Pantas and Ting
Sutardja Center
for Entrepreneurship & Technology
Berkeley Engineering

Blockchain: Beyond Bitcoin

Authors: Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman

This work was created in an open classroom environment as part of a program within the Sutardja Center for Entrepreneurship & Technology and led by Prof. Ikhlaq Sidhu at UC Berkeley. There should be no proprietary information contained in this work. No information contained in this work is intended to affect or influence public relations with any firm affiliated with any of the authors. The views represented are those of the authors alone.

Berkeley
UNIVERSITY OF CALIFORNIA

Sutardja Center for Entrepreneurship & Technology

BREAKTHROUGH

25 years ago a ***breakthrough technology*** that ***connected people***

Connected people around the world, foundation for modern growth

Today the internet gives a new **breakthrough - BLOCKCHAIN**

Changes the way economy & businesses work
Trust without third parties - end of corruption.
Create institutions like never before.

Blockchain technology to **stem government corruption, fight crime and save lives!**

Nasdaq acquires SecondMarket to leverage blockchain technology for **pre-IPO trading**

Overstock to **re-invent public stock** market using blockchain technology

Bank of America, Citi, Goldman, JPM, HSBC + more banks join to form blockchain partnership

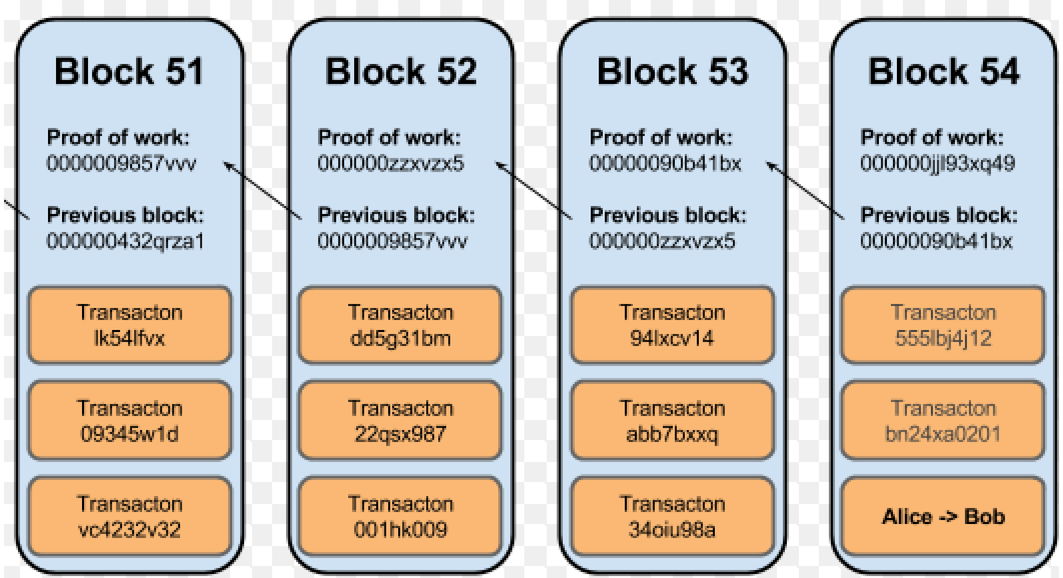
Blockchain considered as a **replacement for ASX clearing & settlement system**

Counterfeit drugs, Academic certificate, High value goods, and more...

What is Blockchain

Decentralized & distributed **public ledger** of transactions

or some people call it



Block 51
Proof of work: 0000009857vvv
Previous block: 000000432qrza1
Transacton lk54lfvx
Transacton 09345w1d
Transacton vc4232v32

Block 52
Proof of work: 000000zzxvzx5
Previous block: 0000009857vvv
Transacton dd5g31bm
Transacton 22qsx987
Transacton 001hk009

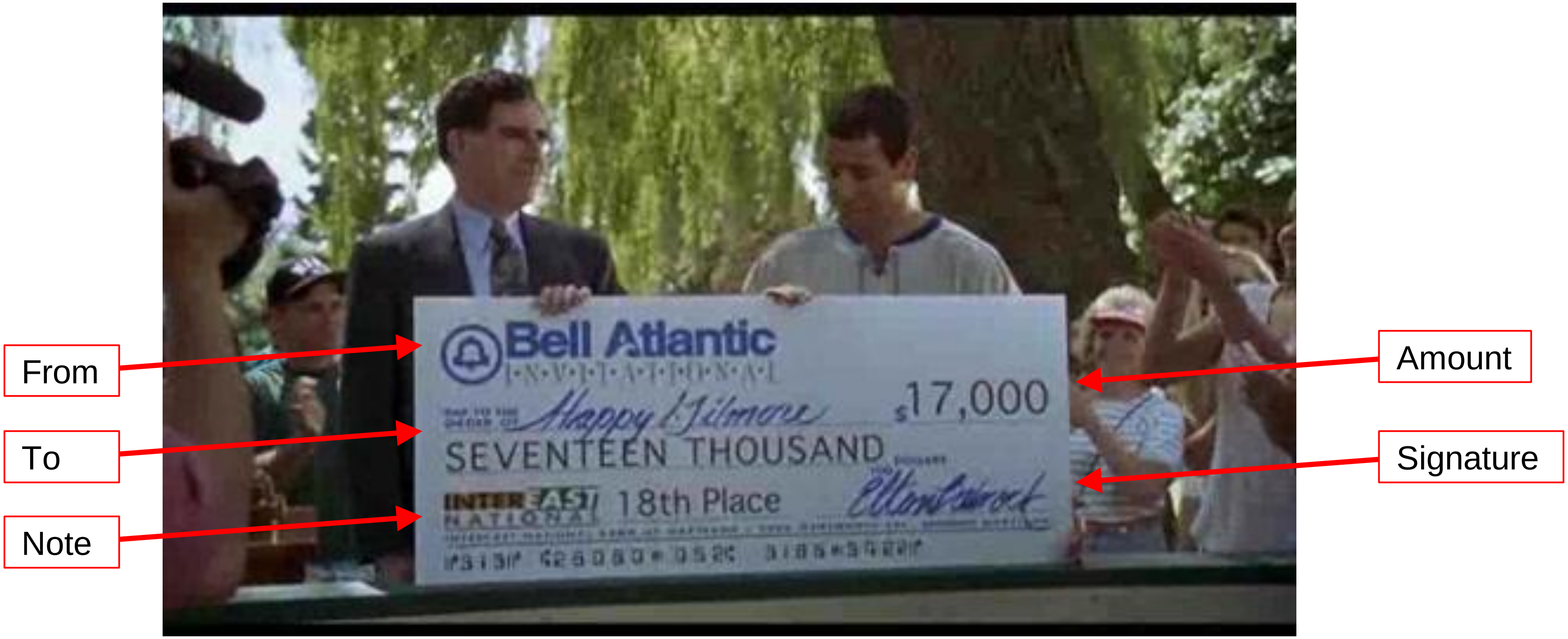
Block 53
Proof of work: 00000090b41bx
Previous block: 000000zzxvzx5
Transacton 94lxcv14
Transacton abb7bxxq
Transacton 34oiu98a

Block 54
Proof of work: 000000jjl93xq49
Previous block: 00000090b41bx
Transacton 555lbj4j12
Transacton bn24xa0201
Alice -> Bob

Agenda

- **Blockchain**
  - – Introduction
  - – Underlying Technology
- **Application of Blockchain**
  - – **Smart Contracts & Smart Property**
  - – **Financial applications**
- **Risks**
- **Q&A**

What’s in a Transaction?



