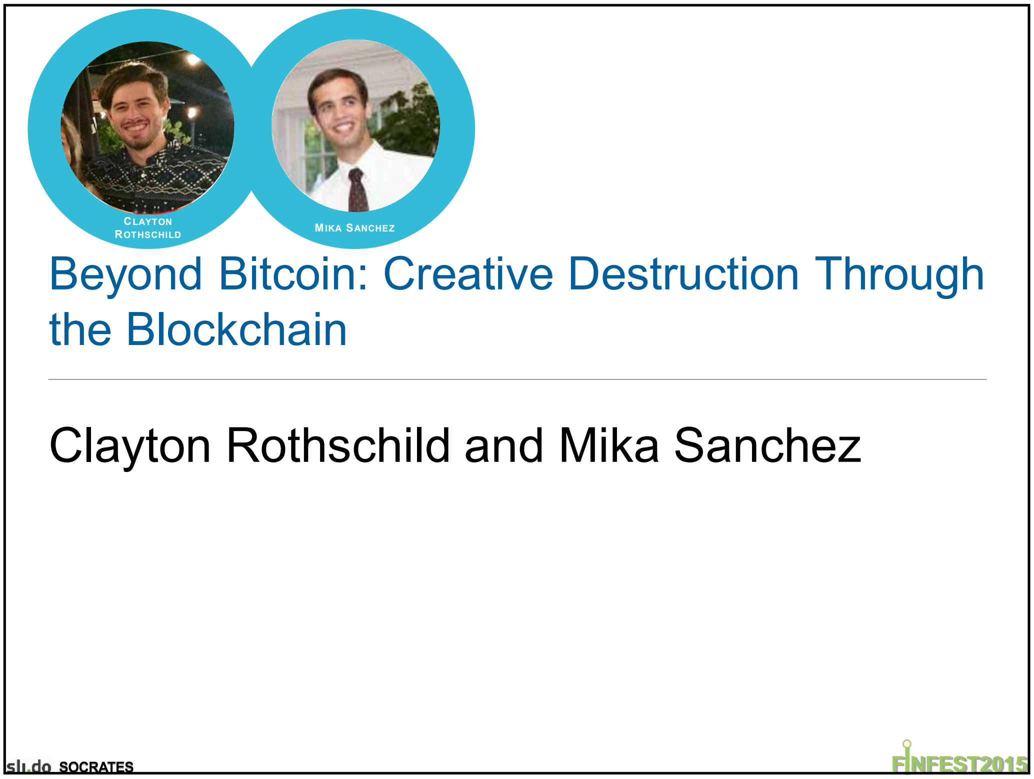


CLAYTON ROTHSCHILD

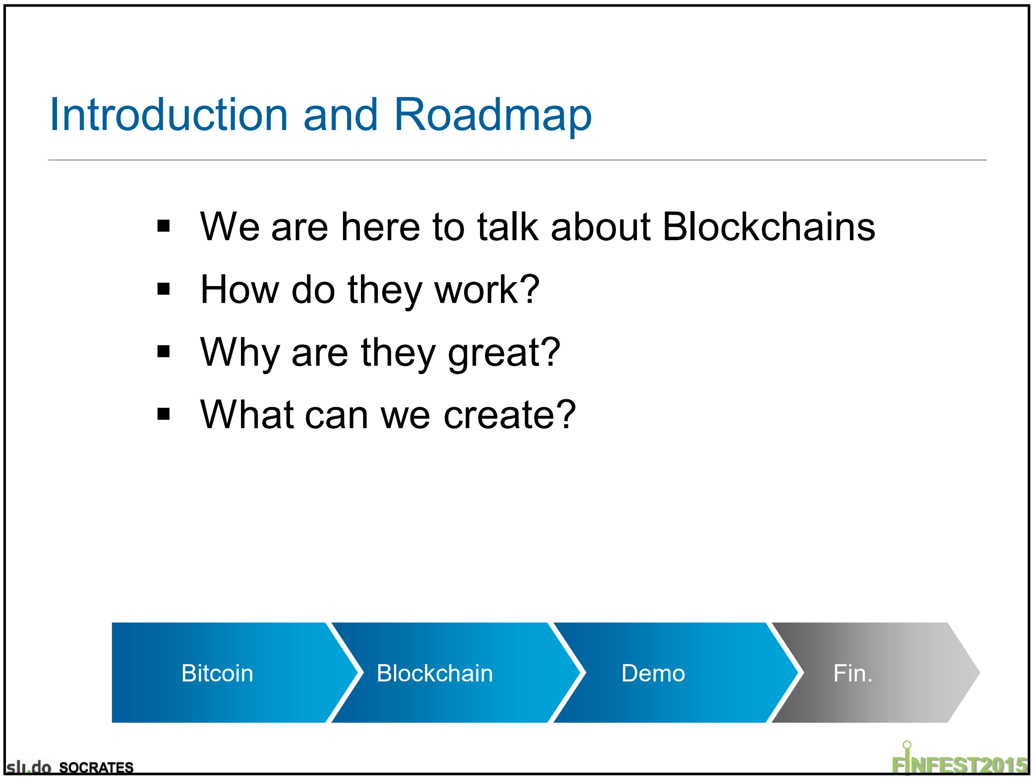
MIKA SANCHEZ

Beyond Bitcoin: Creative Destruction Through the Blockchain

Clayton Rothschild and Mika Sanchez

sli.do SOCRATES

FINFEST2015



Introduction and Roadmap

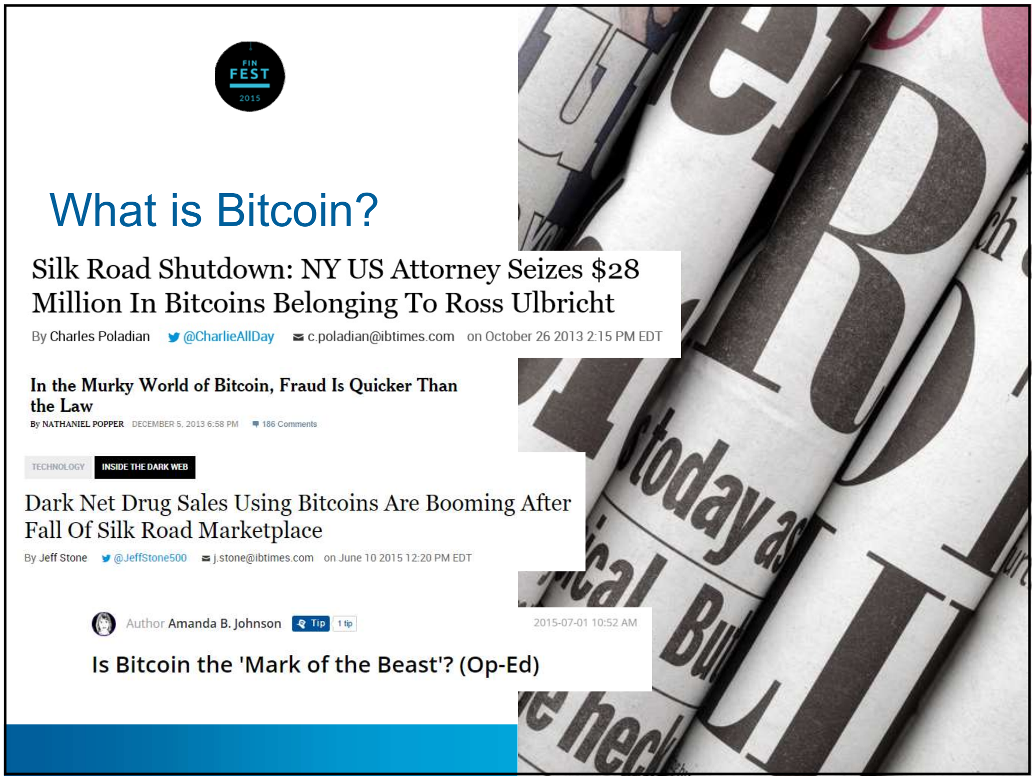
- We are here to talk about Blockchains
- How do they work?
- Why are they great?
- What can we create?

