Making Bitcoin Exchanges Transparent

James Guthrie

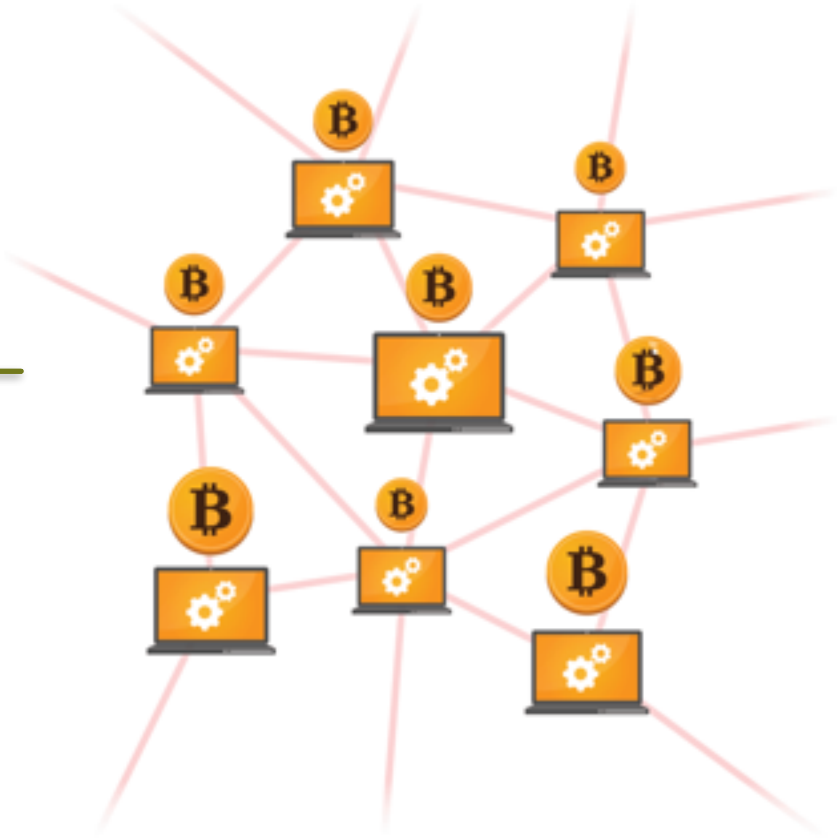
Christian Decker, Jochen Seidel, Roger Wattenhofer

Institut für Technische Informatik
und Kommunikationsnetze
Computer Engineering and Networks Laboratory