From

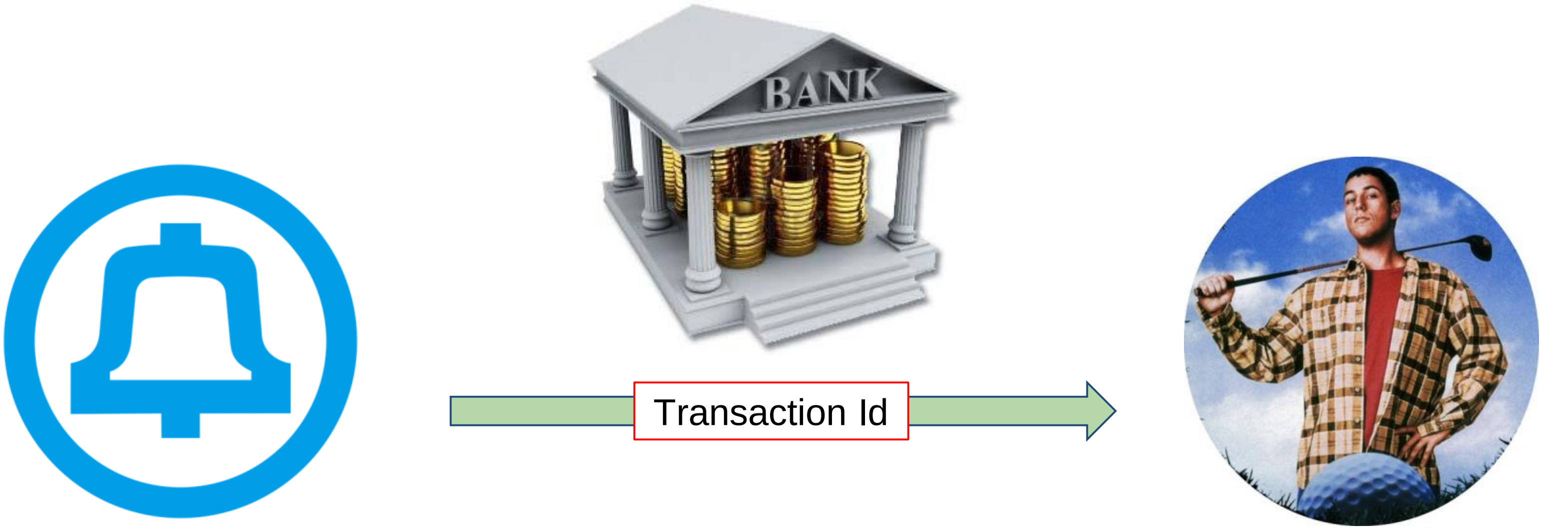
To

Note

Amount

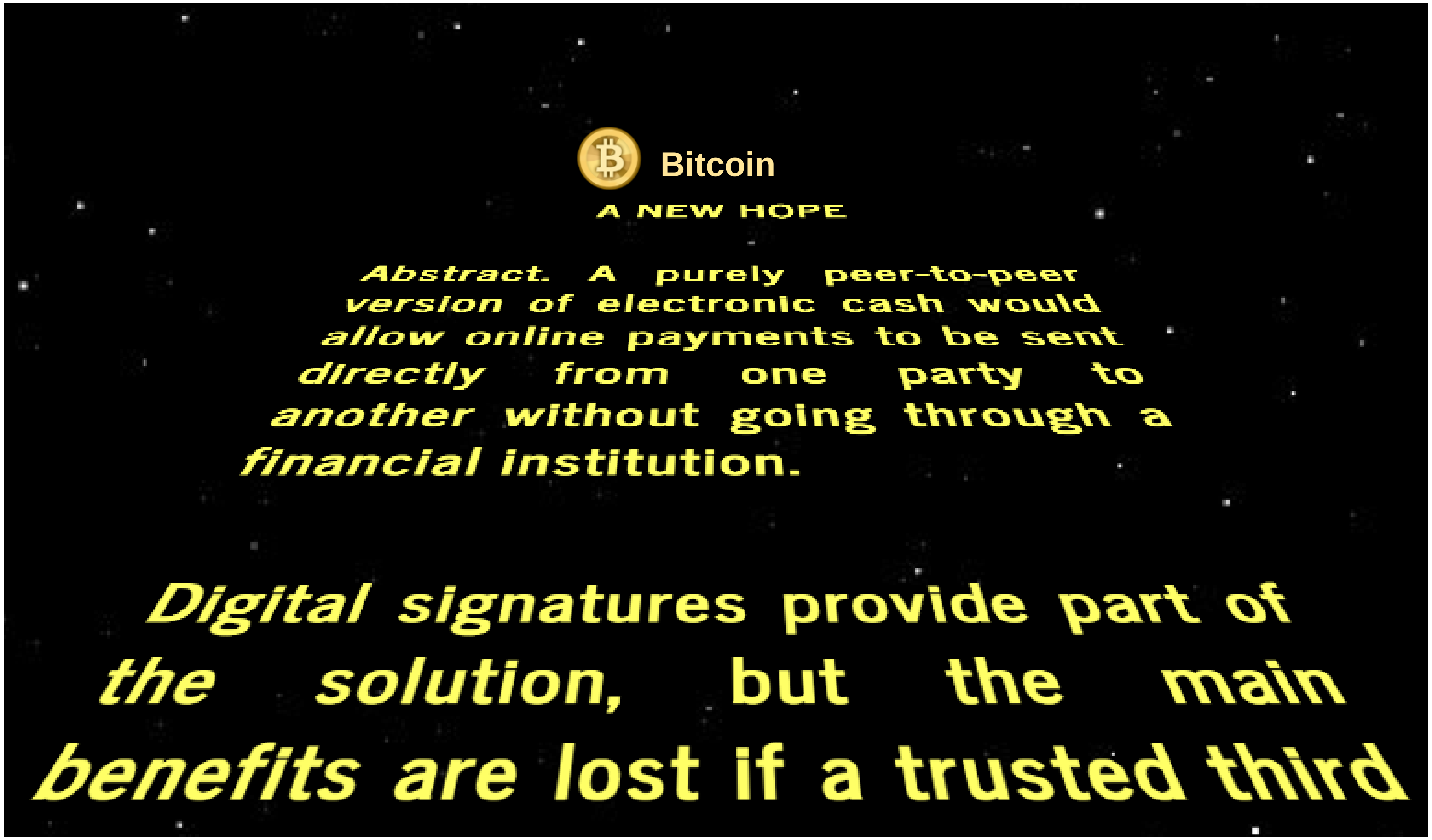
Signature

Bank Completes the Transaction



Transaction Id

- Validate Account, Funds, Signature, etc.
- Preserve Historical Record
- Dispute resolution

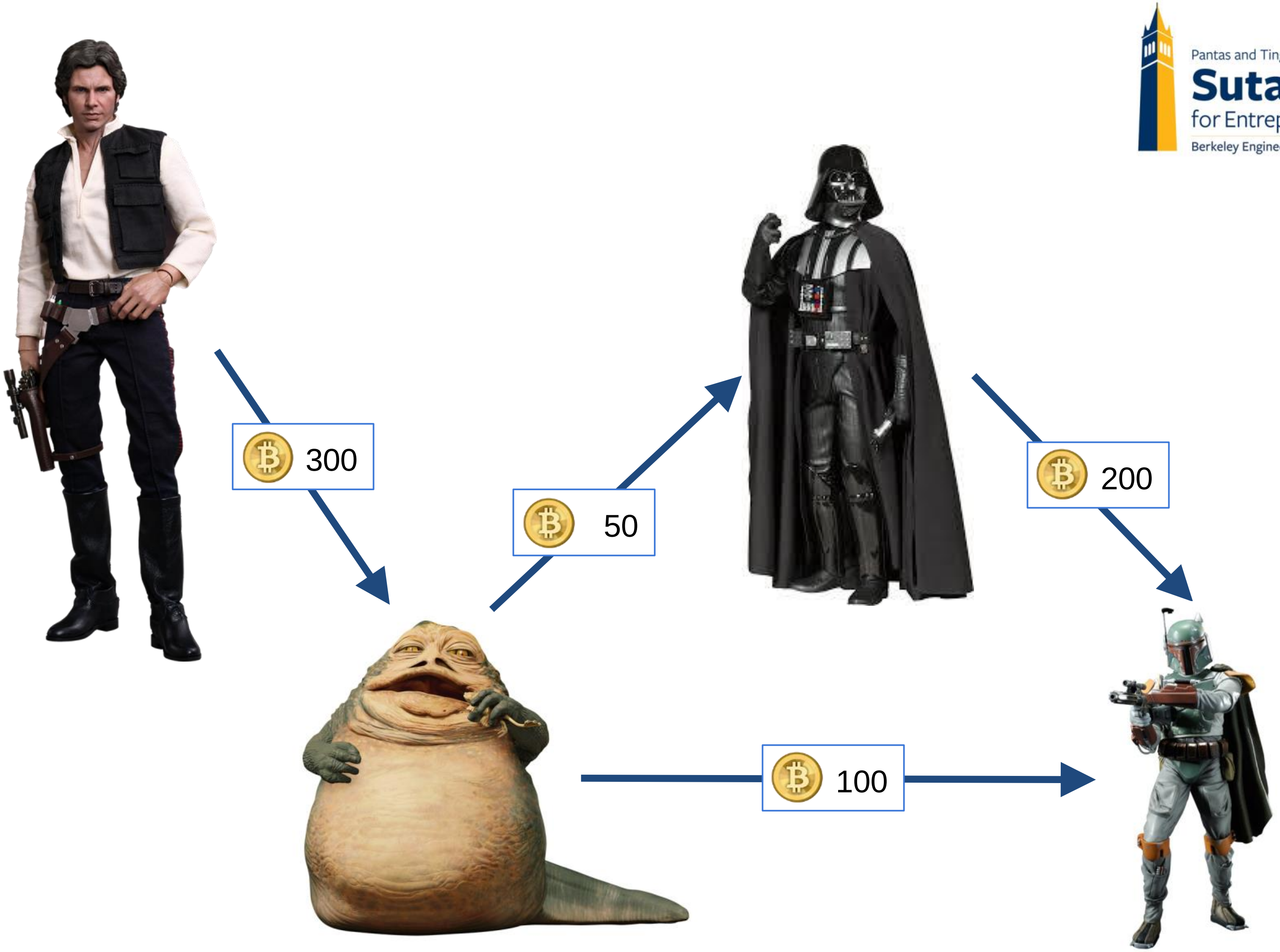


Bitcoin

A NEW HOPE

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.

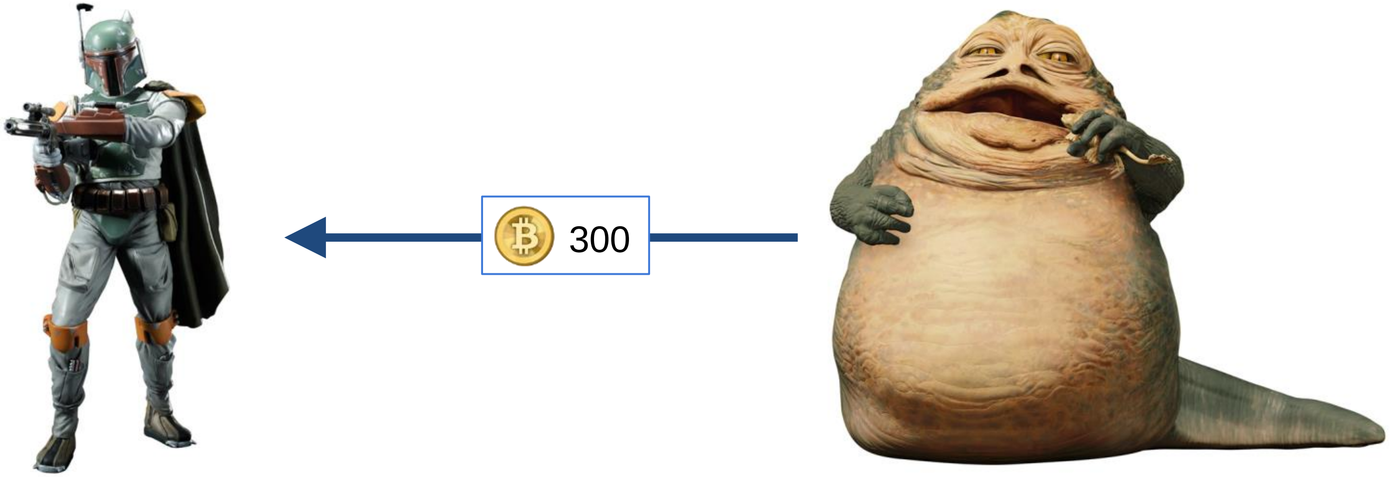
Digital signatures provide part of the solution, but the main benefits are lost if a trusted third


300
50
200
100

Bitcoin has a Public Ledger

From	To	Amount
Han Solo	Jabba	₿ 300
Jabba	Darth Vader	₿ 50
Jabba	Boba Fett	₿ 100
Darth Vader	Boba Fett	₿ 200
...	...	...