Bitcoin → Blockchain → Demo → Fin.

sli.do SOCRATES

FINFEST2015

Bitcoin



What is Bitcoin?

Silk Road Shutdown: NY US Attorney Seizes $28 Million In Bitcoins Belonging To Ross Ulbricht

By Charles Poladian @CharlieAllDay c.poladian@ibtimes.com on October 26 2013 2:15 PM EDT

In the Murky World of Bitcoin, Fraud Is Quicker Than the Law

By NATHANIEL POPPER DECEMBER 5, 2013 6:58 PM 186 Comments

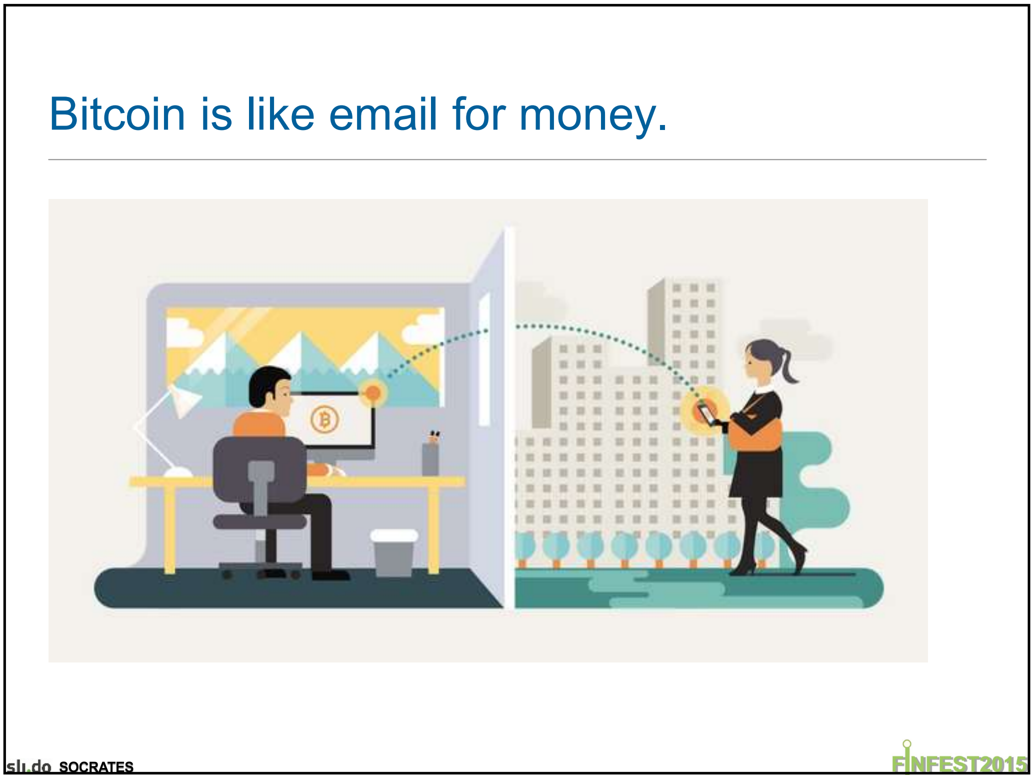
TECHNOLOGY INSIDE THE DARK WEB

Dark Net Drug Sales Using Bitcoins Are Booming After Fall Of Silk Road Marketplace

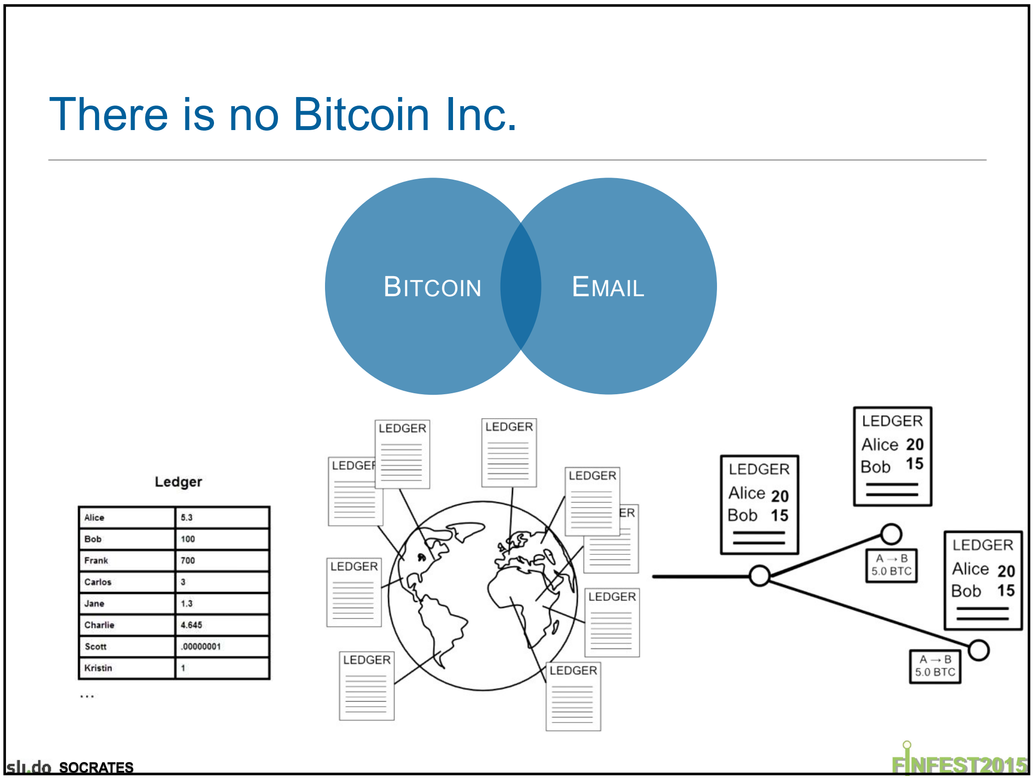
By Jeff Stone @JeffStone500 j.stone@ibtimes.com on June 10 2015 12:20 PM EDT

Author Amanda B. Johnson Tip 1 tip 2015-07-01 10:52 AM

Is Bitcoin the 'Mark of the Beast'? (Op-Ed)



Bitcoin is like email for money.



