

RSA® Conference 2018

San Francisco | April 16–20 | Moscone Center

SESSION ID: SEM-M02

FOUNDATIONS OF BITCOIN, BLOCKCHAIN, AND SMART CONTRACTS

What You Need to Know About Bitcoin & Crypto

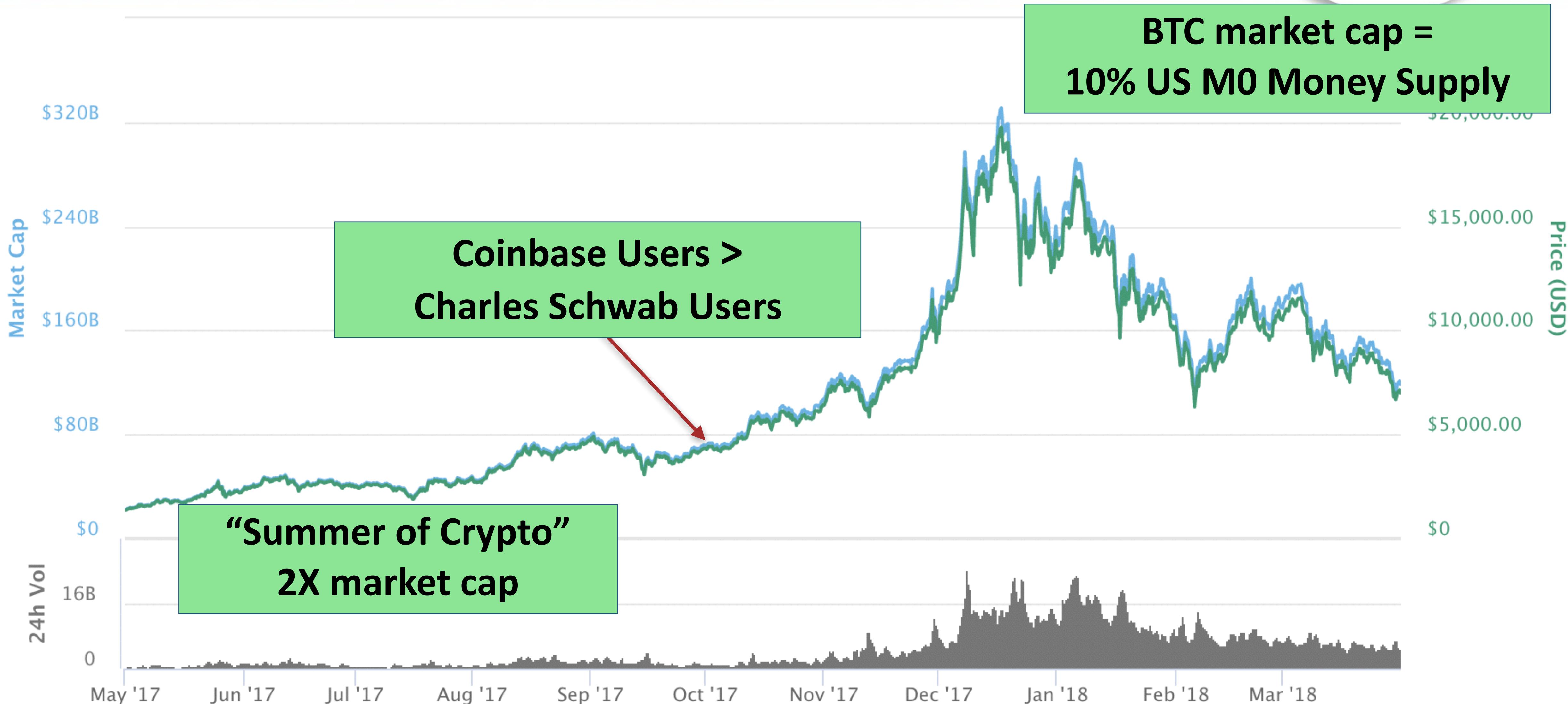
Benjamin Jun, HVF Labs



H V F



Is this the Future of Money?



Today's Agenda



1/ FUNDAMENTALS

- Bitcoin, Blockchain, and Smart Contracts
- Ethereum, Tokens, and ICOs

2/ APPLICATIONS

- Blockchain for the Enterprise
- Case: Identity and Federations
- Legal – Smart Contracts, Blockchain, and ICOs

3/ ATTACKS

- Cryptocurrency Attacks and Security Challenges
- Bad Actors in ICOs, Ransomware

Satoshi's World

Bitcoin: A Peer-to-Peer Electronic Cash System (2008)

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 the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Peer-to-Peer