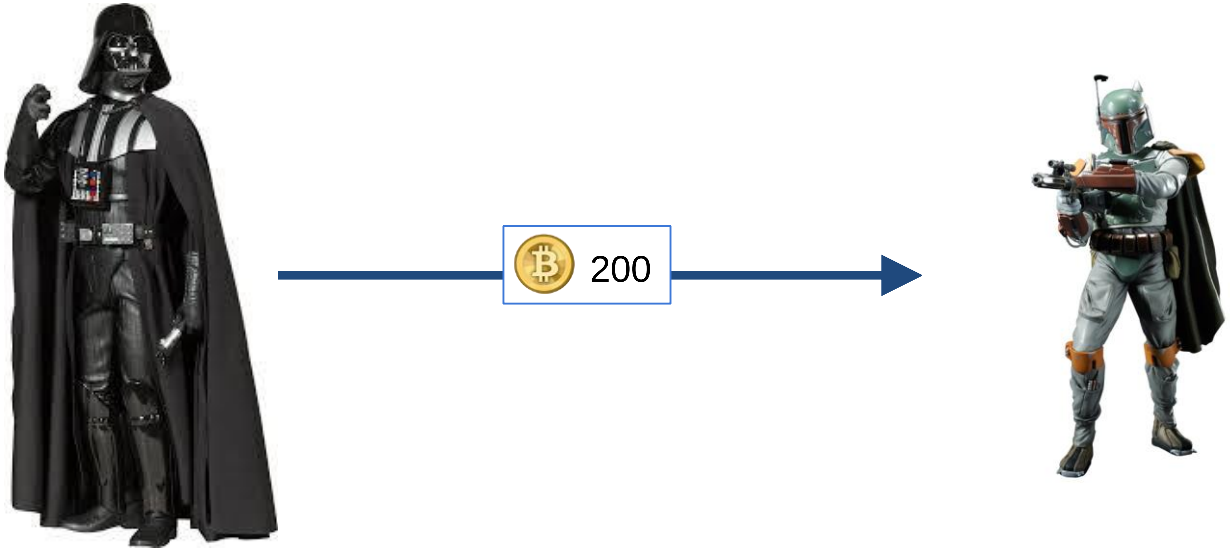
If the Ledger is Public, I'll just send all of Jabba's money to me.



Transactions are Signed with Private Key

From	Signature	To	Amount
Han Solo	z0D8Pm9ITT	Jabba	₿ 300
Jabba	04GNav84TI	Darth Vader	₿ 50
Jabba	fBC5cV0edM	Boba Fett	₿ 100
Darth Vader	mG6VnlKrQL	Boba Fett	₿ 200
...	...	...	...

I don’t want people to know I paid Boba, and my Jedi Mind Tricks don’t work on a public ledger!



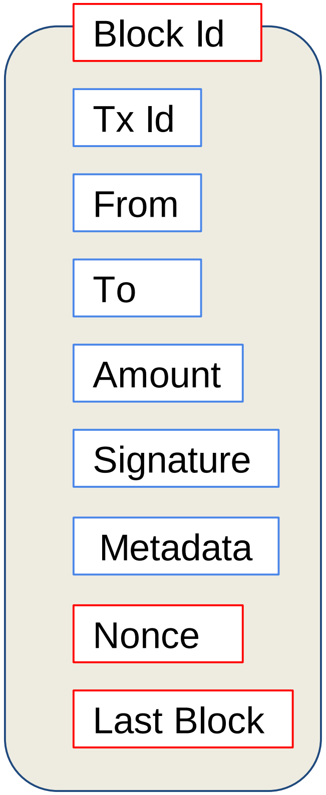
Ledger is both Pseudonymous and Traceable

From	Signature	To	Amount
RFloxXpoYC	z0D8Pm9ITT	z4ZFAMEl0i	₿ 300
z4ZFAMEl0i	04GNav84TI	CHRouGK9WN	₿ 50
z4ZFAMEl0i	fBC5cV0edM	MlAClZmSX6	₿ 100
CHRouGK9WN	mG6VnlKrQL	MlAClZmSX6	₿ 200
...	...	...	...

I’ll just hijack the ledger.

Attacking the blockchain is not my idea of courage. It's more like, suicide.

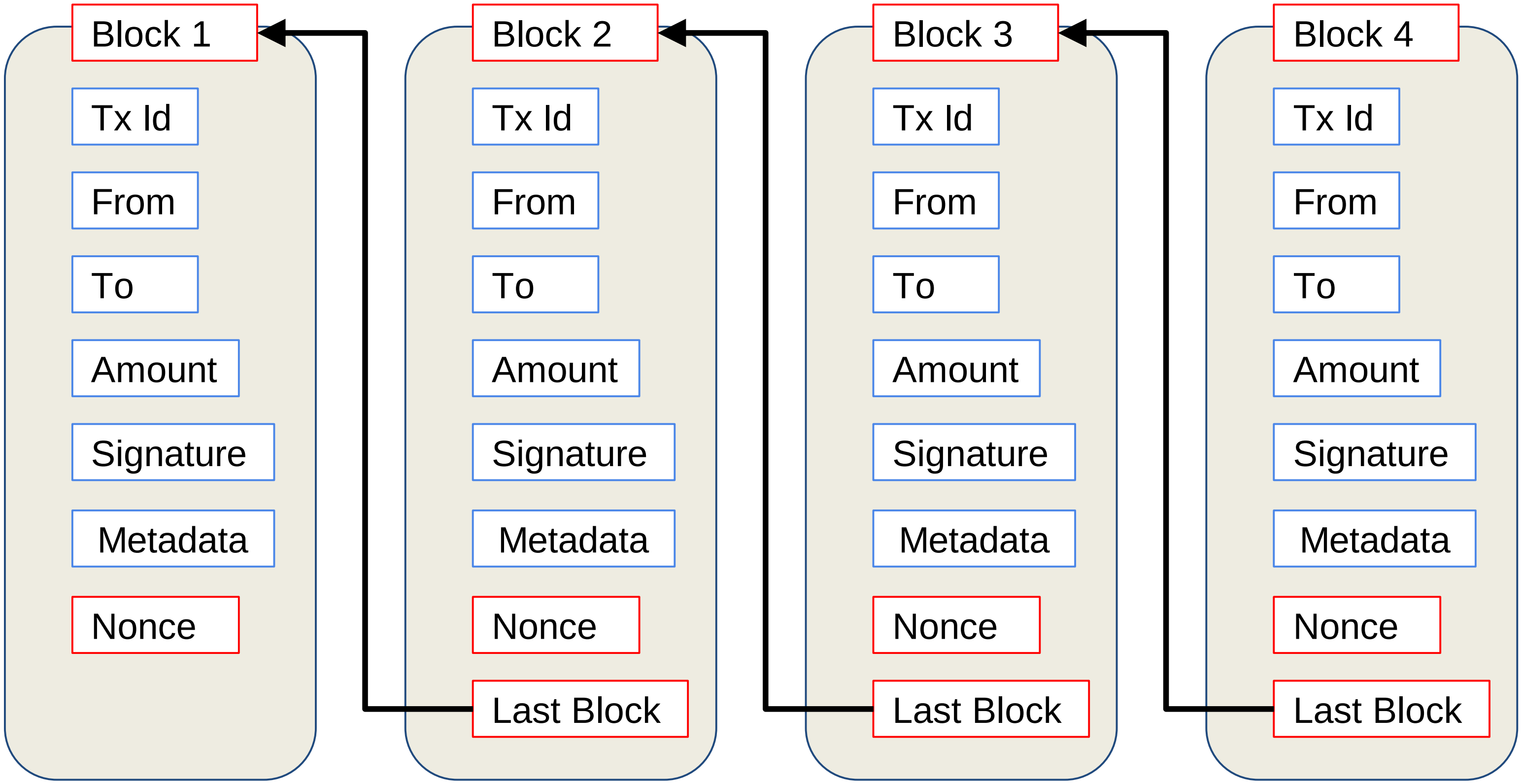
Transactions are grouped into Blocks



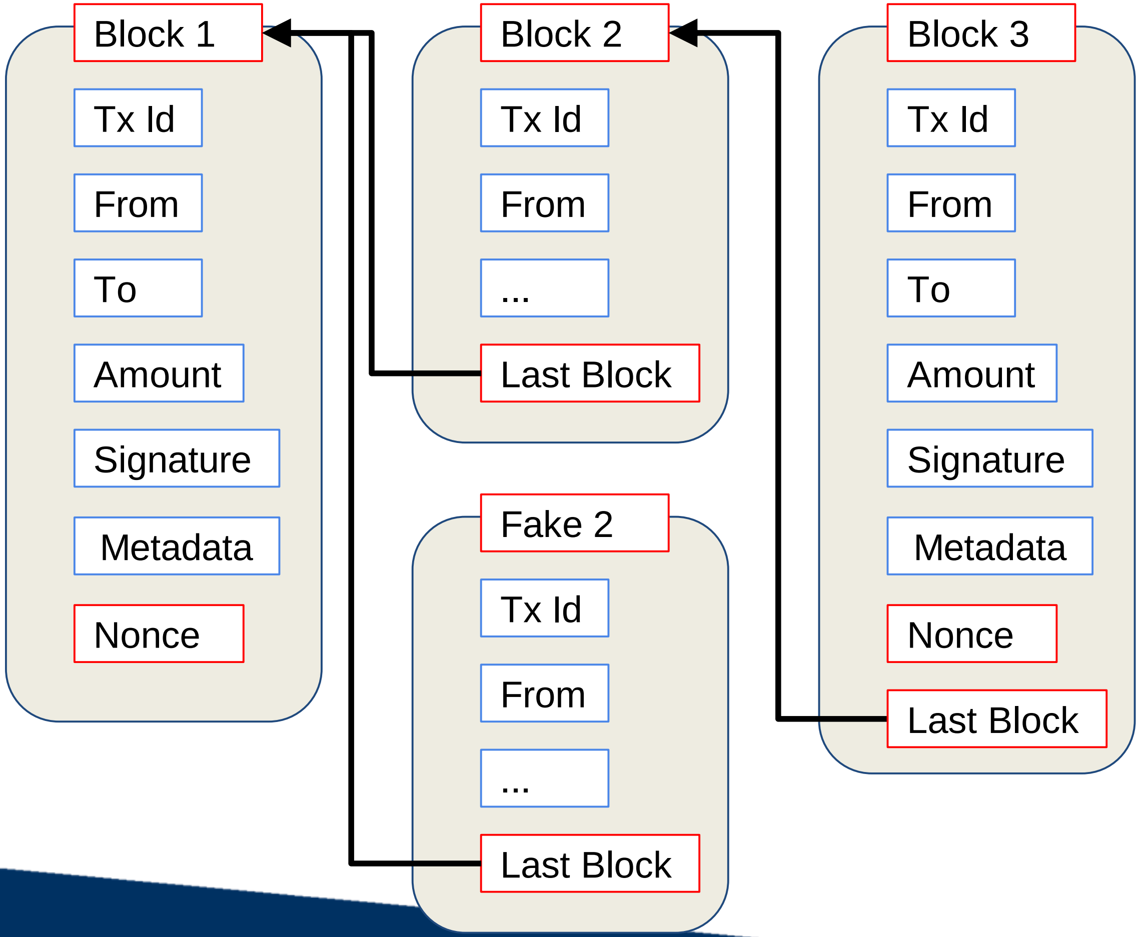
Nonce is just a solution to a puzzle

e.g. Pick a number such that the hash of all the blocks content has 3 leading 1’s.