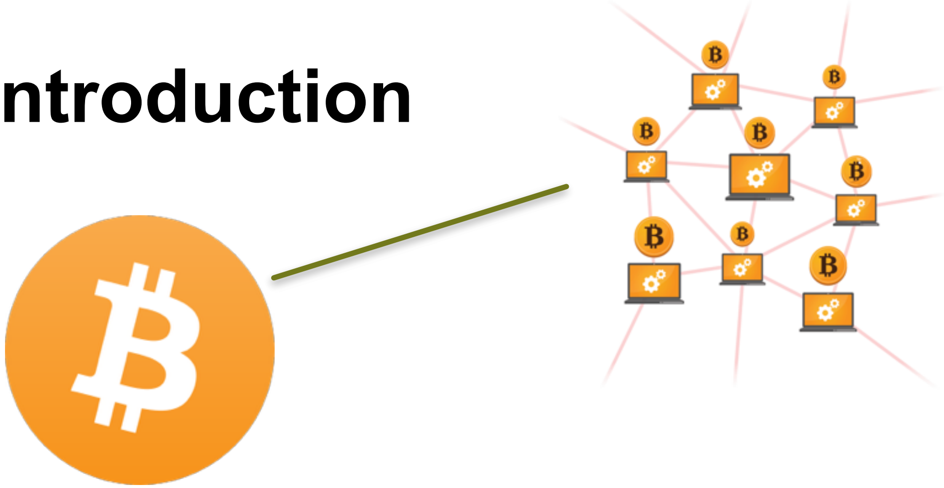
Introduction

Introduction

Introduction

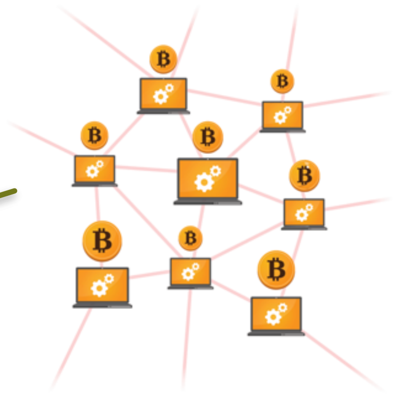


Introduction

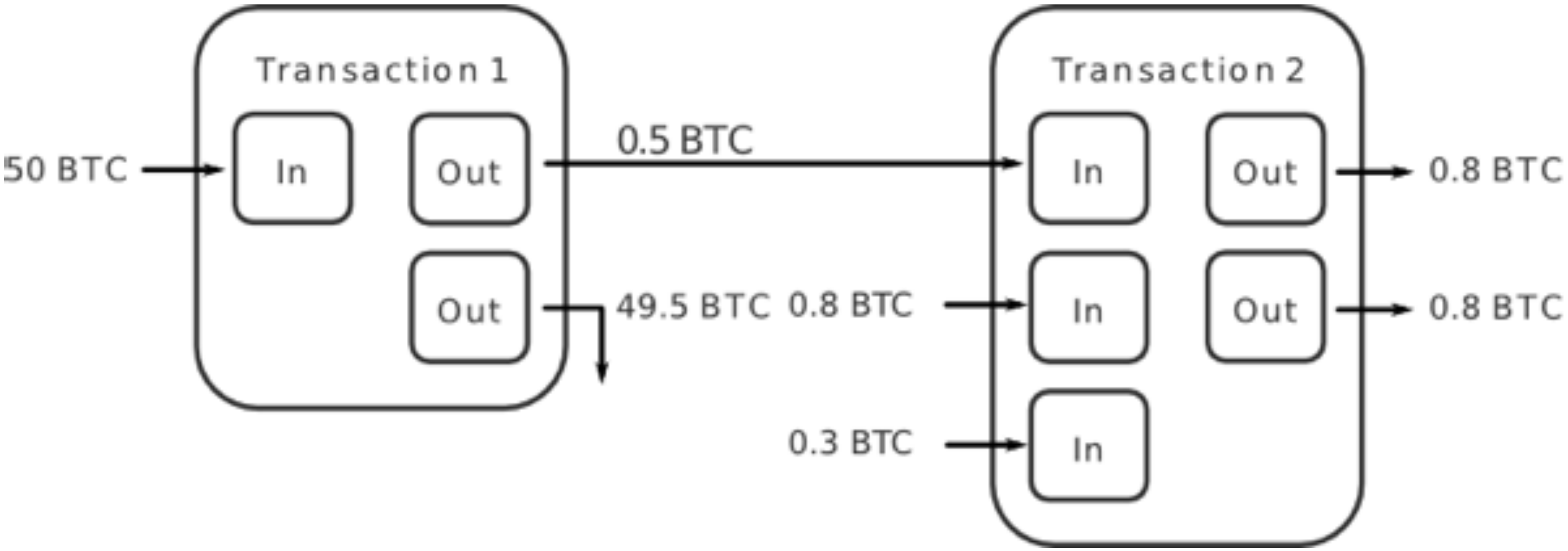


Peer to Peer

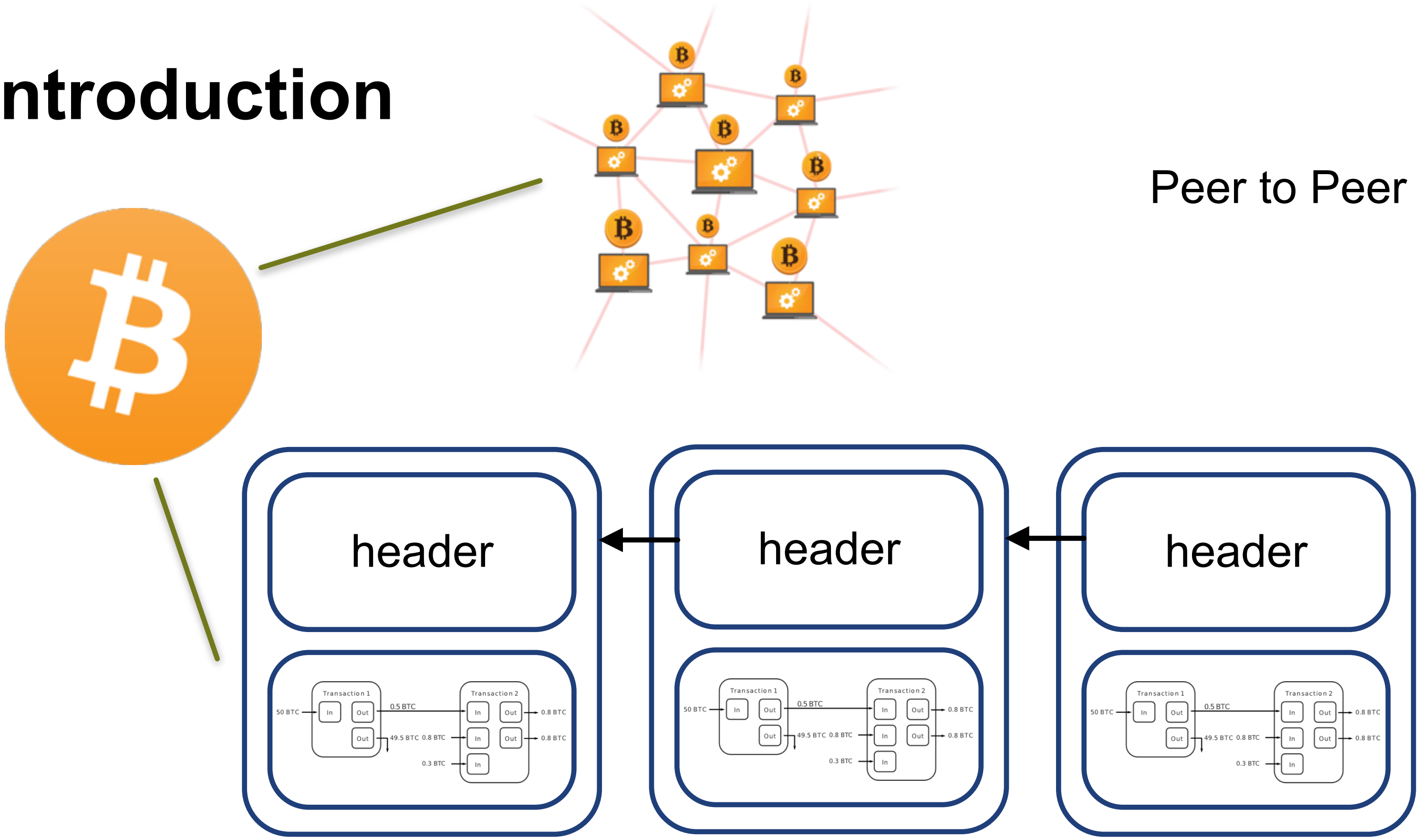
Introduction



Peer to Peer