There is no Bitcoin Inc.

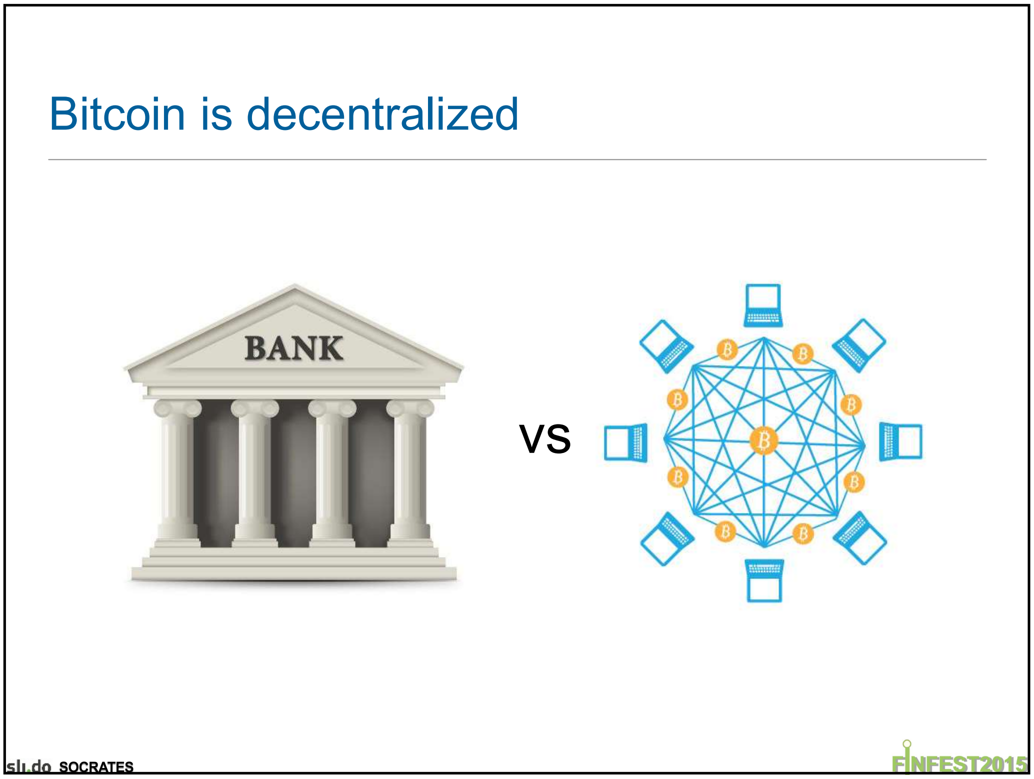
Ledger

Alice	5.3
Bob	100
Frank	700
Carlos	3
Jane	1.3
Charlie	4.645
Scott	.00000001
Kristin	1

…

sli.do SOCRATES

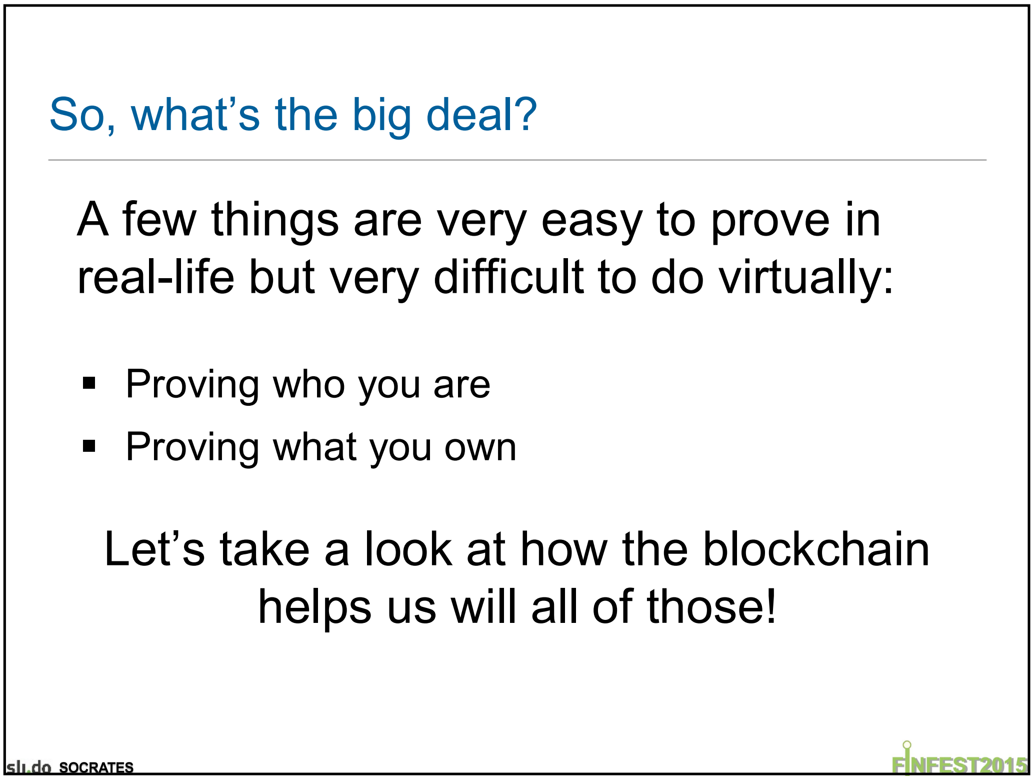
FINFEST2015



Bitcoin is decentralized

sli.do SOCRATES

FINFEST2015



So, what's the big deal?