Digital Signatures

No Trusted Third Party

Decentralized

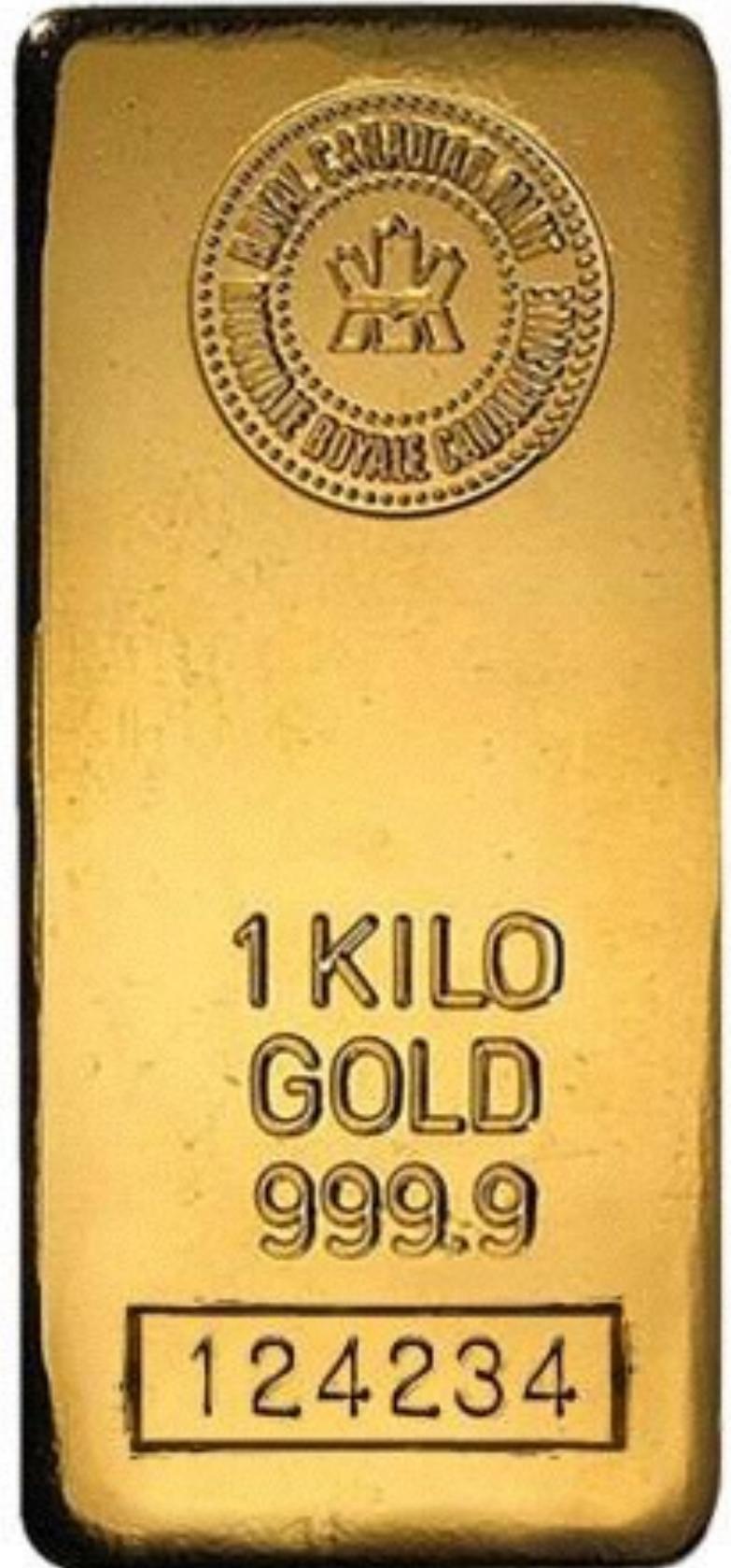
Chained Proof-of Work

Value



bitcoin

Units of Value



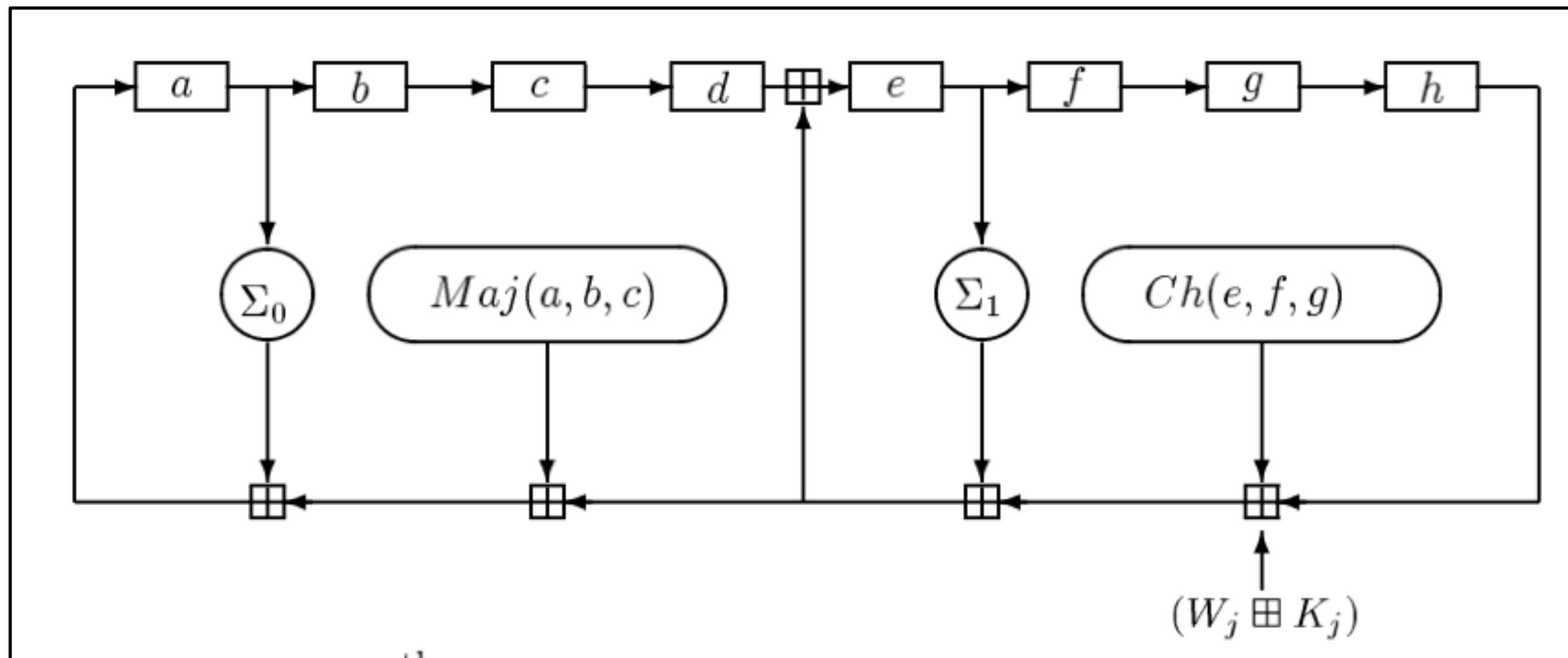
Token value based on
supply & demand

Mining For Value



Bitcoin: “Proof-of-Work” Mining

SHA-256 Hash Function (adopted 2002)



1. Repeat SHA-256 until result = “rare”
2. Credit the finder

Hashes

Hash

0000000000000000000000000000000023279ea4059b36d44a354b1d283560cdb0860c508f620d

Modern Mining Tools

GEFORCE® GTX 1080 Ti

Founders Edition

[LEARN MORE >](#)

\$ 699⁰⁰

OUT OF STOCK

Free Shipping

Limit 2 per customer



GEFORCE® GTX 1080

Founders Edition

[LEARN MORE >](#)

\$ 549⁰⁰

OUT OF STOCK

Free Shipping

Limit 2 per customer

GEFORCE® GTX 1070 Ti

Founders Edition

[LEARN MORE >](#)

\$ 449⁰⁰

NOTIFY ME

Free Shipping

Limit 2 per customer

GEFORCE® GTX 1070

Founders Edition

[LEARN MORE >](#)

\$ 399⁰⁰

OUT OF STOCK

Free Shipping

Limit 2 per customer

GEFORCE® GTX 1060

Founders Edition

[LEARN MORE >](#)

\$ 299⁰⁰

OUT OF STOCK

Free Shipping

Limit 2 per customer

Contracts



Signed Transfers



Alice's Car
Transfer to Bob

STATE OF CALIFORNIA
CERTIFICATE OF TITLE

01234567890

AUTOMOBILE

VEHICLE NUMBER ABCDEFG0123456789
BODY TYPE MODEL 4D
UNLADEN AX WEIGHT FUEL G
TRANSFER DATE 04/17/04 FEES PAID \$15
YR 1991 SOLD CLASS 2004 MO KR
EQUIPMENT/TRUST NUMBER
MOTORCYCLE ENGINE NUMBER
ODOMETER DATE 02/23/1999
ODOMETER READING
REGISTERED OWNER(S)
JOHN DOE
123 MAIN ST
SACRAMENTO, CA 95814