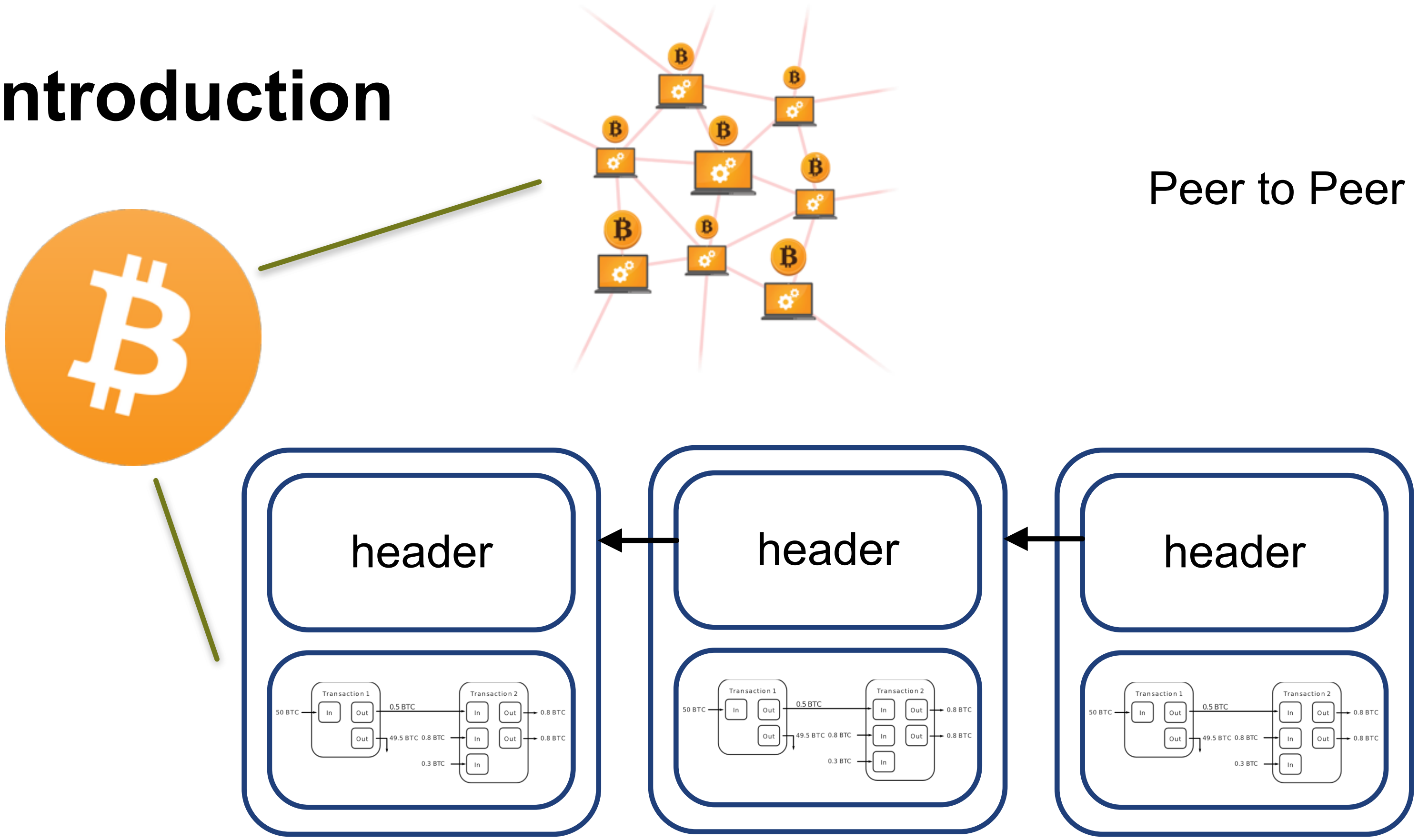


Introduction



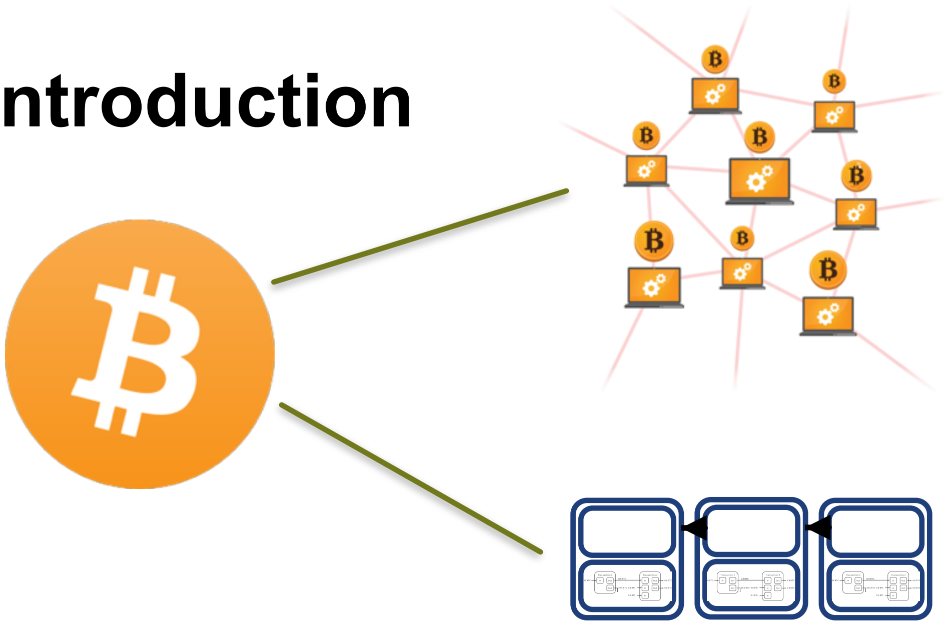
Peer to Peer

Introduction



Peer to Peer

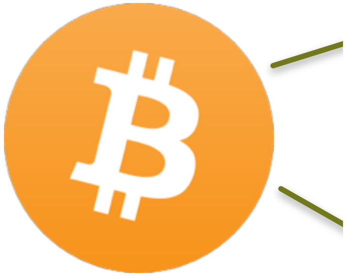
Introduction

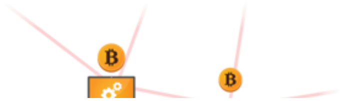


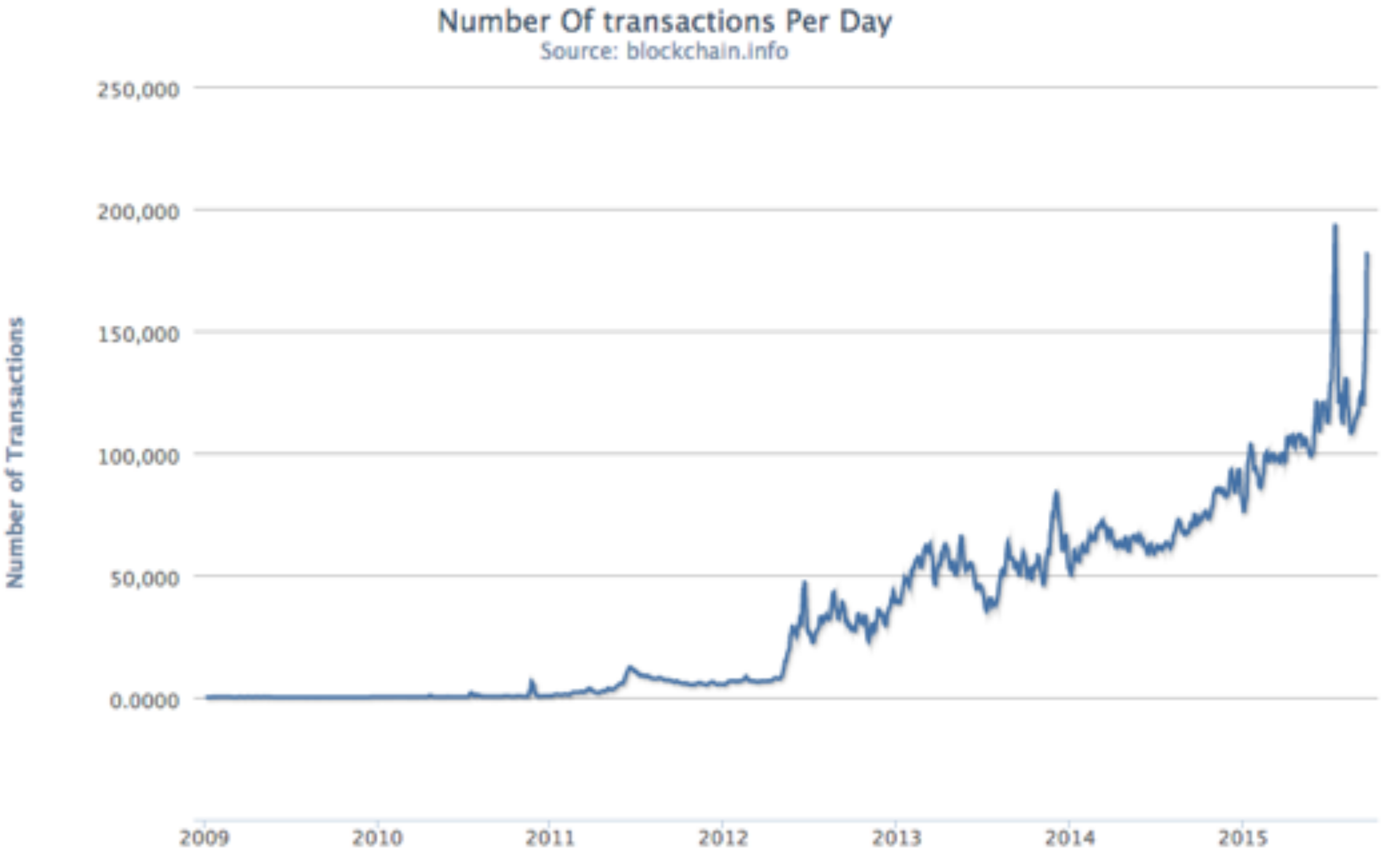
Peer to Peer