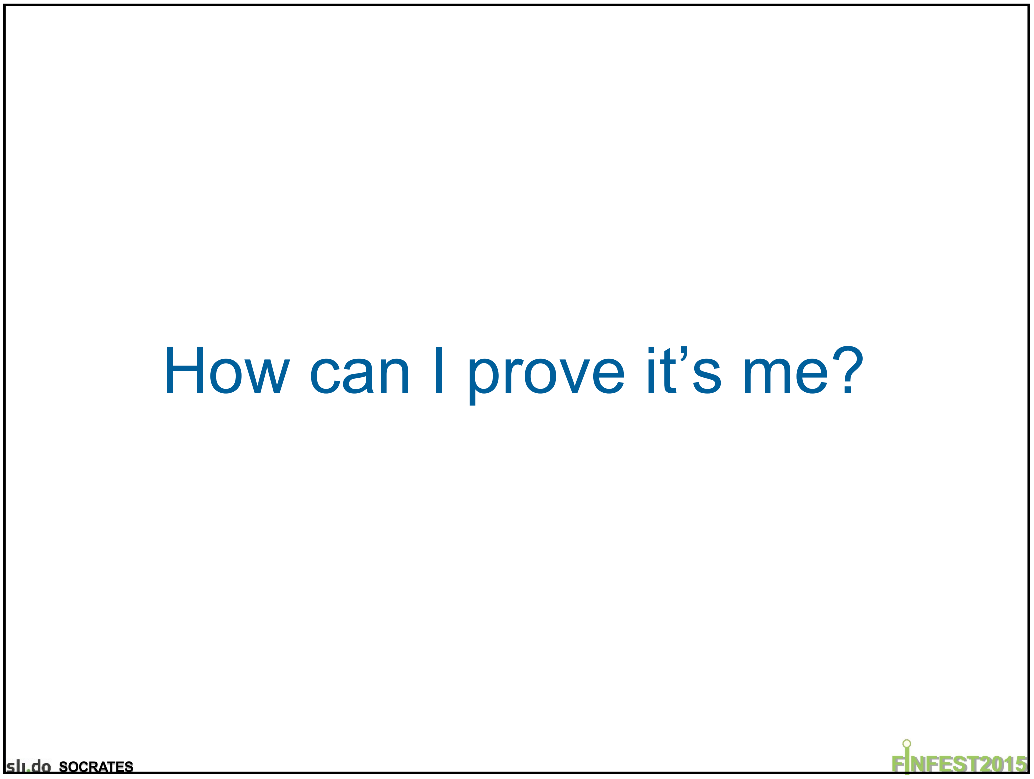
A few things are very easy to prove in real-life but very difficult to do virtually:

- Proving who you are
- Proving what you own

Let's take a look at how the blockchain helps us will all of those!

sli.do SOCRATES

FINFEST2015

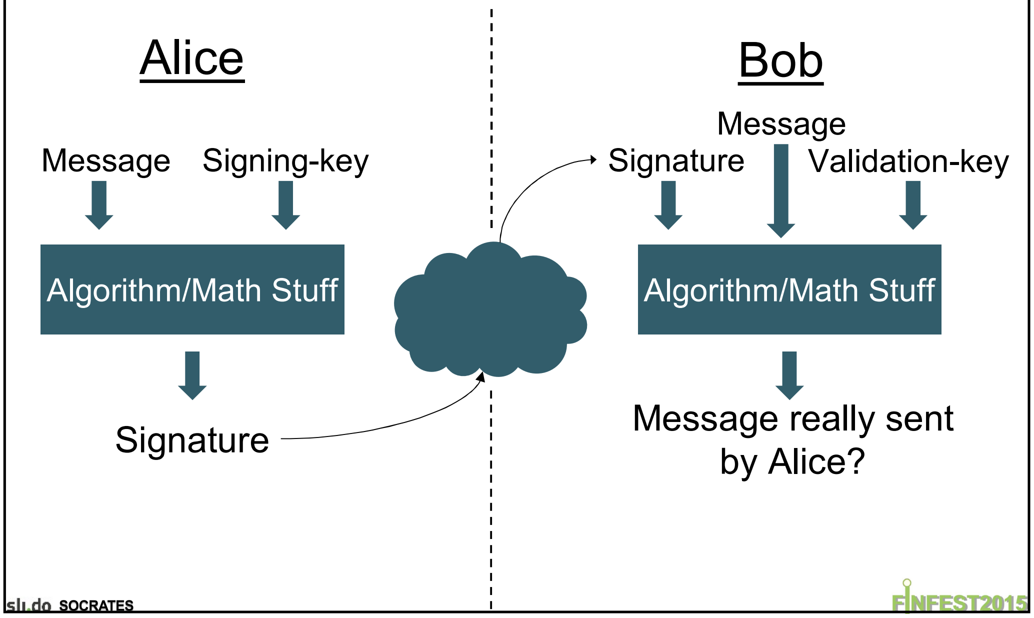


How can I prove it's me?

sli.do SOCRATES

FINFEST2015

Digital Signatures Provide Proof of Identity

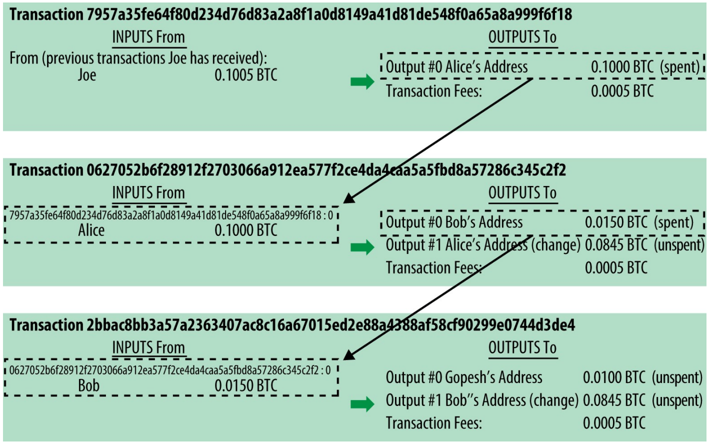


How can I prove I *have* something?

What is *a* Bitcoin?

Transactions are the real base unit of the Blockchain

Transactions are made out of prior transactions



Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18

INPUTS From

From (previous transactions Joe has received):
Joe 0.1005 BTC

OUTPUTS To

Output #0 Alice's Address 0.1000 BTC (spent)
Transaction Fees: 0.0005 BTC

Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

INPUTS From

7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0
Alice 0.1000 BTC

OUTPUTS To

Output #0 Bob's Address 0.0150 BTC (spent)
Output #1 Alice's Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC

Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4

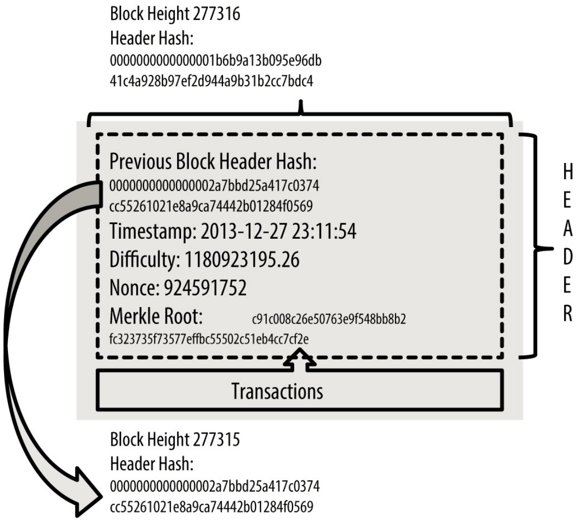
INPUTS From

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0
Bob 0.0150 BTC

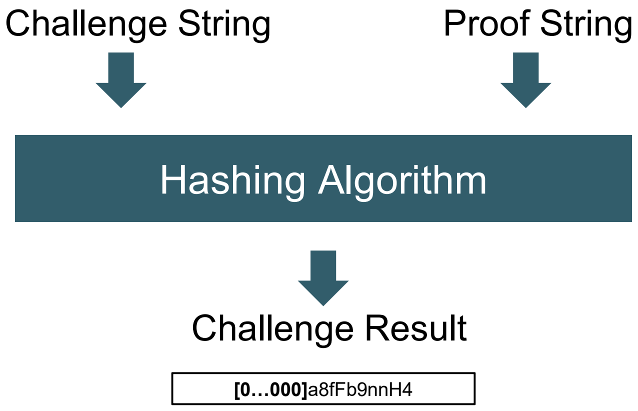
OUTPUTS To

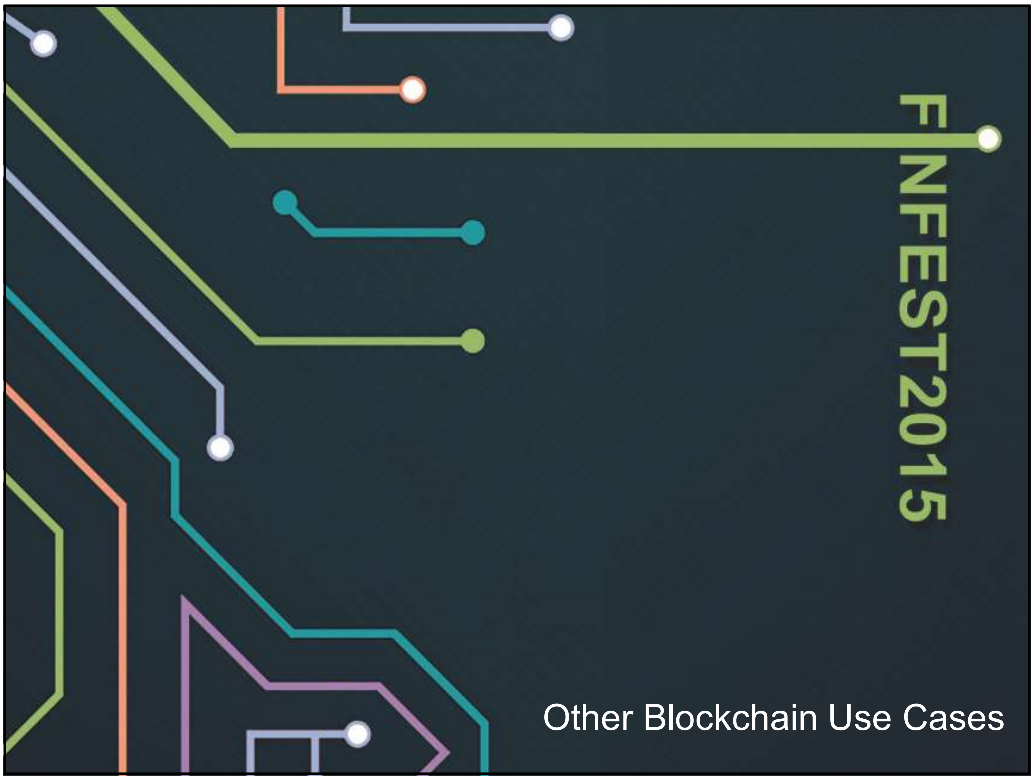
Output #0 Gopesh's Address 0.0100 BTC (unspent)
Output #1 Bob''s Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC

A Block Decomposed

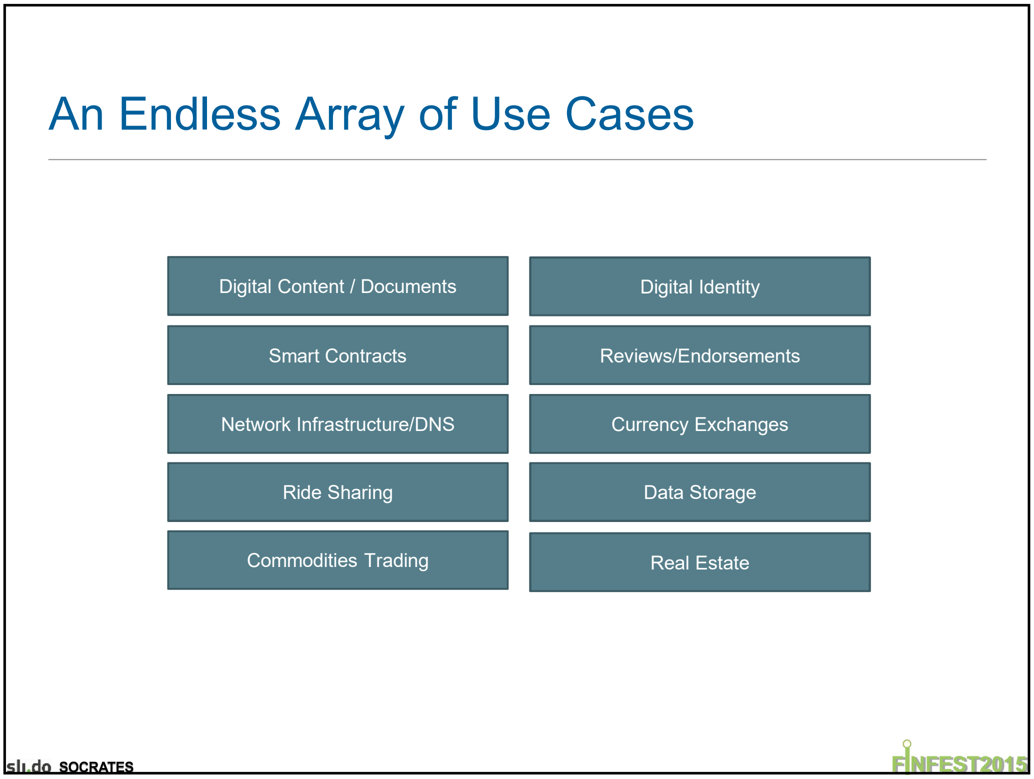

Block Height 277316
Header Hash:
0000000000000001b6b9a13b095e96db
41c4a928b97ef2d944a9b31b2cc7bdc4
Previous Block Header Hash:
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569
Timestamp: 2013-12-27 23:11:54
Difficulty: 1180923195.26
Nonce: 924591752
Merkle Root: c91c008c26e50763e9f548bb8b2
fc323735f73577effbc55502c51eb4cc7cf2e
Transactions
HEADER
Block Height 277315
Header Hash:
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569