I certify under penalty of perjury under the laws of the State of California, that THE SIGNATURE(S) BELOW RELEASES INTEREST IN THE VEHICLE.
1a. DATE X SIGNATURE OF REGISTERED OWNER
1b. DATE X SIGNATURE OF REGISTERED OWNER
Federal and State law requires that you state the mileage upon transfer of ownership. Failure to complete or providing a false statement may result in fines and/or imprisonment.
The odometer now reads _____ (no tens), miles and to the best of my knowledge reflects the actual mileage unless one of the following statements is checked.
WARNING Odometer reading is not the actual mileage. Mileage exceeds the odometer mechanical limits.
I certify under penalty of perjury under the laws of the State of California that the foregoing is true and correct.
SIGN
LIEHOLDERS
SIGN
IMPORTANT READ CAREFULLY
Any change of Lienholder (holder of security interest) must be reported to the Department of Motor Vehicles within 10 days.
LIEHOLDERS
SIGN
2. X SIGNATURES RELEASES INTEREST IN VEHICLE. (Company names must be countersigned)
Release Date _____
CA12345678
000123
REO. 17-30R (REV. 10-03)

KEEP IN A SAFE PLACE - VOID IF ALTERED

Alice Signs

Bob's Car
Transfer to Cheryl

STATE OF CALIFORNIA
CERTIFICATE OF TITLE

01234567890

AUTOMOBILE

VEHICLE NUMBER ABCDEFG0123456789
BODY TYPE MODEL 4D
UNLADEN AX WEIGHT FUEL G
TRANSFER DATE 04/17/04 FEES PAID \$15
YR 1991 SOLD CLASS 2004 MO KR
EQUIPMENT/TRUST NUMBER
MOTORCYCLE ENGINE NUMBER
ODOMETER DATE 02/23/1999
ODOMETER READING
REGISTERED OWNER(S)
JOHN DOE
123 MAIN ST
SACRAMENTO, CA 95814

I certify under penalty of perjury under the laws of the State of California, that THE SIGNATURE(S) BELOW RELEASES INTEREST IN THE VEHICLE.
1a. DATE X SIGNATURE OF REGISTERED OWNER
1b. DATE X SIGNATURE OF REGISTERED OWNER
Federal and State law requires that you state the mileage upon transfer of ownership. Failure to complete or providing a false statement may result in fines and/or imprisonment.
The odometer now reads _____ (no tens), miles and to the best of my knowledge reflects the actual mileage unless one of the following statements is checked.
WARNING Odometer reading is not the actual mileage. Mileage exceeds the odometer mechanical limits.
I certify under penalty of perjury under the laws of the State of California that the foregoing is true and correct.
SIGN
LIEHOLDERS
SIGN
IMPORTANT READ CAREFULLY
Any change of Lienholder (holder of security interest) must be reported to the Department of Motor Vehicles within 10 days.
LIEHOLDERS
SIGN
2. X SIGNATURES RELEASES INTEREST IN VEHICLE. (Company names must be countersigned)
Release Date _____
CA12345678
000123
REO. 17-30R (REV. 10-03)