Transaction History

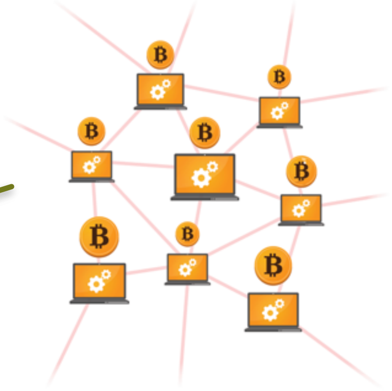
Introductio



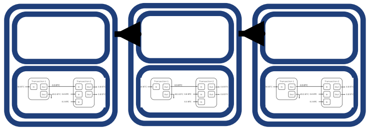




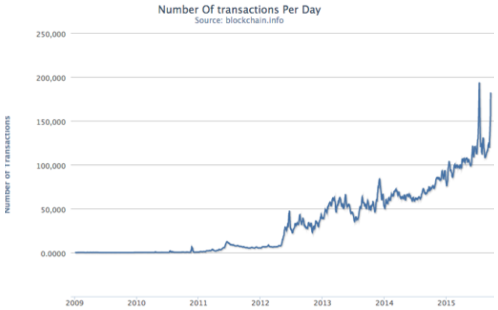
Introduction



Peer to Peer



Transaction History



Number Of transactions Per Day

Source: blockchain.info

Growth