Proof of Work





Other Blockchain Use Cases

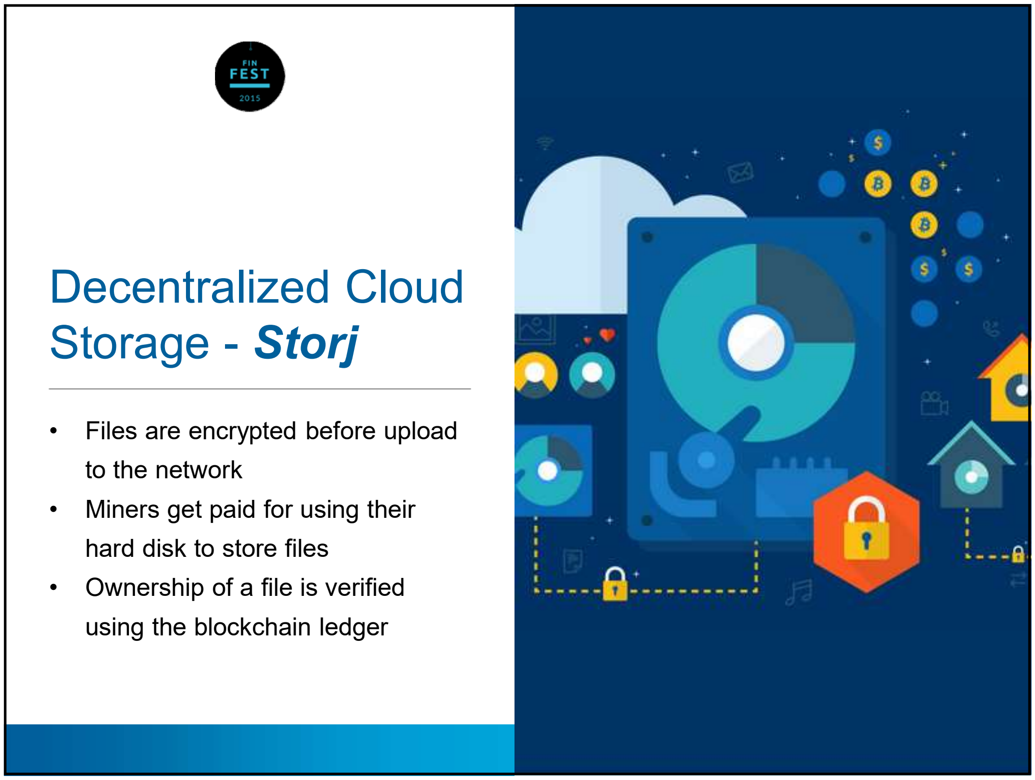


An Endless Array of Use Cases

Digital Content / Documents	Digital Identity
Smart Contracts	Reviews/Endorsements
Network Infrastructure/DNS	Currency Exchanges
Ride Sharing	Data Storage
Commodities Trading	Real Estate

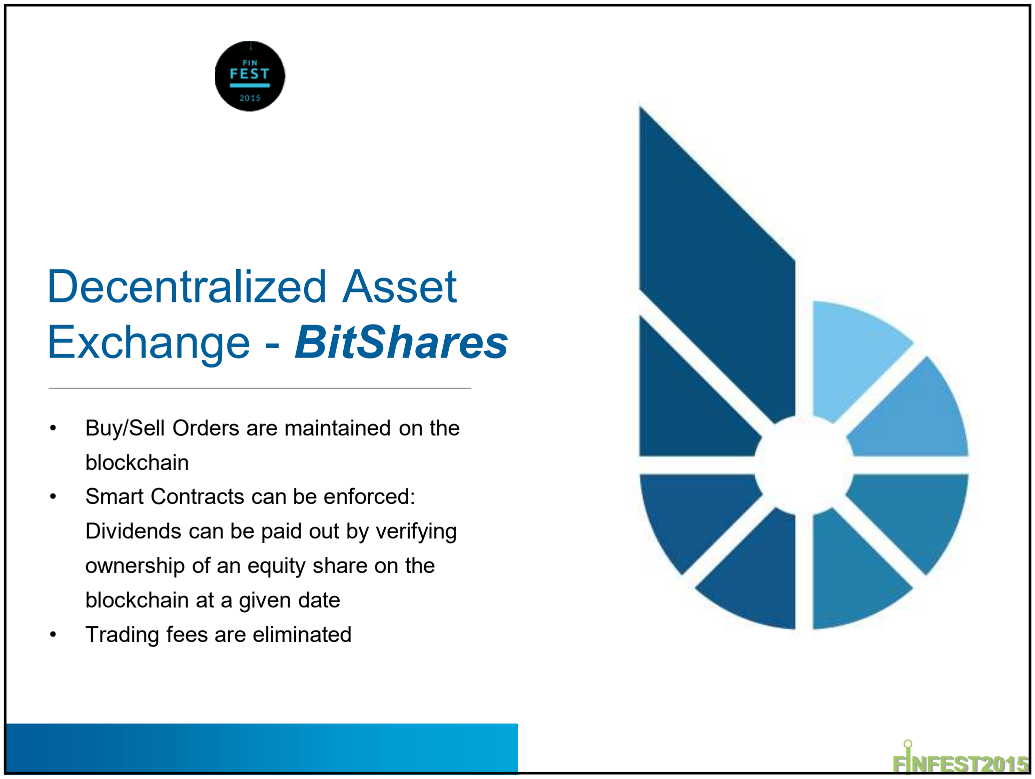
sli.do SOCRATES

FINFEST2015



Decentralized Cloud Storage - ***Storj***

- Files are encrypted before upload to the network
- Miners get paid for using their hard disk to store files
- Ownership of a file is verified using the blockchain ledger



Decentralized Asset Exchange - ***BitShares***

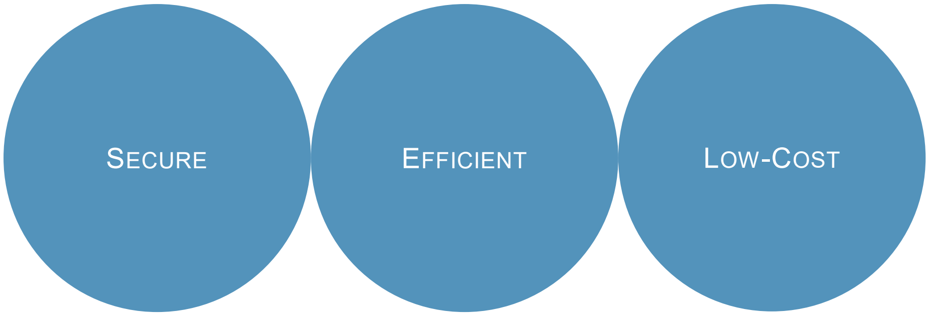
- Buy/Sell Orders are maintained on the blockchain
- Smart Contracts can be enforced: Dividends can be paid out by verifying ownership of an equity share on the blockchain at a given date
- Trading fees are eliminated