KEEP IN A SAFE PLACE - VOID IF ALTERED

Bob Signs

Digital Signatures

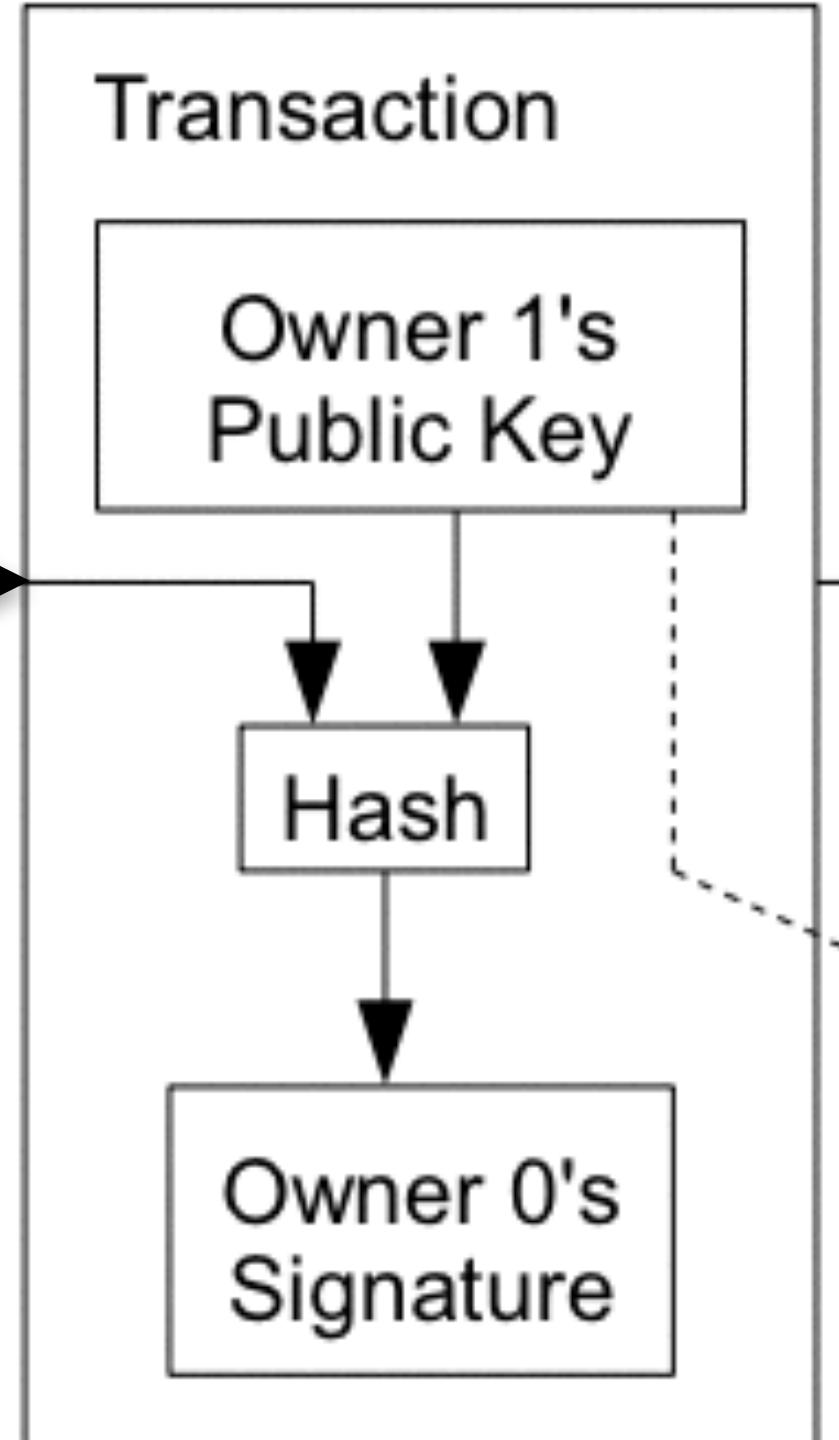
Alice → Bob



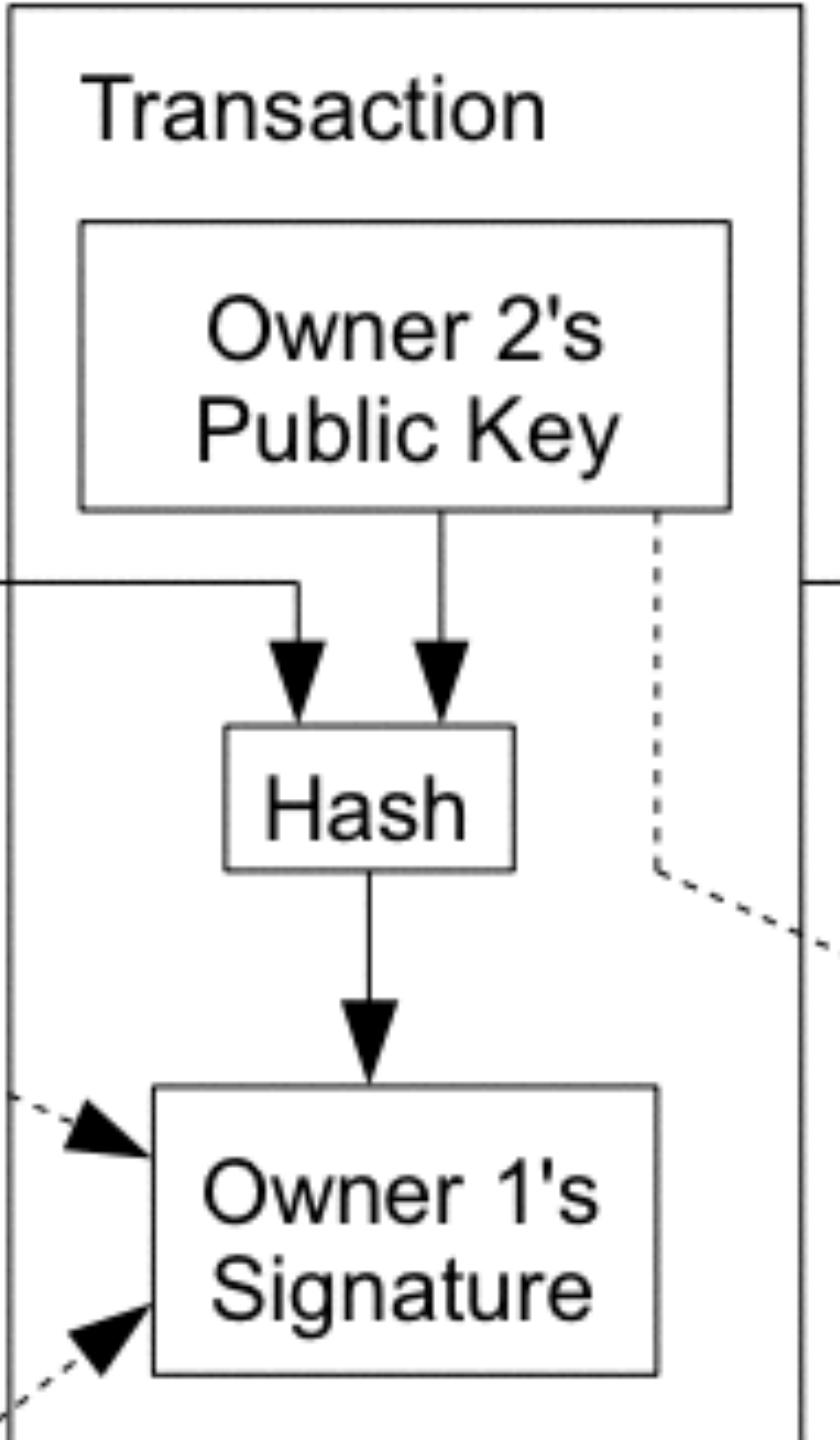
Bob → Cheryl



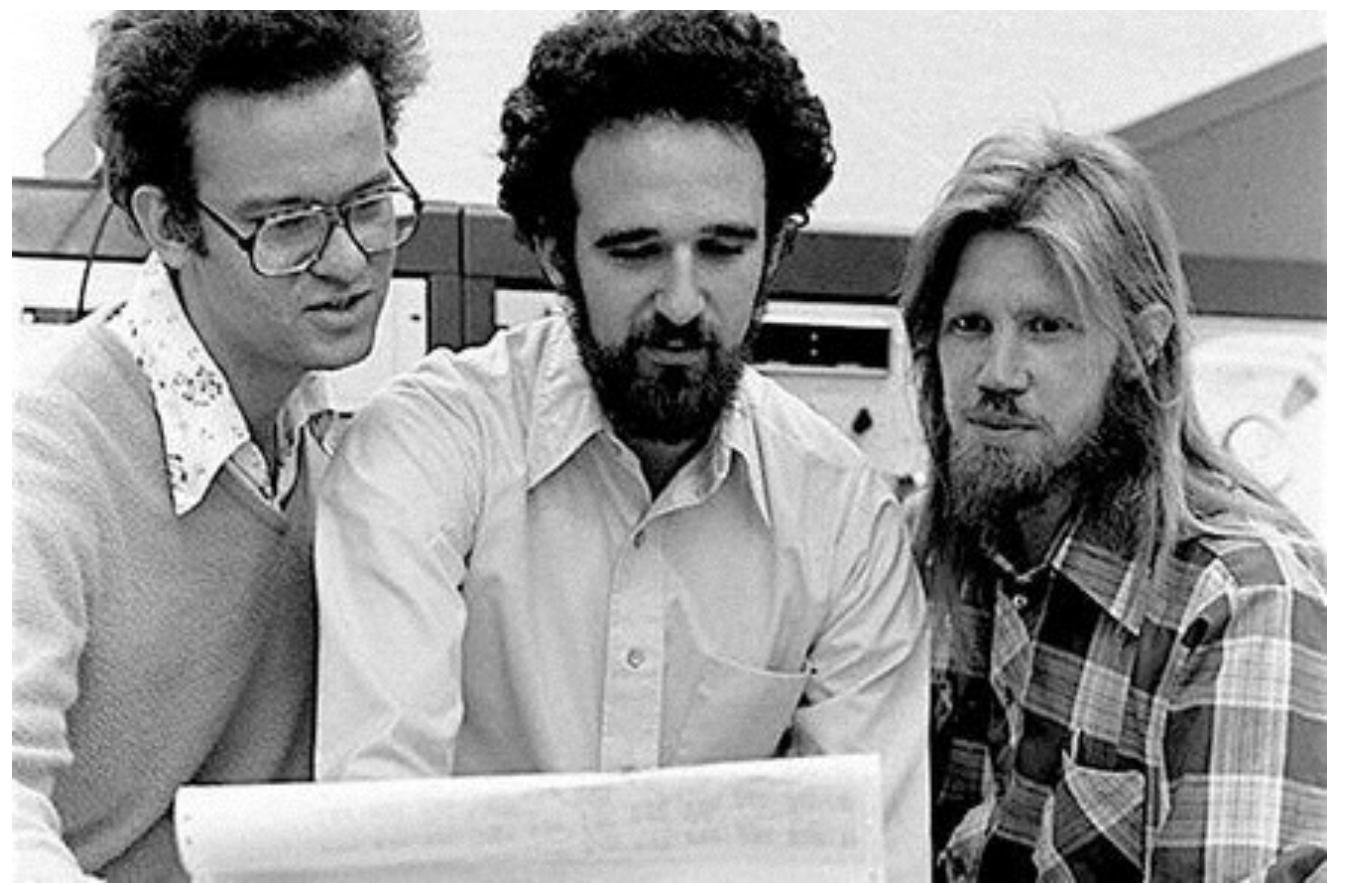
Cheryl → Dan



Dan → Eve



Merkle - Diffie - Hellman



Owner 1's
Private Key

Owner 2's
Private Key

Ledgers





Luca Pacioli ~1500

Medici Family

Debtors & Creditors (1605-1633)

14

UPenn ms. codex 1312 91r

When Contracts Aren't Centralized...



Two California Certificate of Title documents are shown side-by-side. Both documents feature a large red 'X' over the signature area. The signatures are clearly forged, appearing as yellow-green scribbles. The documents contain standard title information including vehicle details, owner information, and a release of interest section.