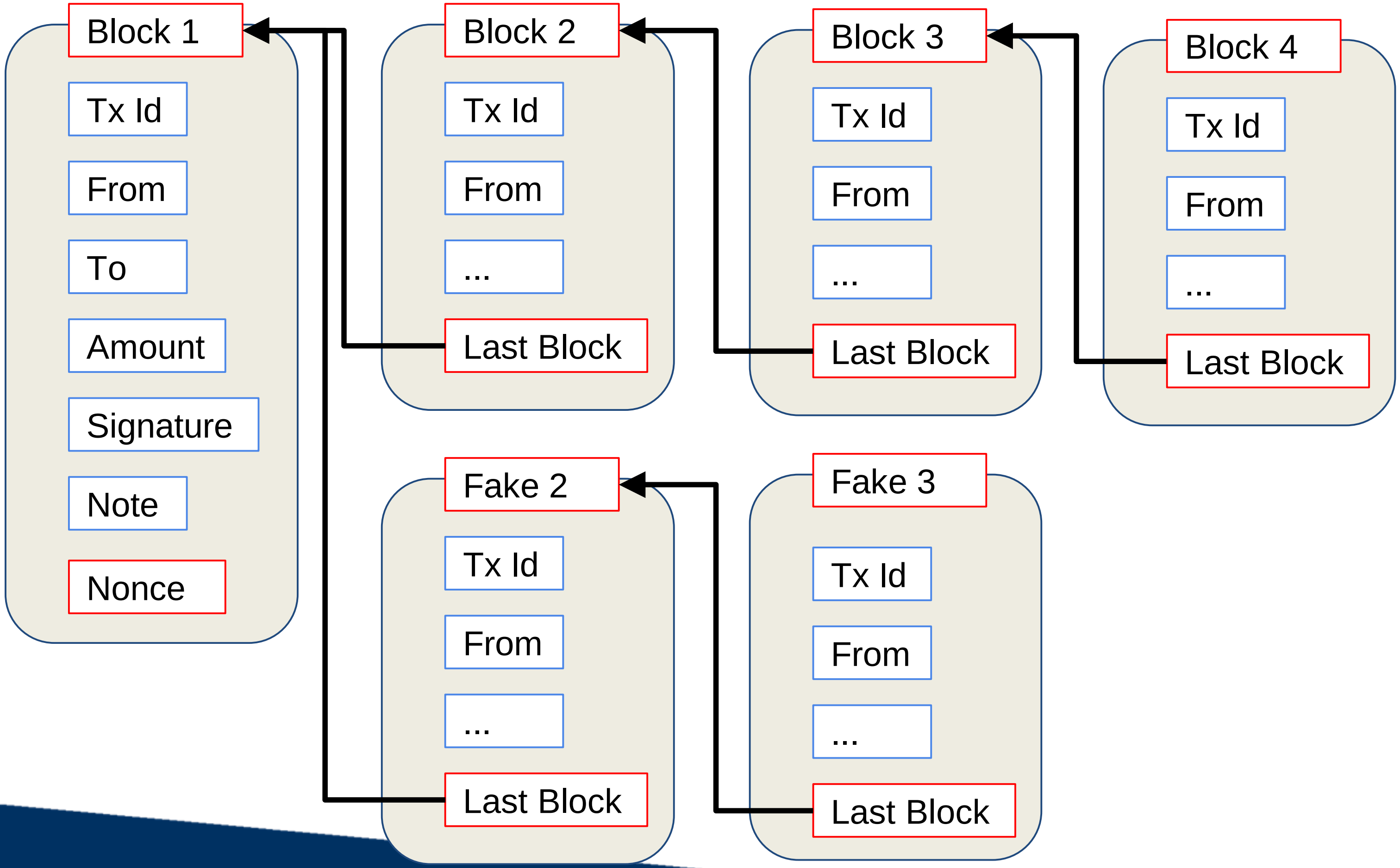
Transactions are Grouped into Blocks and Chained

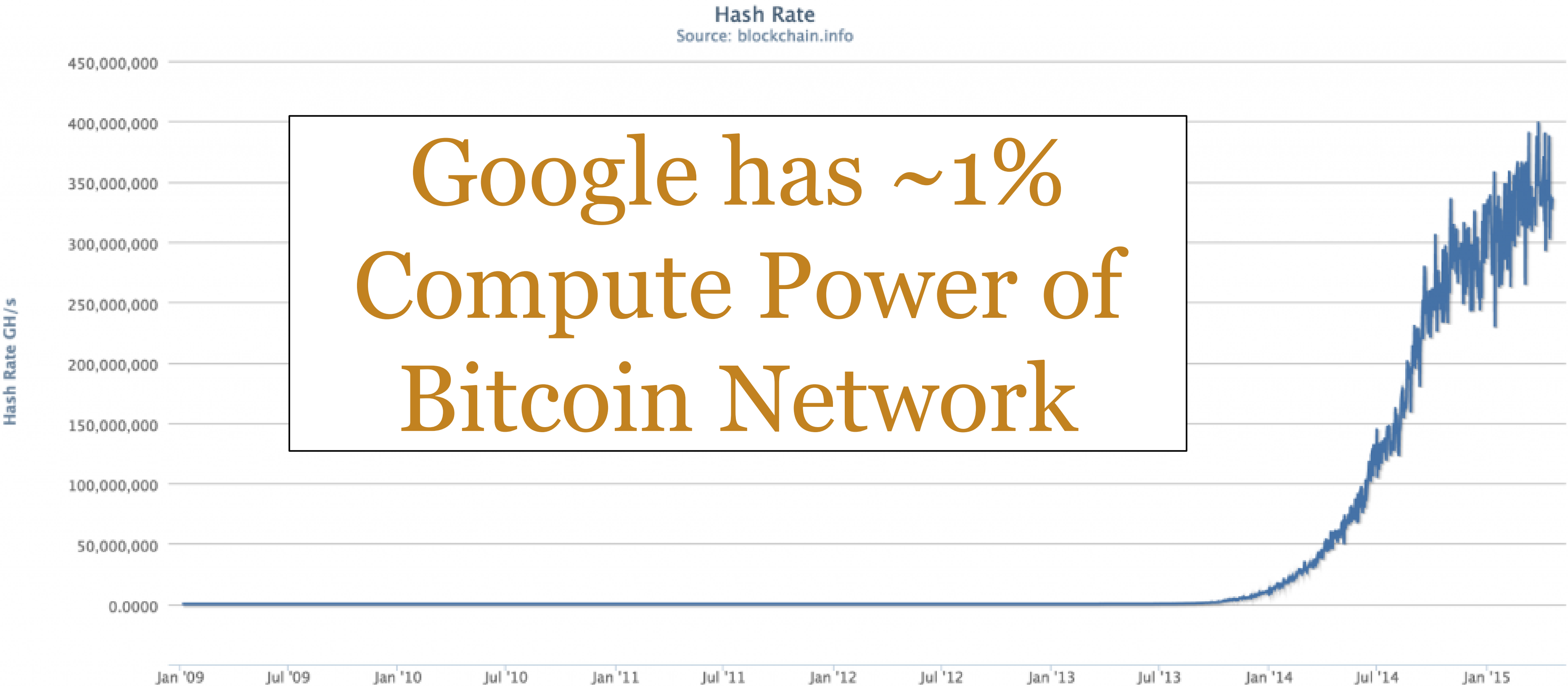


Blocks are Grouped into Chains



Fraudulent Blocks are in a Race





Google has ~1% Compute Power of Bitcoin Network

Properties of the Blockchain

- Public Ledger
- Pseudonymous
- Fault Tolerant (No Central Authority)
- Distributed Transactions
- Good for Untrustworthy/Hostile Environments

Applications of Blockchain

- Non-Financial Applications
- Financial Applications

Nick Szabo (1994): [Inventor of Smart Contract]

