sender] -= amount;
        coinBalanceOf[receiver] += amount;
        CoinTransfer(msg.sender, receiver,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

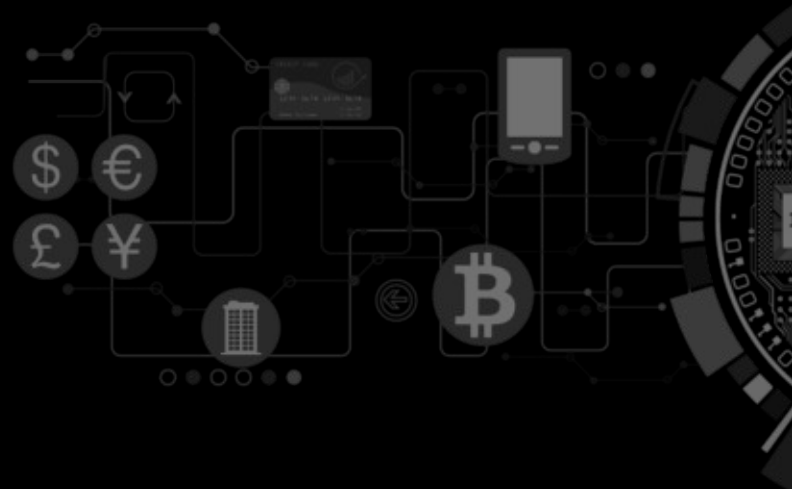
INVESTING REIMAGINED

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%)





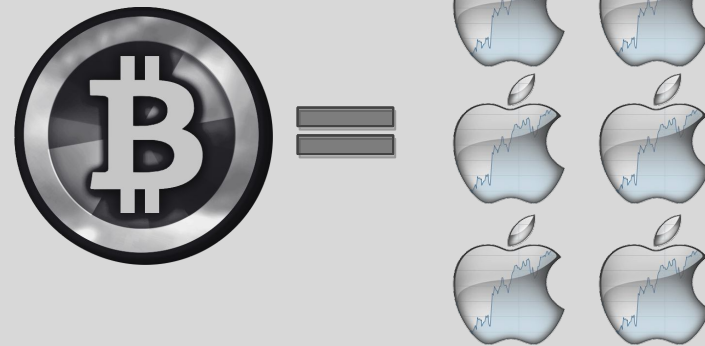
COLORED COINS

OPEN ASSETS PROTOCOL

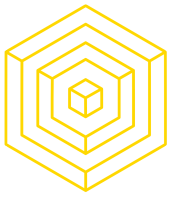
26



$\$1\text{BTC} = \1USD

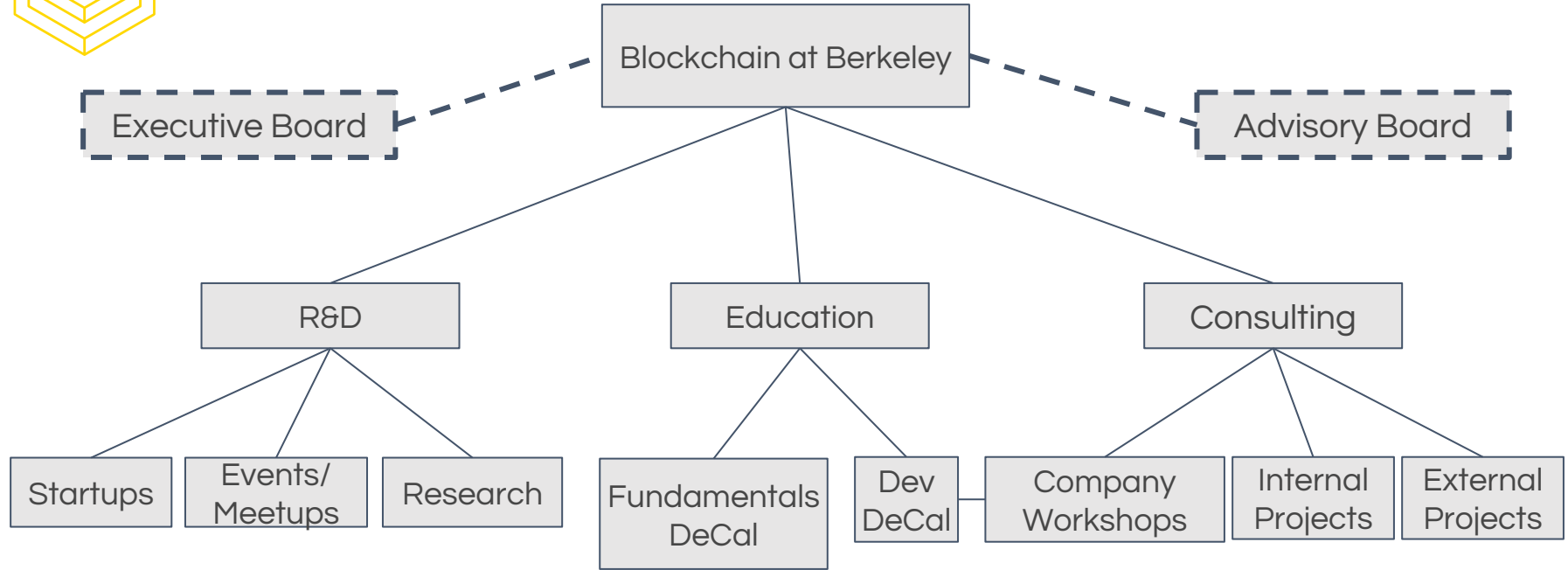


$\$1\text{BTC} = 10 \text{ APPL}$



5

BLOCKCHAIN AT BERKELEY





JOBS! JOBS! JOBS!

ExxonMobil




Deloitte.



QUALCOMM®



**THE COINTELEGRAPH**
future of money

BTC
\$ 1,237.63
▼ -1.19 %

ETH
\$ 48.2
▼ -0.17 %

News ▾ Guides & Analytics ▾ Events ▾ Podcast Altrader Blog



By Guest Author

DEC 08, 2016

Solving the Blockchain Industry's Number One Problem - Talent Shortage



BITCOIN MAGAZINE

NEWS

GUIDES ▾

PRICE

MEMPOOL

TECHNICAL

ARCHI

/ BLOCKCHAIN

by Michael Scott

Oct 31, 2016 12:20 PM EST



The Blockchain Developer Shortage: Emerging Trends and Perspectives

Bitcoin.com

Start here

News

Forum

Games

Home › Blockchain › Japan Risks Falling Behind Amid Blockchain Talent Shortage

BLOCKCHAIN

EMERGING MARKETS

NEWS

Japan Risks Falling Behind Amid Blockchain Talent Shortage



BLOCKCHAIN
AT BERKELEY



AIRBUS

30

Decentralized Auction Bidding & Smart Contract Modularity

Chrome File Edit View History Bookmarks People Window Help
localhost:3000

Add Contract Field New Contract

Bids

Contract id	Supplier	Price	Time to Complete
0	Ali	7	31
0	Sunny	1809	2425
0	Hug	3671	4819
0	Ronen	5503	7213
0	Nihar	7335	9607

Previous Page 1 of 2 5 rows: - Next

Get Contract Bids New Bid



BLOCKCHAIN
AT BERKELEY



PHARMACEUTICALS TRACEABILITY

Immutable Audit Trail for Traceability of Physical Goods