**FORGED
DATA**

Two California Certificate of Title documents are shown side-by-side. Both documents feature a large red exclamation mark over the signature area. The signatures are clearly forged, appearing as yellow-green scribbles. The documents contain standard title information including vehicle details, owner information, and a release of interest section.

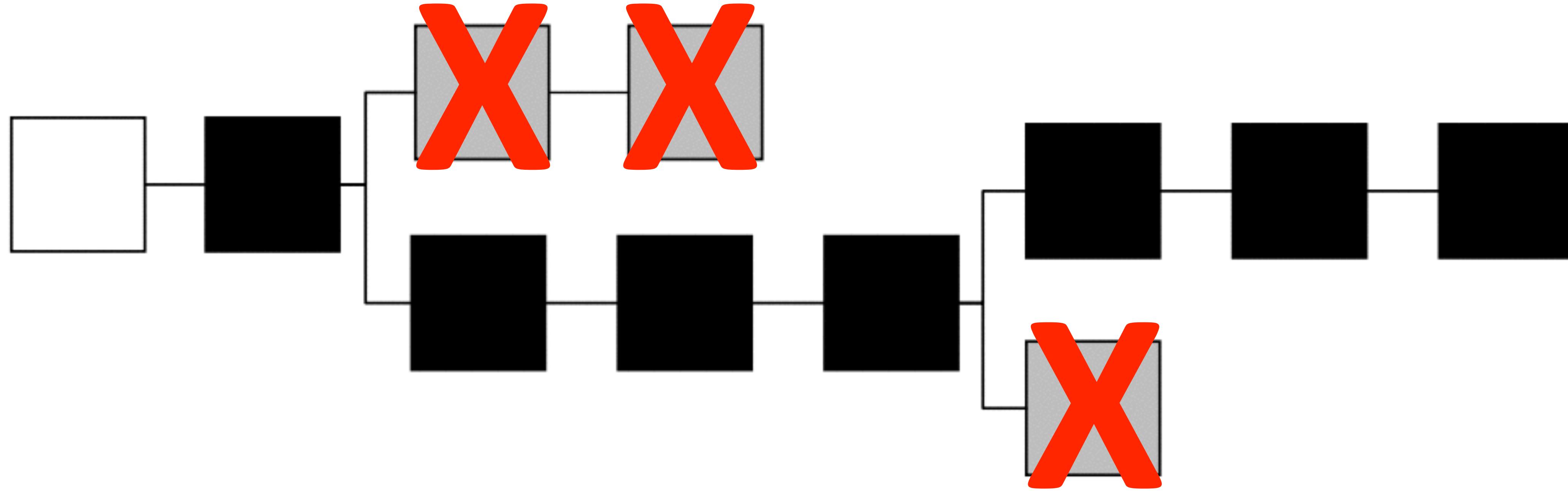
**DOUBLE
SPEND**

Two California Certificate of Title documents are shown side-by-side. Both documents feature a large red exclamation mark over the signature area. The signatures are clearly forged, appearing as yellow-green scribbles. The documents contain standard title information including vehicle details, owner information, and a release of interest section.