Smart Contract

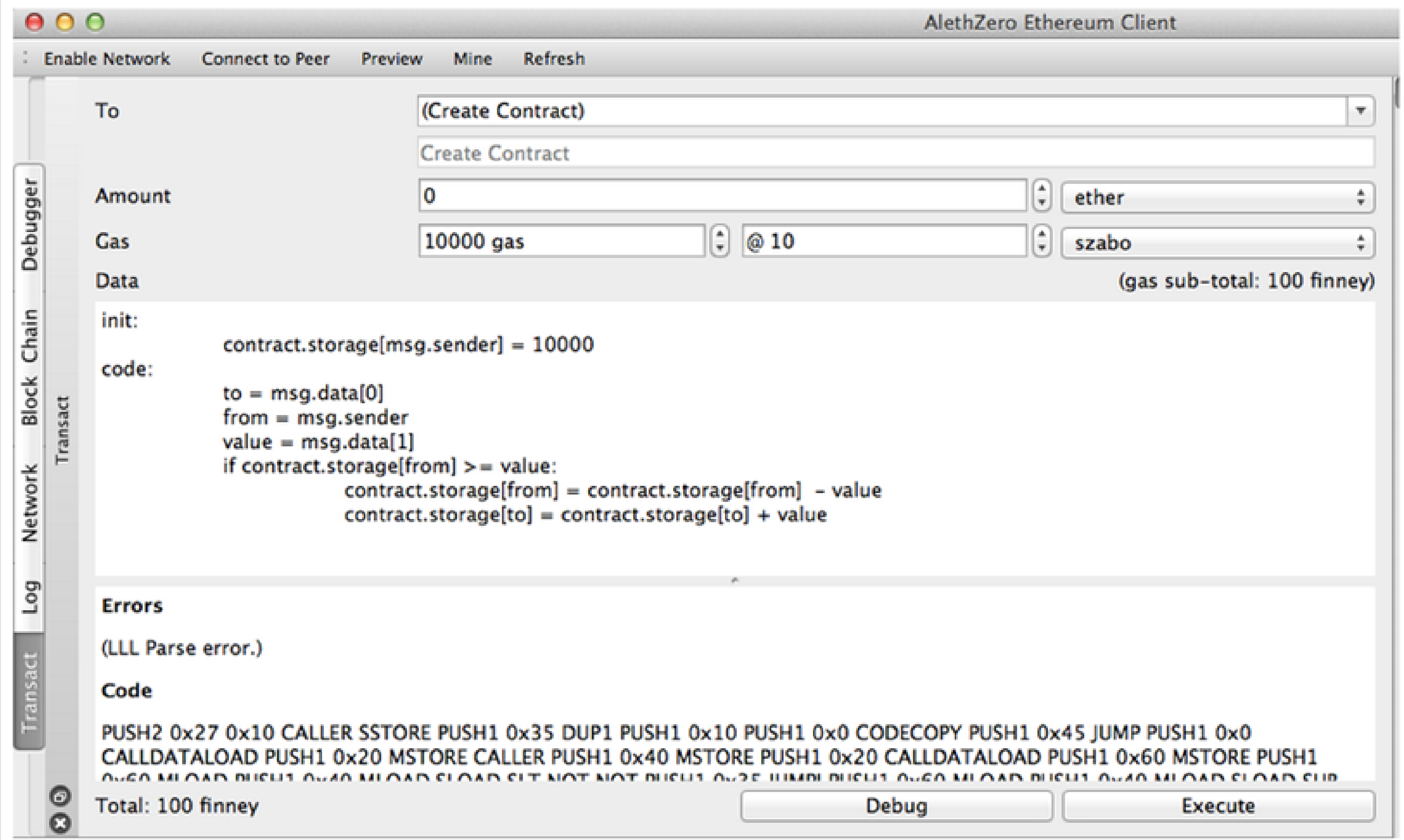
“Smart contracts are really the killer app of the cryptocurrencies world.”

What is Smart Contract?

Computer Program that automatically executes the terms of a contract

- Self-Enforceable
- Transparent
- Faster
- Cheaper

Easy to create contract



To: (Create Contract)

Create Contract

Amount: 0 ether

Gas: 10000 gas @ 10 szabo

Data (gas sub-total: 100 finney)

```
init:
              contract.storage[msg.sender] = 10000
code:
              to = msg.data[0]
              from = msg.sender
              value = msg.data[1]
              if contract.storage[from] >= value:
                            contract.storage[from] = contract.storage[from]  - value
                            contract.storage[to] = contract.storage[to] + value
```

Errors

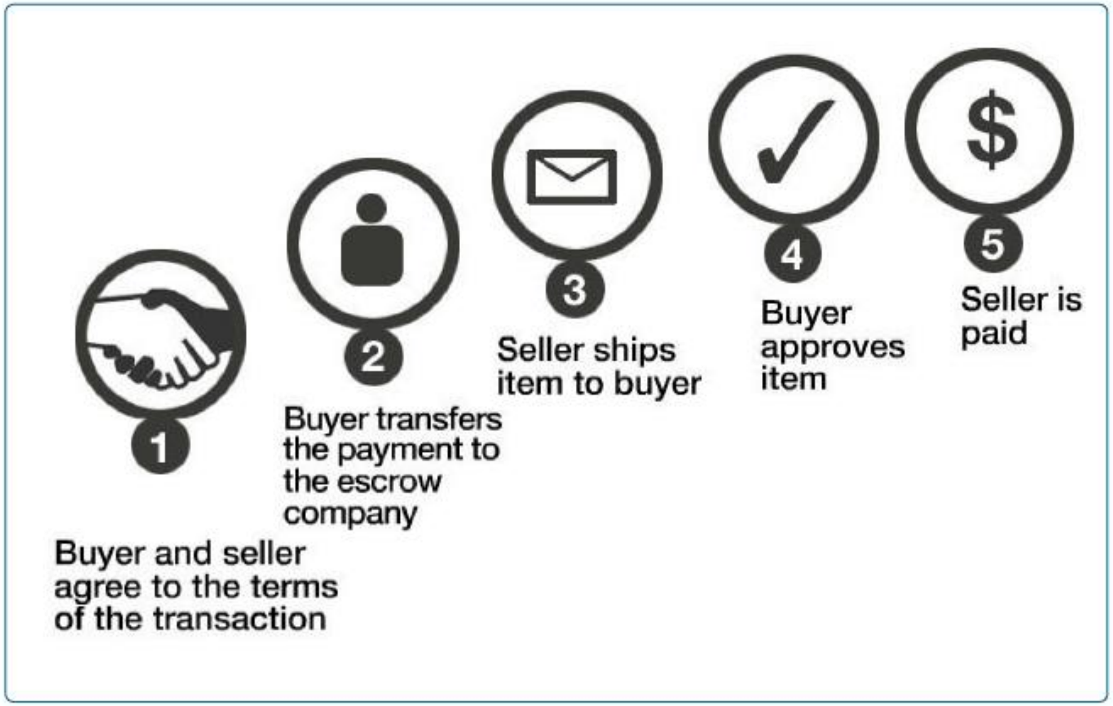
(LLL Parse error.)

Code

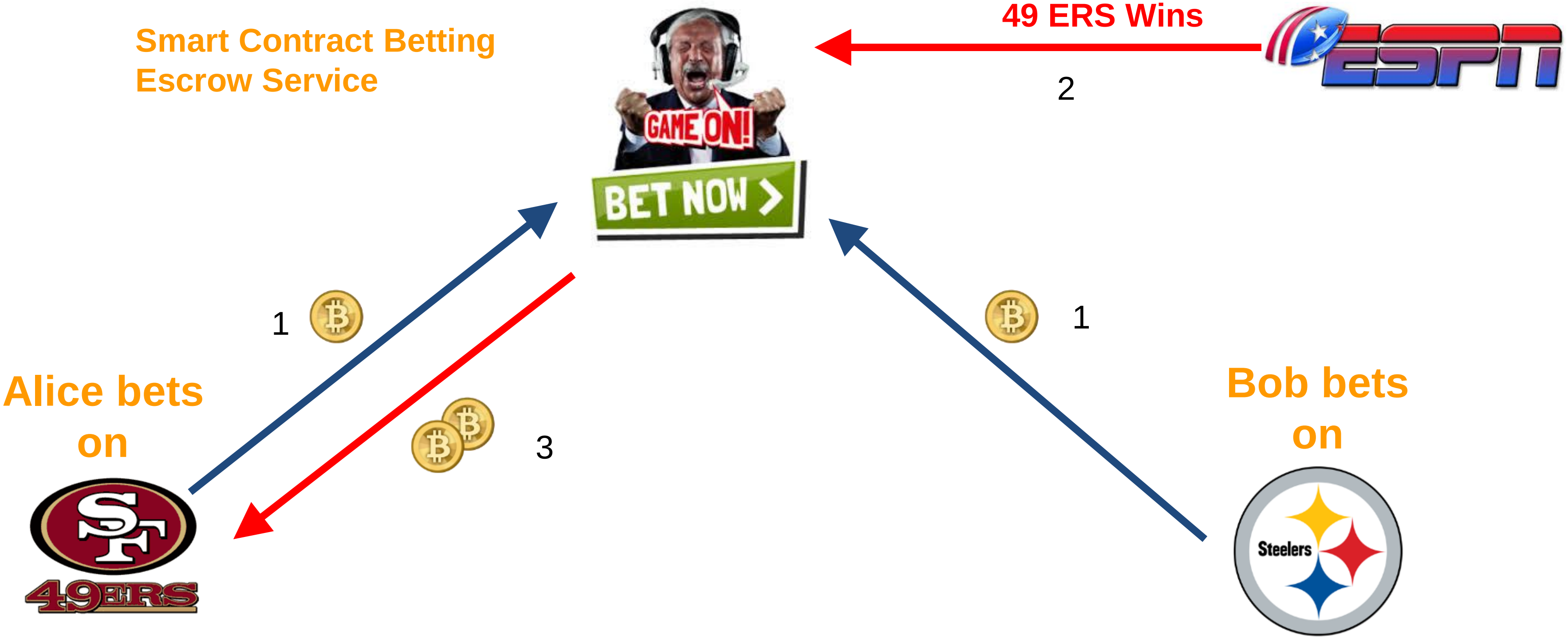
```
PUSH2 0x27 0x10 CALLER SSTORE PUSH1 0x35 DUP1 PUSH1 0x10 PUSH1 0x0 CODECOPY PUSH1 0x45 JUMP PUSH1 0x0
CALLDATALOAD PUSH1 0x20 MSTORE CALLER PUSH1 0x40 MSTORE PUSH1 0x20 CALLDATALOAD PUSH1 0x60 MSTORE PUSH1
0x60 MLOAD PUSH1 0x40 MLOAD SLOAD SLT NOT NOT PUSH1 0x35 JUMPI PUSH1 0x60 MLOAD PUSH1 0x40 MLOAD SLOAD SUB
```

Total: 100 finney

Smart Contract: Escrow Service


1
Buyer and seller agree to the terms of the transaction
2
Buyer transfers the payment to the escrow company
3
Seller ships item to buyer
4
Buyer approves item
$
5
Seller is paid

Example: SUPER BOWL BET



Smart Contract Betting
Escrow Service

49 ERS Wins

2

1

1

Alice bets
on

3

Bob bets
on

Smart Property

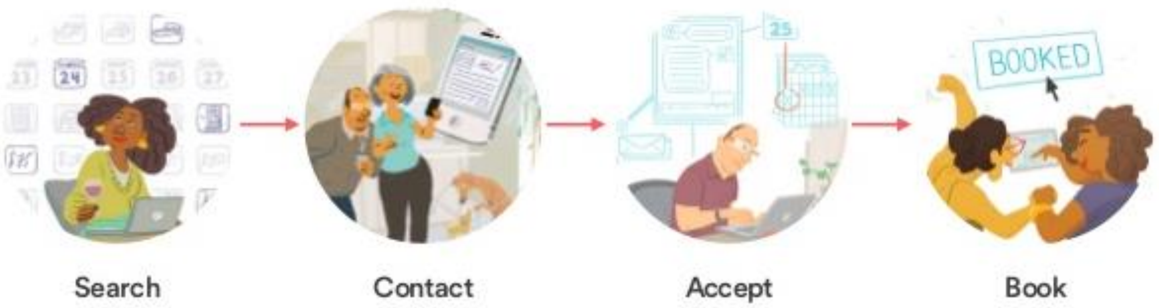
Physical Property whose ownership is controlled by via a blockchain using smart contracts.