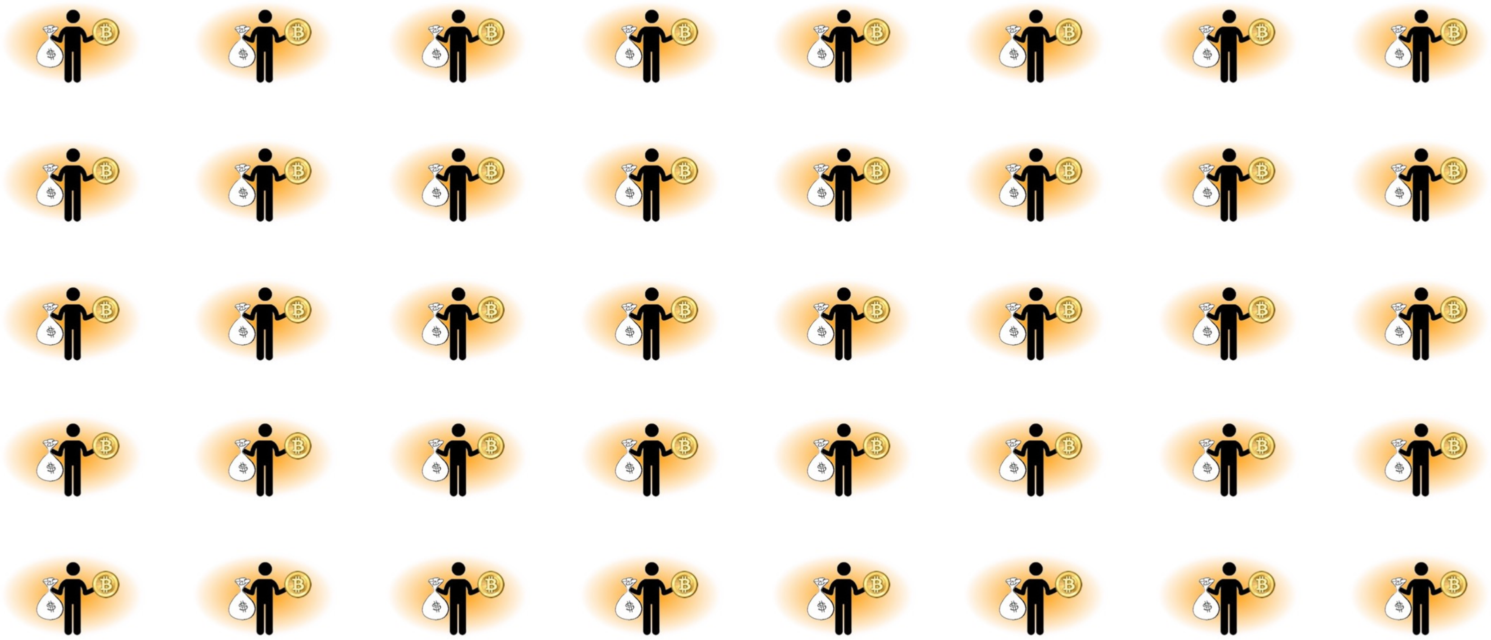
Bitcoin Exchanges

Buyers

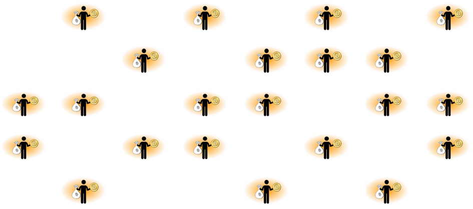
Exchange

Sellers

Trust in Bitcoin Exchanges



Trust in Bitcoin Exchanges

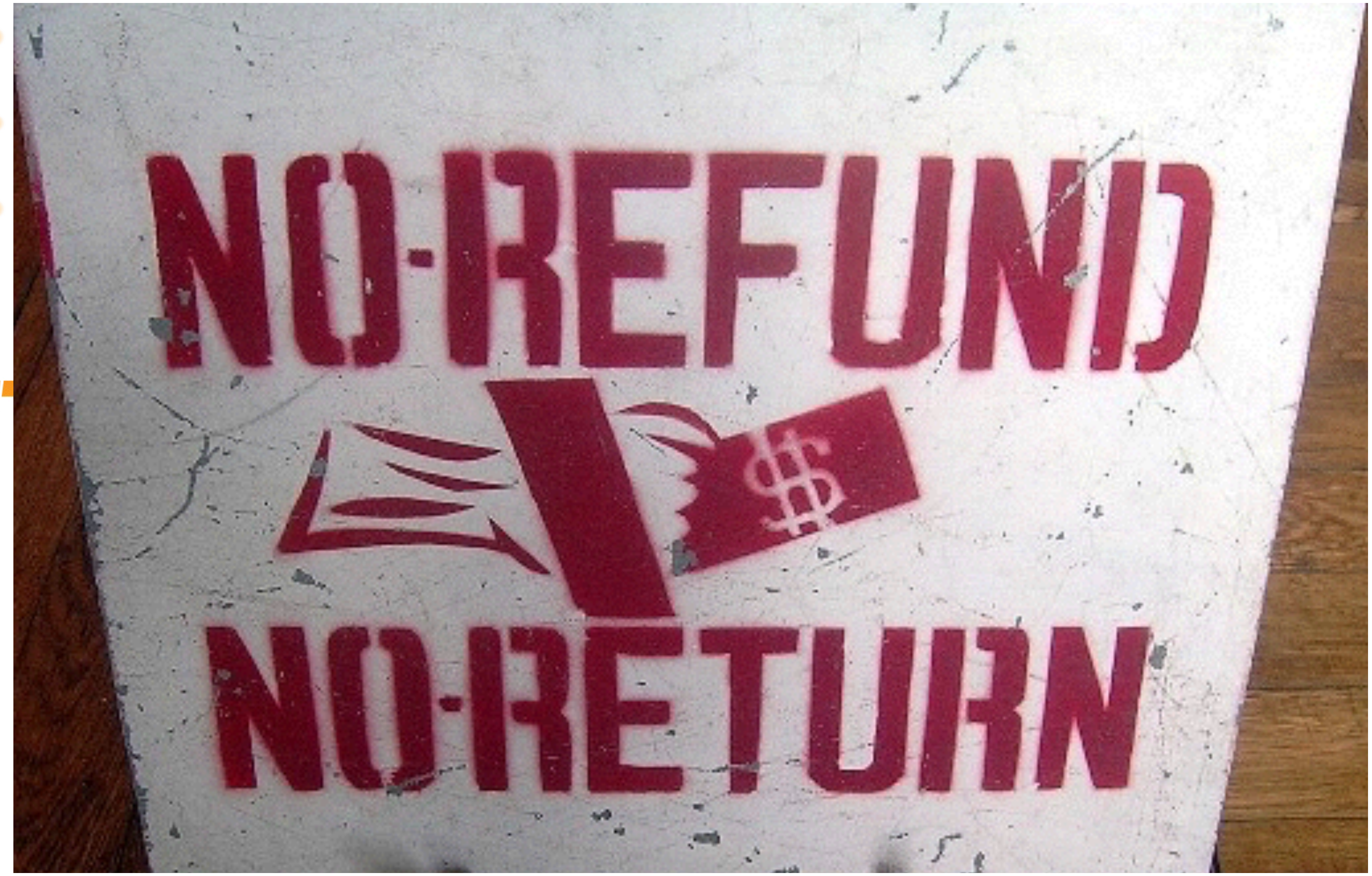


18 of 40 exchanges folded

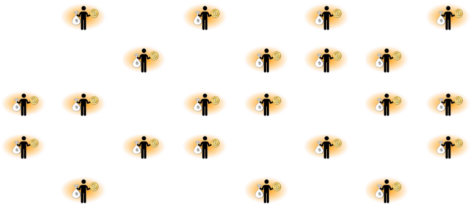