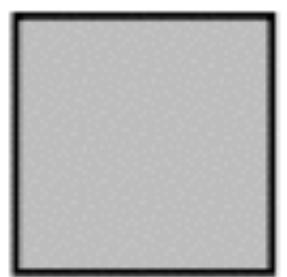
Public Ledger



Satoshi's Blockchain



Genesis Block



Orphaned blocks



Main blocks

Order From Crowds



A Closer Look



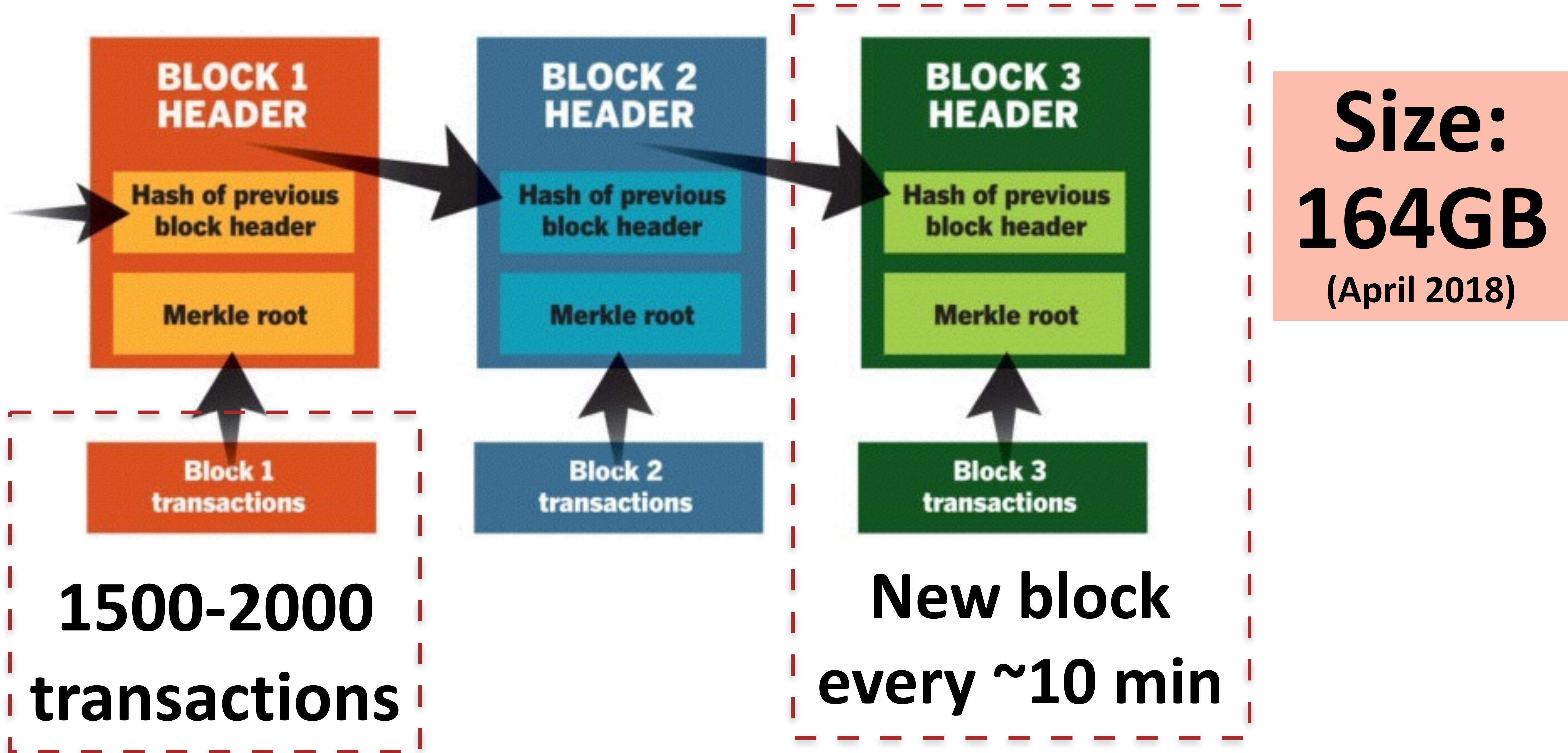
Bitcoin Statistics (April 2018)

Supply = ~17M bitcoins (BTC)

Demand = exchange rate: \$8000 USD per BTC

- \$137B in circulation (3.6% of US M0 money supply)
- Daily on-chain transactions: \$5B (3.5%)
- Daily mining: 144 “winners”, 1800 BTC, \$14.4M

Bitcoin Blockchain (Ledger!)



Block #132749: Header Data

Block Depth & Time

Height

132749 (Main Chain)

Timestamp

2011-06-23 06:50:15

Hashes

Lots of leading zeros...

Hashes

Hash

0000000000004bea72d0f390194b08162665a4fc99469c576338cd37164a15a

Previous Block

000000000000107de3a0e9fb1ea091780bcfef5ce4967efd86d536859f9e6b8a

Block #132749: Transactions

Transactions

f2ee93039126a28bd352e708bd67c2edaa10f0f2e18a9a1305129468fdf22b37

2011-06-23 06:50:15

No Inputs (Newly Generated Coins)



1KWFWpC4tmKQuhraK6XyAFz9ypKqFva4RH

50.10132691 BTC

Minning “winner” gets 50 BTC

50.10132691 BTC

3a1b9e330d32fef1ee42f8e86420d2be978bbe0dc5862f17da9027cf9e11f8c4

2011-06-23 06:50:15

17dxcM1cdeXPL1rZNJDAFwU2C4H9Xf5VqR
19H4PcfyPCw8FUh5J1pma5Bb9w2srhYcQ4
1LfddcwINnJ7Hk3KpBv5AfcTMD1fCahLqY
15oGga9EJ7BzdZxFnEcDxQDZvh1dHZ6Zco
1FfsbQntU2BAkVy2xaaRpSmLEDMEUwPbG1
1MtyGxTeWmjNhXyBf85JPKL5vrhTRJ7HnD
14yX4kRDME61BbM7DMnuv1PKUtk8K65J4y
191sZm1o7WZ1baNqUmRow6RPo293gbeJLW
1Q4EpJ6eaXDV1mEHx7JgupBuGNi4GBcMbV