Smart Property also includes non-physical property such as shares in a company or access rights to a remote computer.

Examples: Smart Phones, Cars, Houses, Diamonds, Shares etc.

Example: AirBnb Vacation Rental Business Model: A Brokerage Service

Booking Model



Both Guest and Host rely on AirBnB for Trust: AirBnb charges hefty fees for providing “Brokerage service”.

Smart Property: Applied to AirBnB Business

- Assumption : “Locks” are Internet enabled.
- AirBnB “Brokerage Service” now becomes “Escrow Service”:
  - “Guest” and “Host” enters an agreement regarding “Payment” for renting.
  - Smart Property Token (“key”) is delivered to smart device (phone or wearable device) for the duration of the stay once payment is received.
  - Guest Need not Trust Host--Past History/Rating of the renter from blockchain (public ledger)

Brokerage Services like AirBnB and Uber go through transformation.

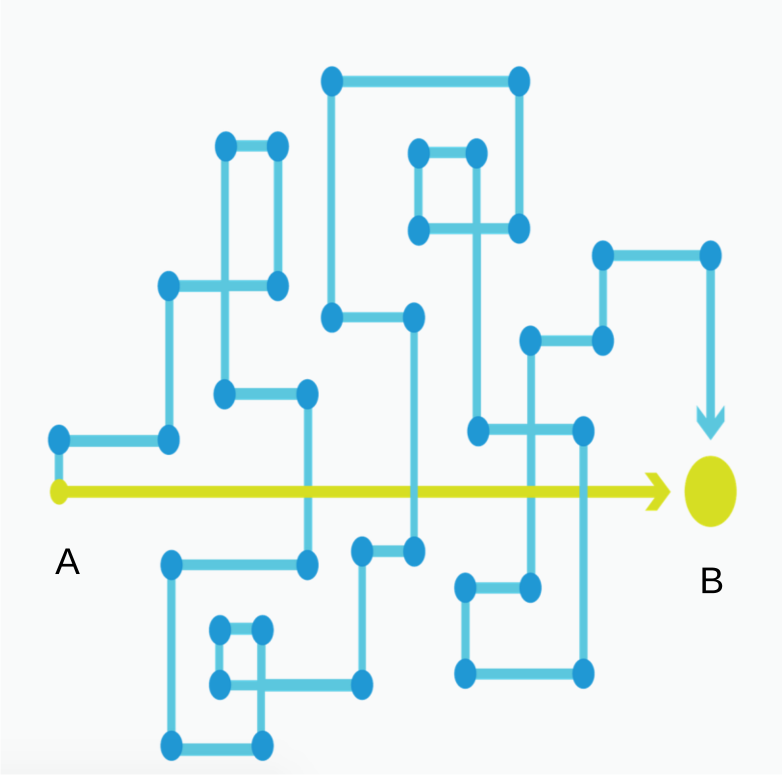
Financial Applications

- Private Securities
  - Private companies to raise fund by selling shares
  - Example: Chain, Medicii, Coinsetter, Augur, Bitshares, etc.
- Remittance Services
  - Ex: Music royalty payment, Pre-paid phone charges, Forex transactions, etc.
- Insurance
  - Insuring properties, goods, valuables, etc through smart contract
  - Example : EverLedger

Private Equity : NASDAQ

NASDAQ Private Market:

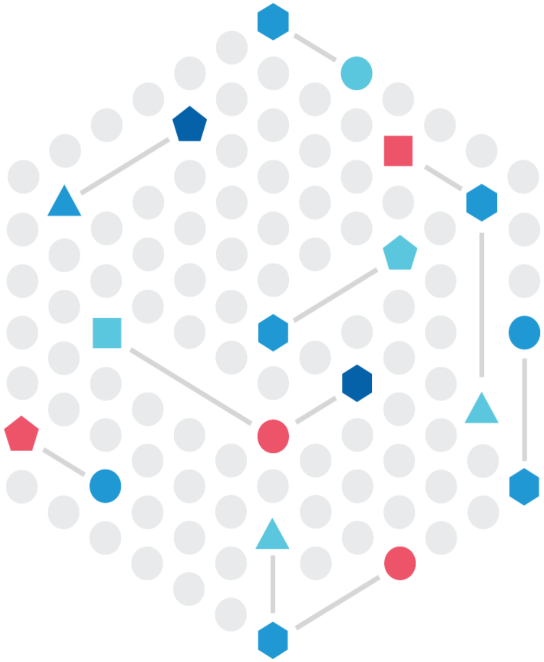
- Launched in 2014 for Equity ownership (cap table) and relationship management
- Inefficient Process:
  - Slow
  - Multiple intermediaries



Source: chain.com

NASDAQ - Chain Tie up

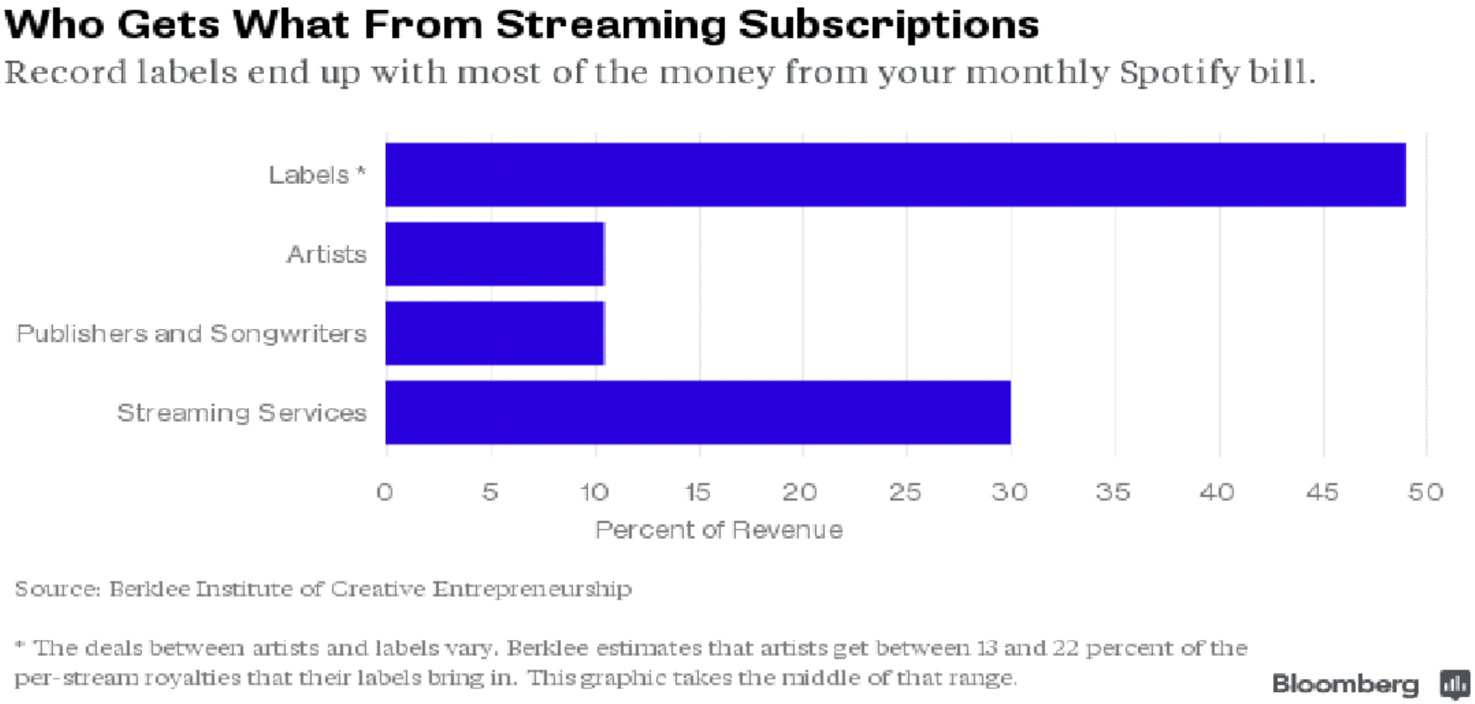
- Blockchain based solution for Private Equity Market
- Advantages:
  - Efficient (no 3rd party)
  - Traceable
  - Faster



Source: chain.com

Music Royalties

Current Framework



Who Gets What From Streaming Subscriptions

Record labels end up with most of the money from your monthly Spotify bill.