Trust in Bitcoin Exchanges

Trust in Bitcoin Exchanges

Trust in Bitcoin Exchanges



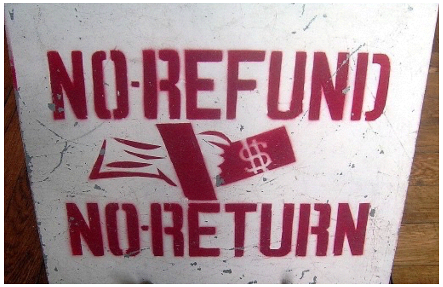
Trust in Bitcoin Exchanges



18 of 40 exchanges folded

MT.GOX

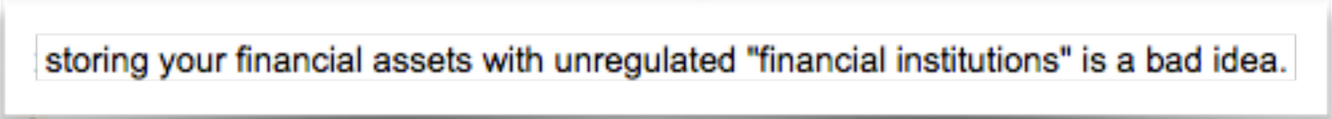
650k bitcoins lost/stolen