1Hzpk4eXTbrAfmH2noWrkrhx6ewH6qncd
1eHhgW6vquBYhwMPhQ668HPjxTtpvZGPC

17,757.57575758 BTC
424,242.42424242 BTC

Transfer of 424 BTC

442,000 BTC

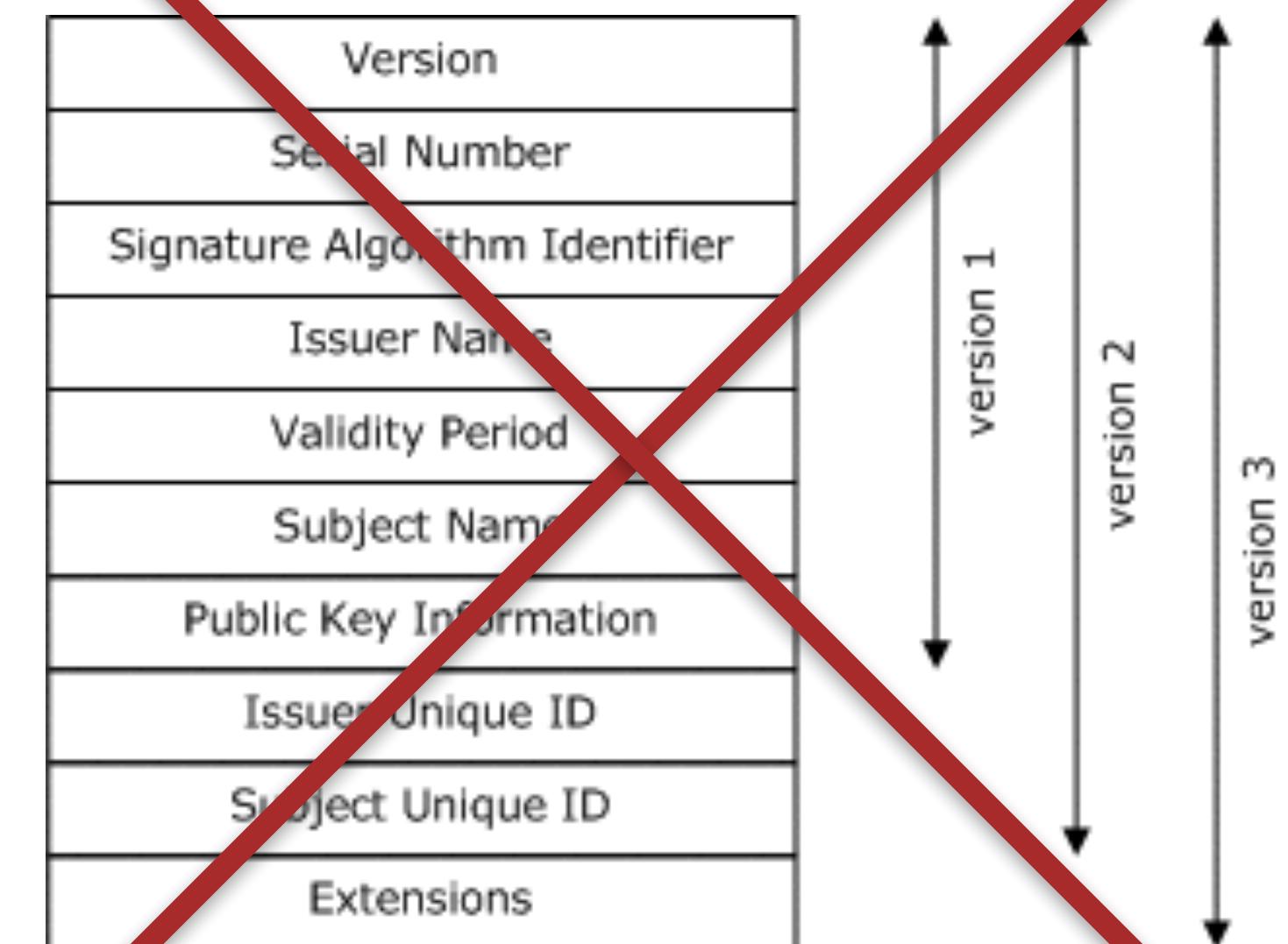
Identity (“Wallet”) Management

Bitcoin Address

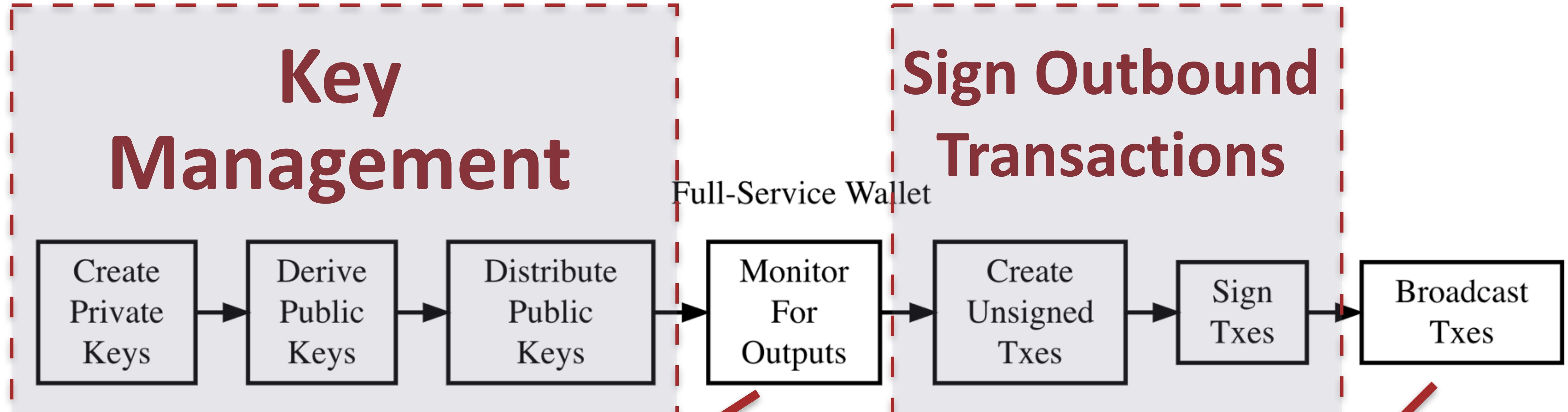
Summary		
Address	1eHhgW6vquBYhwMPhQ668HPjxTtpvZGPC	
Hash 160	070d550bc5bc843149410b8863b5b72857d91439	
Transactions		
No. Transactions	48	
Total Received	474,320.43446353 BTC	
Final Balance	0.00011111 BTC	



NOT
X.509



Wallet Operations



Monitor Blockchain
For Incoming BTC

Place Outbound
Transactions to Blockchain

Decentralized, Trustless, Transparent

Bitcoin is coordinated under policies set in motion by Satoshi in 2008. It has no central administrator and no governing body*.

*** These folks may want to talk to you:**

- *Securities and Exchange Commission*
- *Commodity Futures Trading Commission*
- *Internal Revenue Service*
- *US States*
- *Department of Treasury*

Post-Satoshi World



“Trust” and Enforcement

1. Fiat



REWARD
up to \$10,000

HOLLYWOOD MAIL THIEVES



The U.S. Postal Inspection Service is offering a reward of up to \$10,000 for information leading to the arrest and conviction of suspects who have been using a U.S. Postal Service master key to enter apartment complexes and steal U.S. Mail in the area of Franklin, La Brea, and Hawthorne of Hollywood, CA. The suspects were described as:

SUSPECT #1 – Male, possible Hispanic, mid to late 20s, approx. 5'6" to 5'9", medium build with goatee.