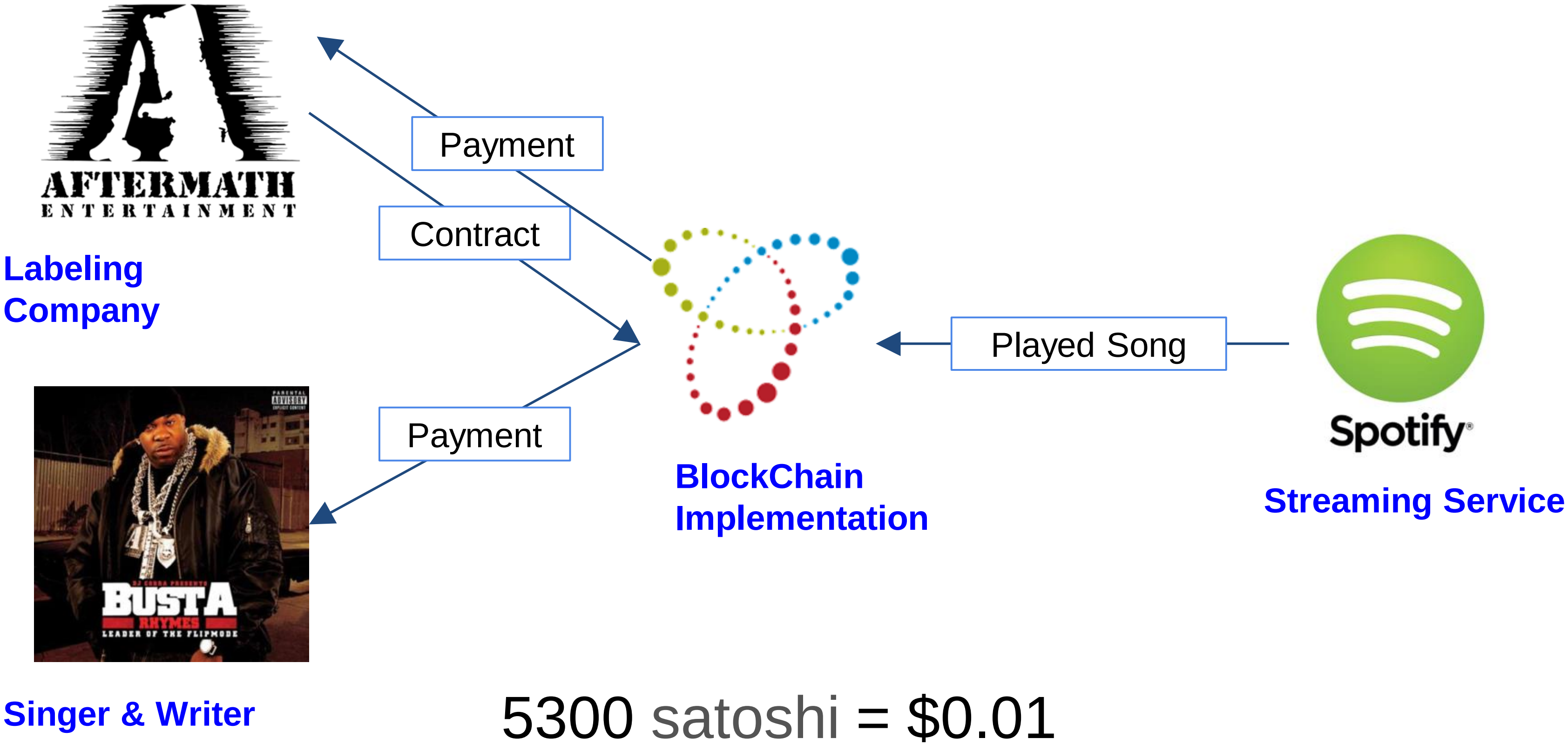
Source: Berklee Institute of Creative Entrepreneurship

* The deals between artists and labels vary. Berklee estimates that artists get between 13 and 22 percent of the per-stream royalties that their labels bring in. This graphic takes the middle of that range.

Current Rev Share Framework lacks:

- Transparency
- Accuracy
- Slow

Music Royalties:
as Smart Contracts



Payment

Contract

Payment

Played Song

Labeling Company

BlockChain Implementation

Streaming Service

Singer & Writer

5300 satoshi = $0.01

Risks & Conclusion

- Change is constant, but people are hesitant to change!
- How can intermediaries stay relevant with blockchain?
- Scaling has headwinds in terms of bootstrap issues
- Government regulations bureaucracy!

Thanks

Q&A

Risks

Significant adoptions risk due to:

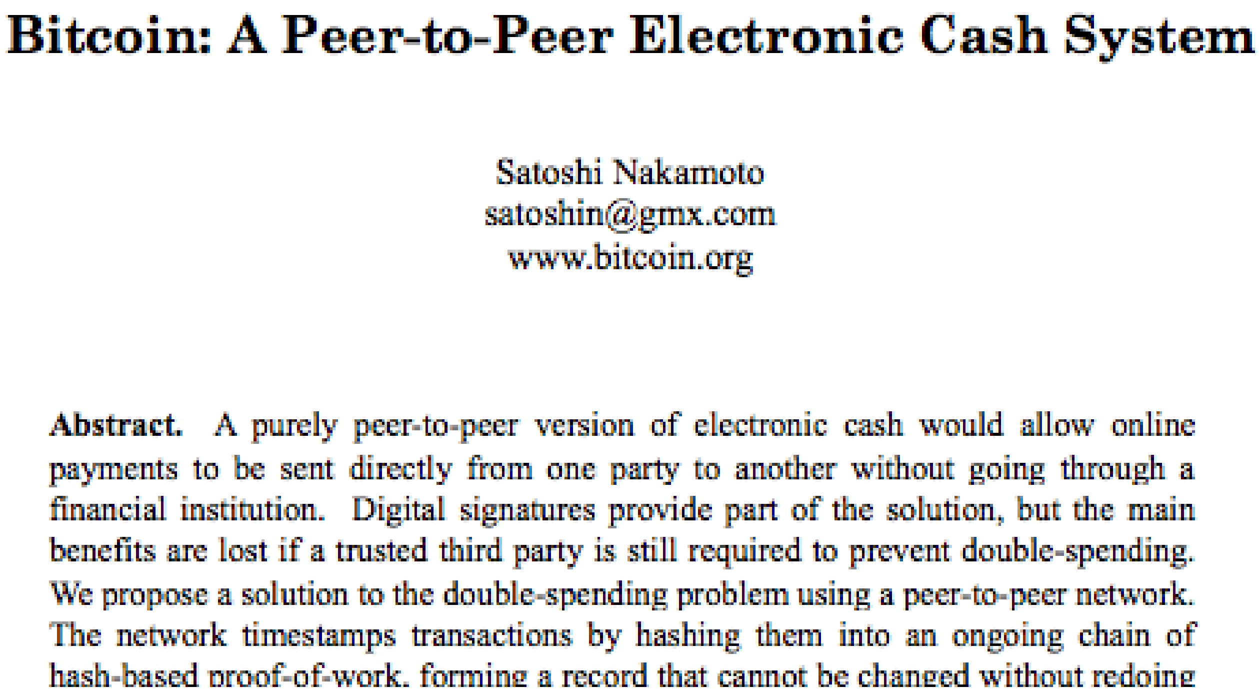
- Behavioral change in trade without a trusted 3rd party
- Government regulations
- Illegal activities (Money laundering)
- Scalability
- Quantum Computing Advancement