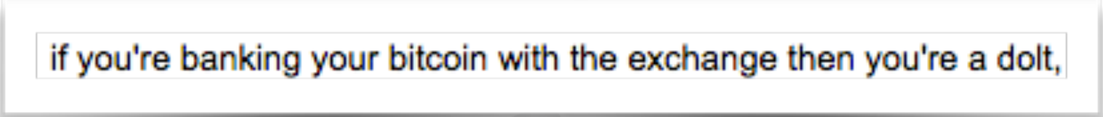
No higher power

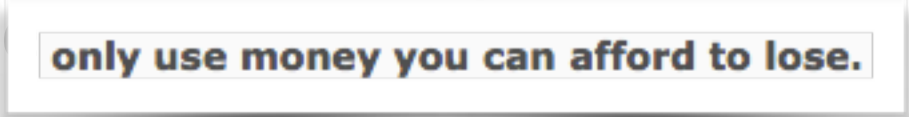
No help from law enforcement

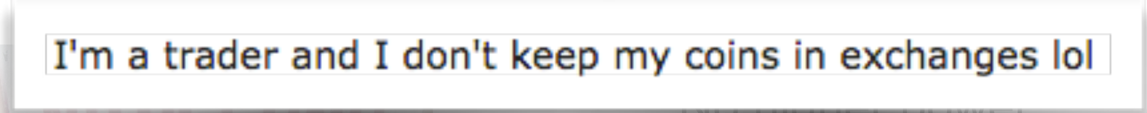
Trust in Bitcoin Exchanges


storing your financial assets with unregulated "financial institutions" is a bad idea.