Demonstration

Our Company

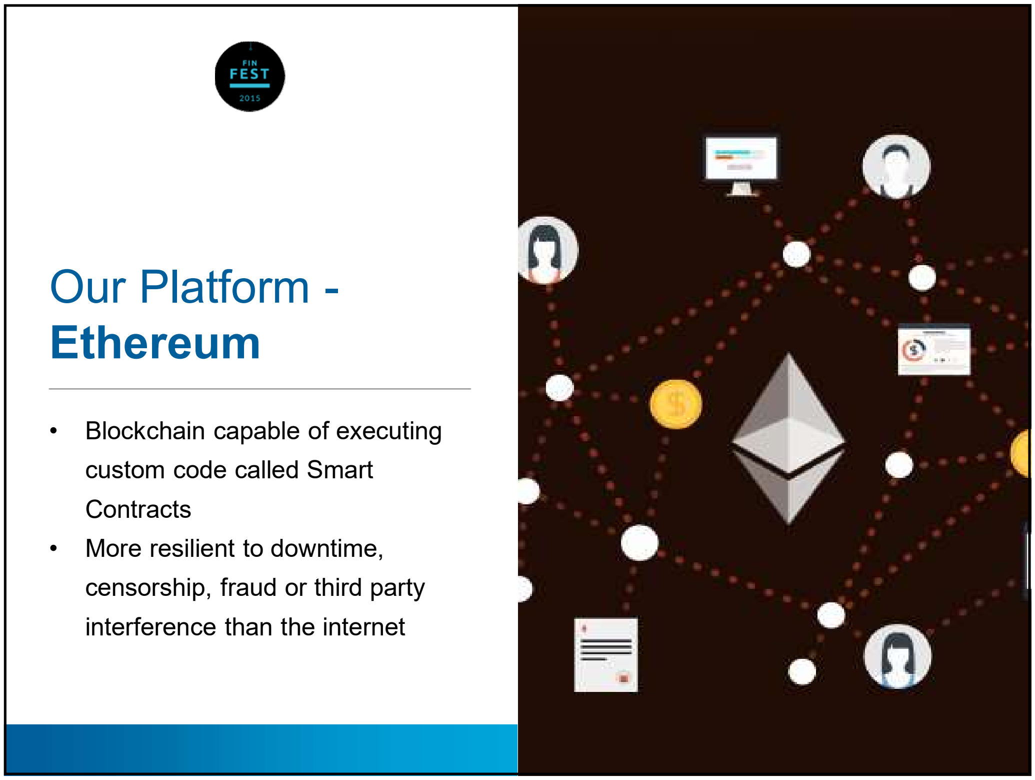
FinFest Vote 2.0

- A Distributed, Trustless, and Efficient voting platform on the blockchain



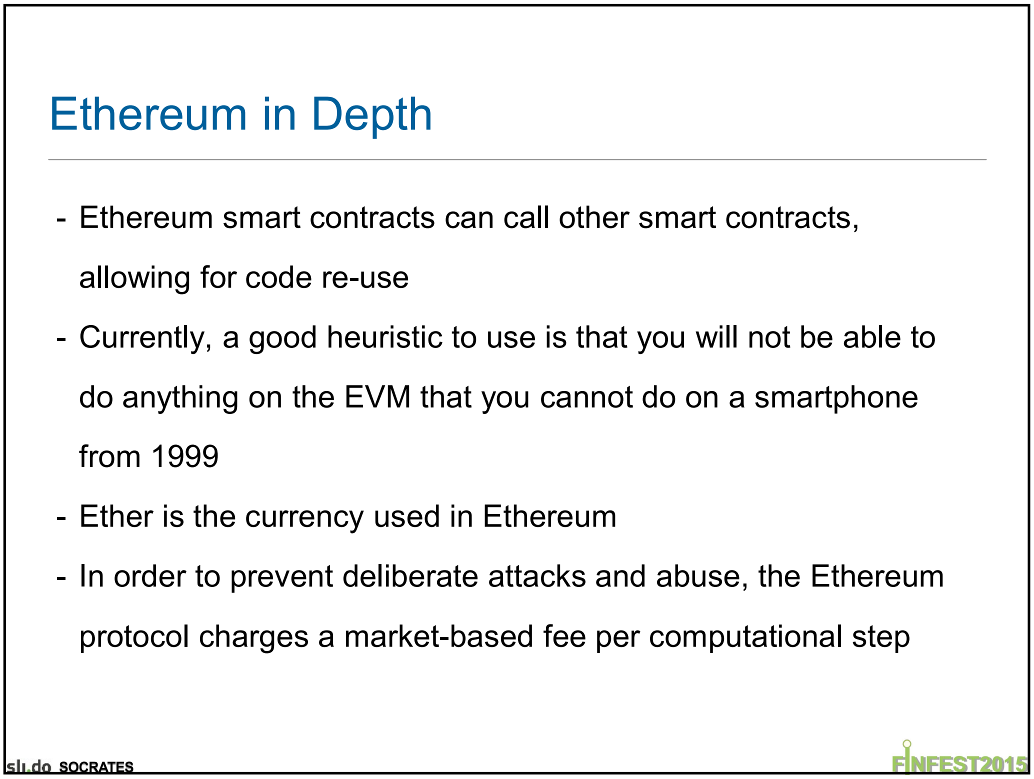
sli.do SOCRATES

FINFEST2015



Our Platform - **Ethereum**

- Blockchain capable of executing custom code called Smart Contracts
- More resilient to downtime, censorship, fraud or third party interference than the internet



Ethereum in Depth

- Ethereum smart contracts can call other smart contracts, allowing for code re-use
- Currently, a good heuristic to use is that you will not be able to do anything on the EVM that you cannot do on a smartphone from 1999
- Ether is the currency used in Ethereum
- In order to prevent deliberate attacks and abuse, the Ethereum protocol charges a market-based fee per computational step

sli.do SOCRATES FINFEST2015

Ethereum in Depth contd.

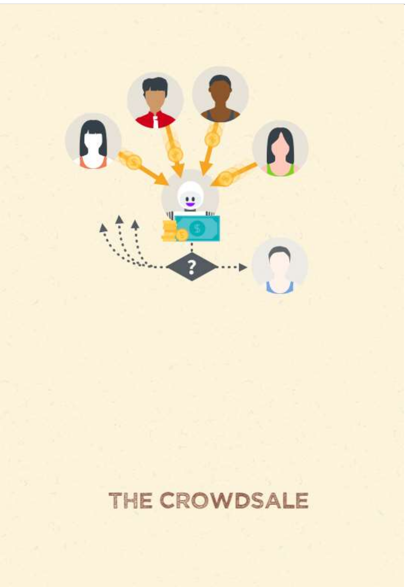
- The blockchain is one globally distributed VM
- It has its own machine code that it uses
- Multiple Programming Languages exist for it
- The programming language we used was Solidity
- Solidity code is compiled and then deployed

Solidity in Depth

- Syntactically a mix between C++ and JavaScript
- Two types of variables state and local, state variables are stored permanently in the blockchain
- Statically typed and has value types and reference types
- Libraries can also be deployed to the blockchain and be used for importing code into a contract
- Contracts can inherit from other contracts
- Contracts can publish events