Non-Financial application

- Notary
  - Convenient, fast and private
  - Example : Stamperey

- Music Industry
  - Simplifying the royalty distribution

Bitcoin Whitepaper - 10/31/08

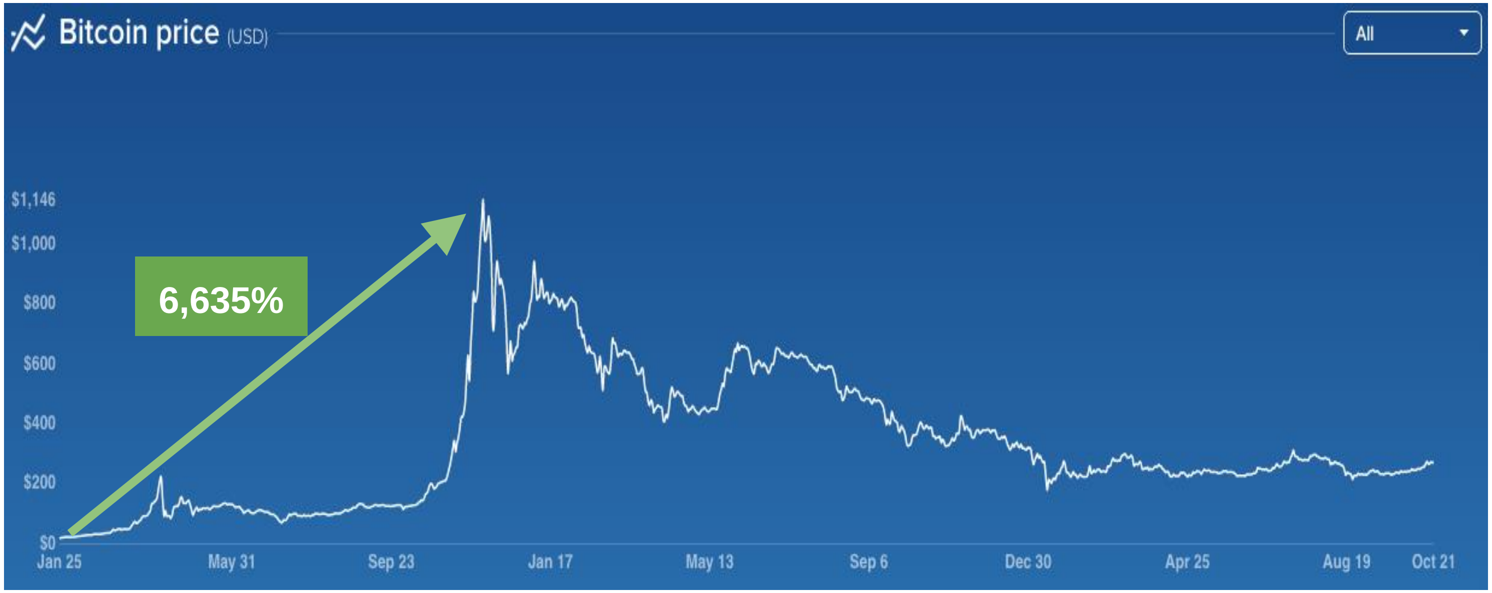


Bitcoin: A Peer-to-Peer Electronic Cash System

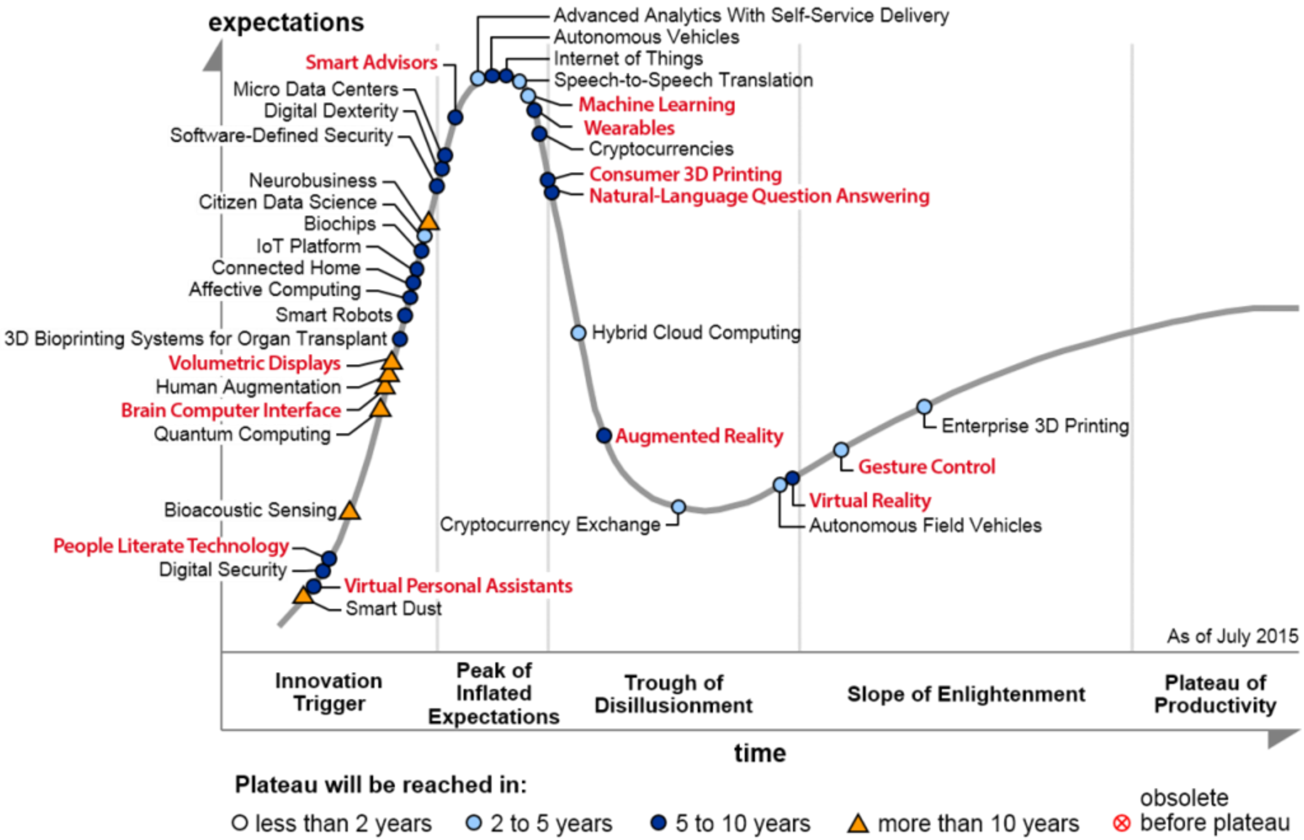
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing

Bitcoin to USD



The Emerging Technology Hype Cycle (2105)

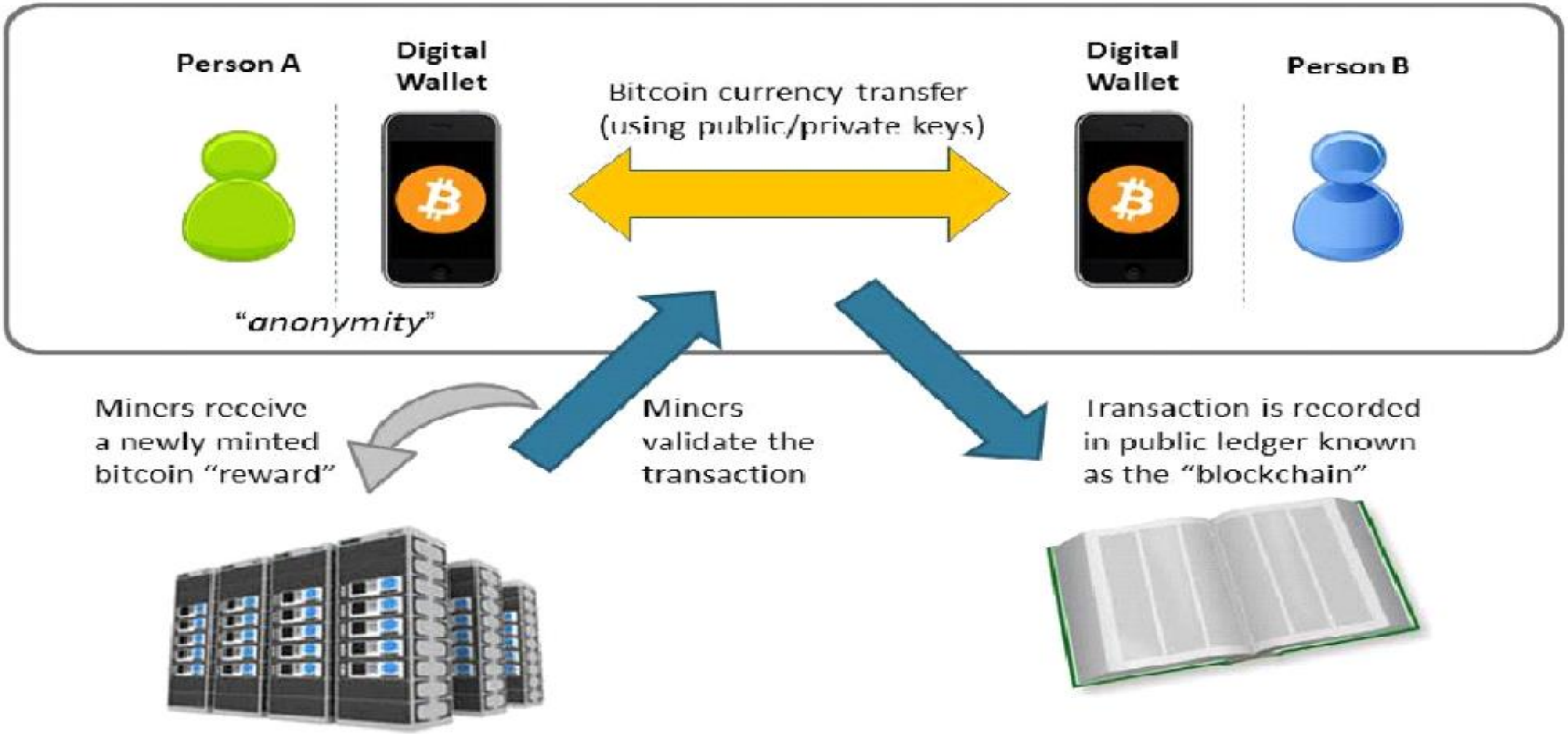


*Adapted from "Gartner Emerging Technology Hype Cycle 2015"

Music Royalties as Smart Contracts

Artists often claim that streaming service providers and labels are making money off of streaming, which has generated massive distrust and anger among artists.

Streaming services pay the labels, who typically pay nothing to the artists.

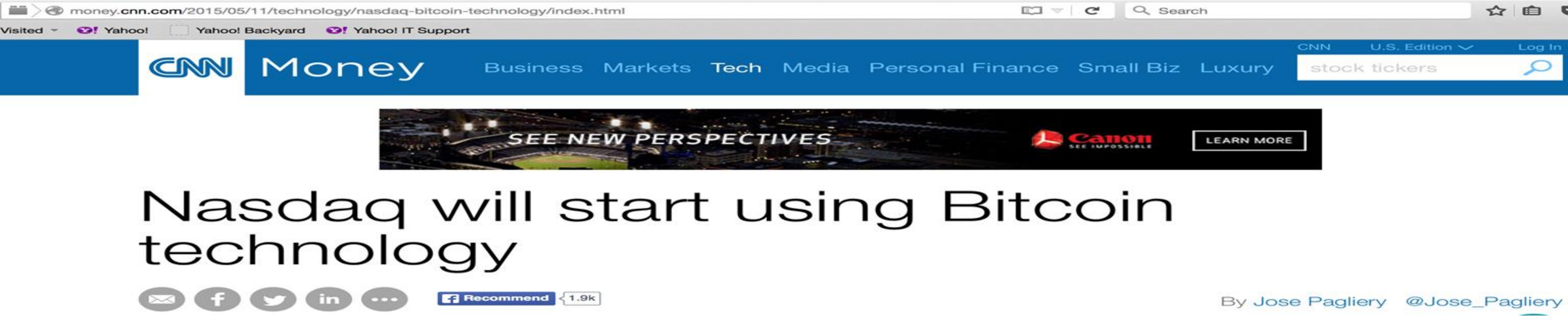


Miners receive a newly minted bitcoin "reward"

Miners validate the transaction

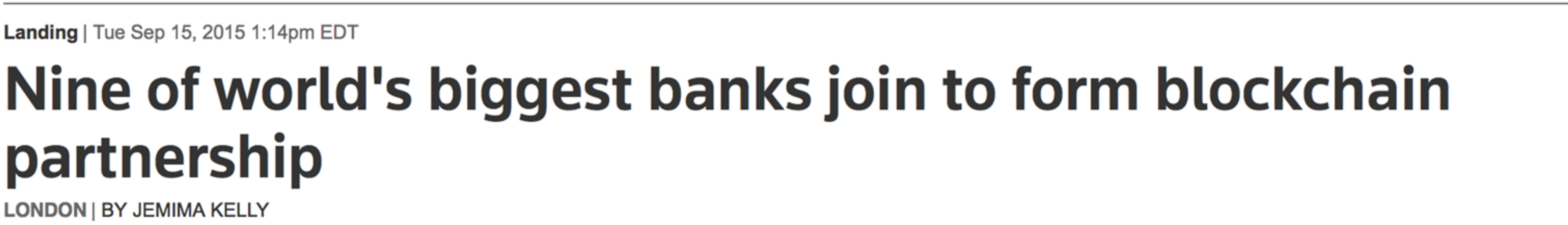
Transaction is recorded in public ledger known as the "blockchain"

placeholder for headlines for blockchain



Nasdaq will start using Bitcoin technology

By Jose Pagliery @Jose_Pagliery



Landing | Tue Sep 15, 2015 1:14pm EDT

Nine of world's biggest banks join to form blockchain partnership

LONDON | BY JEMIMA KELLY