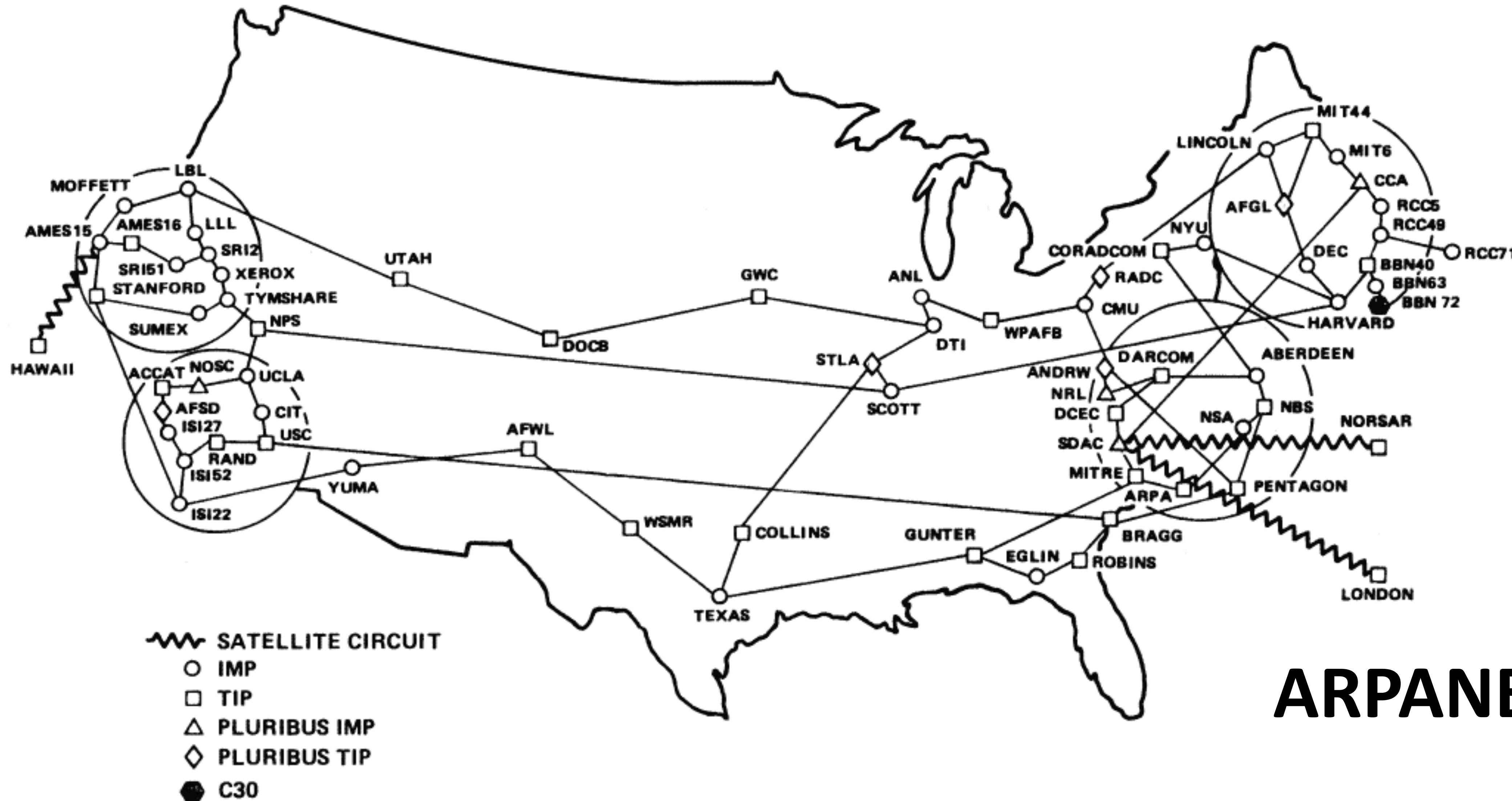
2. Guarantor



3. Consensus, Transparency



Internet-Scale Routing, Membership



ARPANET, 1980

Contract Virtualization



Satoshi's World

Bitcoin: A Peer-to-Peer Electronic Cash System (2008)

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 the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Peer-to-Peer

Digital Signatures

No Trusted Third Party

Decentralized

Chained Proof-of Work

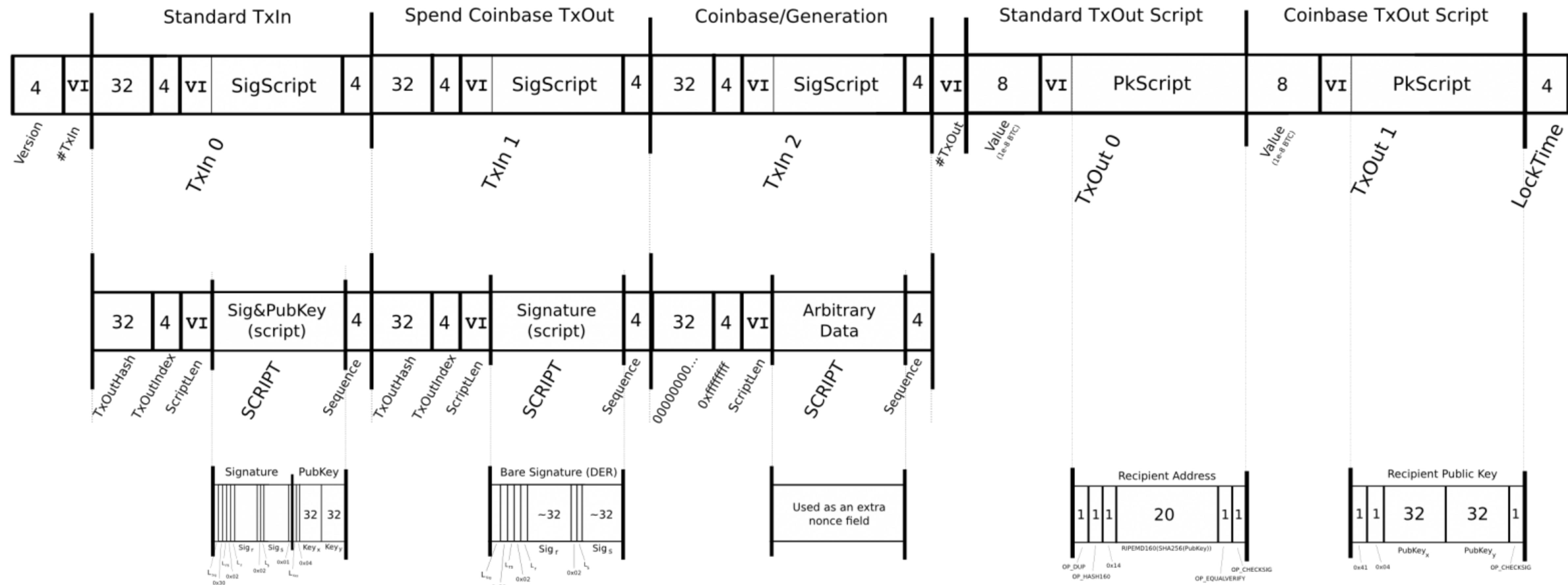


H V F

HVF Labs

ben@hvflabs.com

Transaction



Scripts and DER encoding both use big-endian values, all other serializations use little-endian