Startups on the Ethereum Blockchain

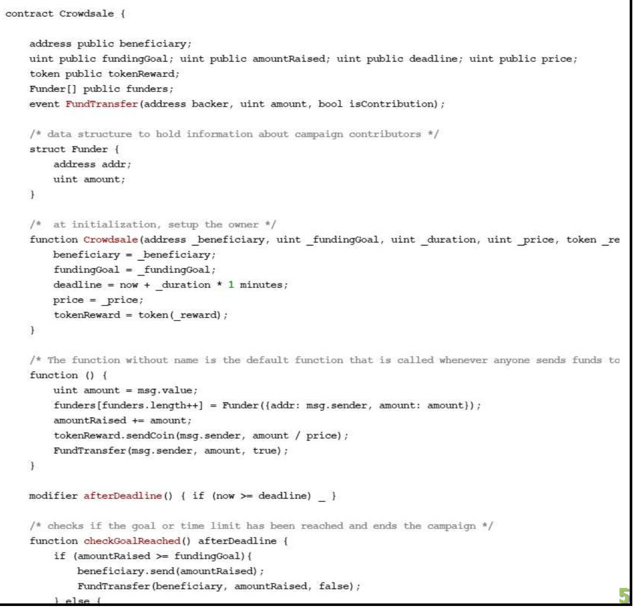
1. Lets kickstart our project with a crowdsale!
2. We will use Ethereum to create a contract that will hold people’s money until our funding goal is reached.
3. Depending on the outcome, the funds will either be released to us, or returned.
4. All without requiring a centralized arbitrator, clearing house, or needing to trust anyone.



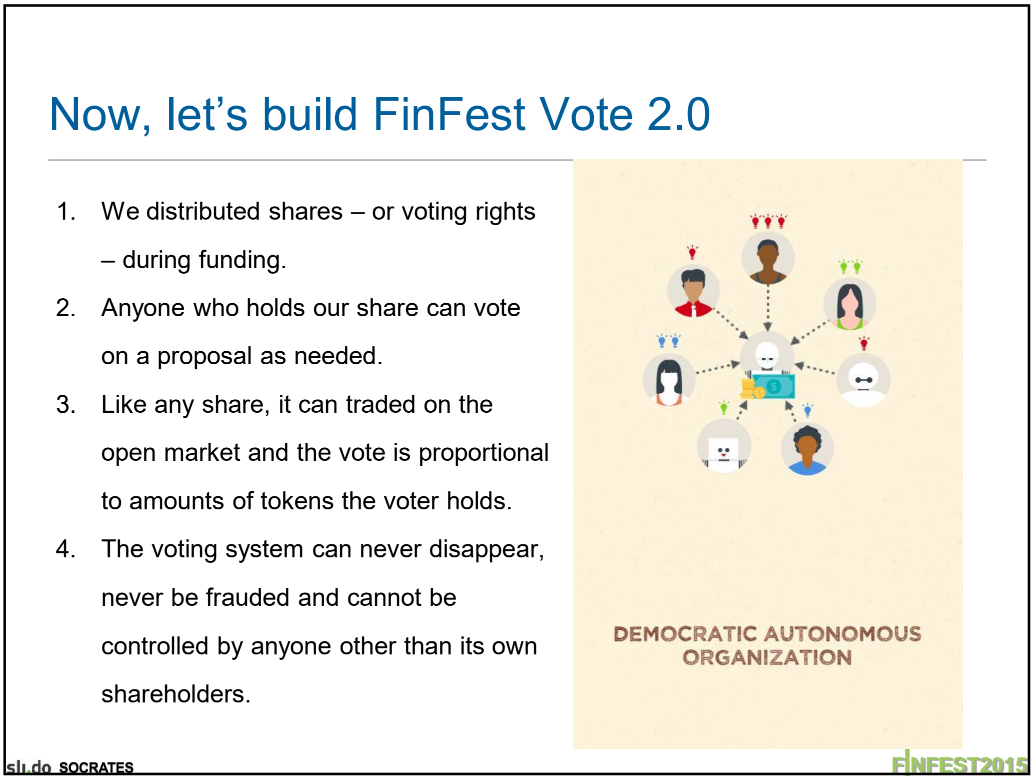
Funding in depth

Parameters:
- Funding Goal
- Deadline
- Beneficiary
- Exchange Rate of equity to Ether

… We got funded!
Now lets use the blockchain to build our application



```
contract Crowdsale {

    address public beneficiary;
    uint public fundingGoal; uint public amountRaised; uint public deadline; uint public price;
    token public tokenReward;
    Funder[] public funders;
    event FundTransfer(address backer, uint amount, bool isContribution);

    /* data structure to hold information about campaign contributors */
    struct Funder {
        address addr;
        uint amount;
    }

    /*  at initialization, setup the owner */
    function Crowdsale(address _beneficiary, uint _fundingGoal, uint _duration, uint _price, token _re
        beneficiary = _beneficiary;
        fundingGoal = _fundingGoal;
        deadline = now + _duration * 1 minutes;
        price = _price;
        tokenReward = token(_reward);
    }

    /* The function without name is the default function that is called whenever anyone sends funds to
    function () {
        uint amount = msg.value;
        funders[funders.length++] = Funder({addr: msg.sender, amount: amount});
        amountRaised += amount;
        tokenReward.sendCoin(msg.sender, amount / price);
        FundTransfer(msg.sender, amount, true);
    }

    modifier afterDeadline() { if (now >= deadline) _ }

    /* checks if the goal or time limit has been reached and ends the campaign */
    function checkGoalReached() afterDeadline {
        if (amountRaised >= fundingGoal){
            beneficiary.send(amountRaised);
            FundTransfer(beneficiary, amountRaised, false);
        } else {
```



Now, let's build FinFest Vote 2.0

1. We distributed shares – or voting rights – during funding.
2. Anyone who holds our share can vote on a proposal as needed.
3. Like any share, it can traded on the open market and the vote is proportional to amounts of tokens the voter holds.
4. The voting system can never disappear, never be frauded and cannot be controlled by anyone other than its own shareholders.

sli.do SOCRATES

FINFEST2015

Lessons Learned

Lessons Learned/Summary

1. The blockchain is useful for creating an application that implements smart contracts: software programs the operate as intended, without censorship, fraud, or intervention.

2. This creates efficiencies in the marketplace, and can replace any entity that operates as an intermediary or ledger system – payment networks, stock exchanges, titles and contract enforcement, DNS.

3. The technology is not in its primetime yet, but it is easy to see how a number of applications may run on the blockchain due to the immense security and low overhead of the applications. It is how the Internet was supposed to work: no possibility of downtime, censorship, fraud or third party interference.

4. Our voting system is transparent, low-cost, incorruptible, and uncensorable.

Thank you.

LinkedIn: Mika Sanchez

Twitter: @ClayRothschild

LinkedIn: ClaytonRothschild

Slack: #BeyondBitcoin

FINFEST2015