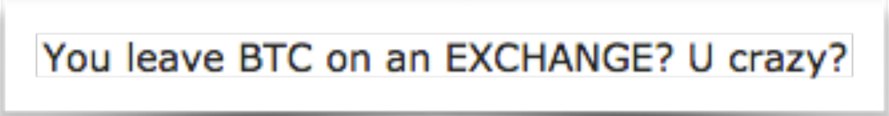
18 of 40 exchanges folded


if you're banking your bitcoin with the exchange then you're a dolt,

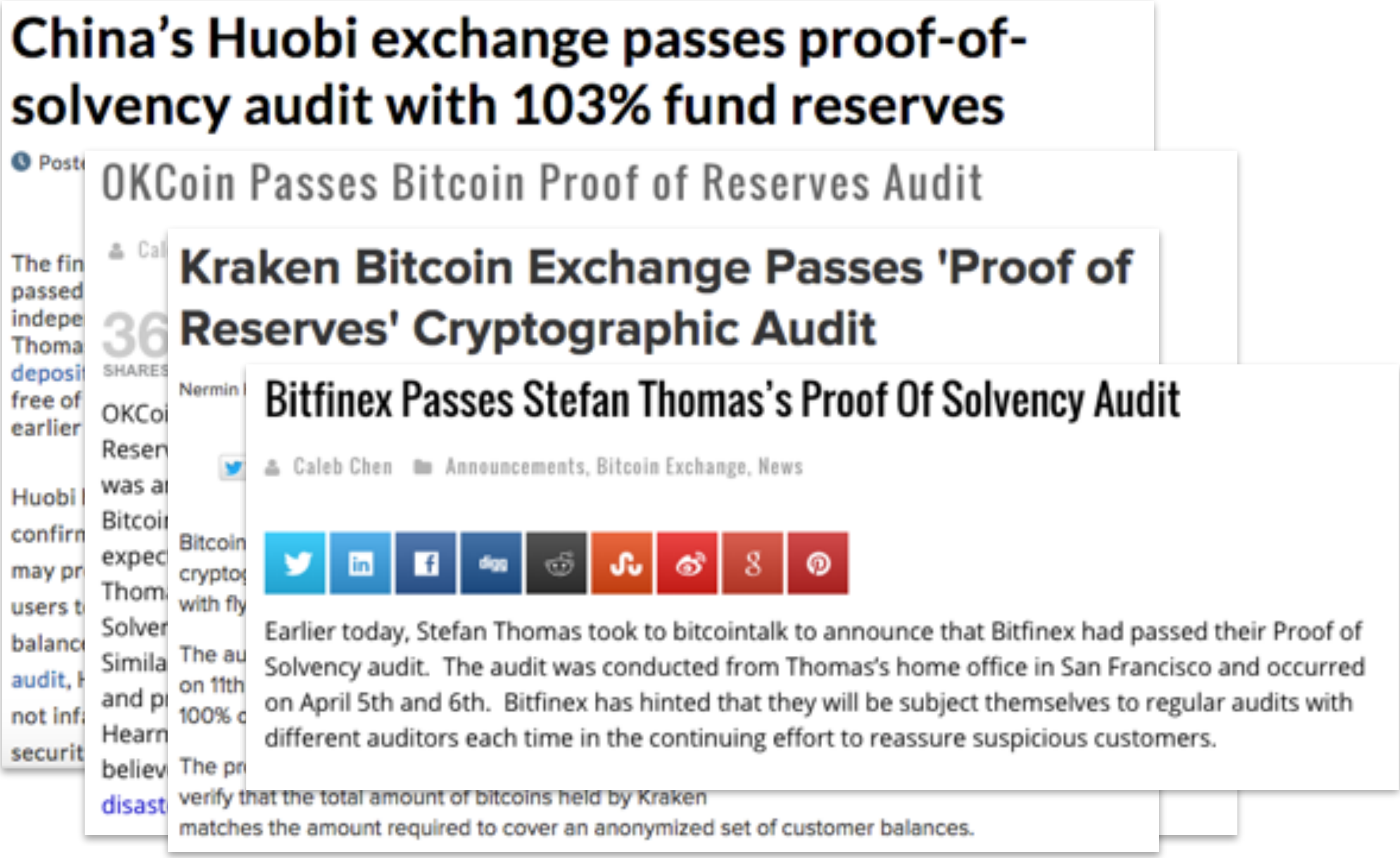

only use money you can afford to lose.


I'm a trader and I don't keep my coins in exchanges lol

No higher power


You leave BTC on an EXCHANGE? U crazy?

Legitimacy of Bitcoin Exchanges



China's Huobi exchange passes proof-of-solvency audit with 103% fund reserves

Post

The fir
passed
indepe
Thoma
deposi
free of
earlier

Huobi
confirm
may pr
users t
balanc
audit,
not inf
securit

OKCoin Passes Bitcoin Proof of Reserves Audit

Cal

36
SHARES

OKCoi
Reser
was a
Bitcoi
expec
Thom
Solver
Simila
and p
Hearn
believ
disast

Kraken Bitcoin Exchange Passes 'Proof of Reserves' Cryptographic Audit

Nermin

Bitcoin
crypto
with fly

The au
on 11th
100% c

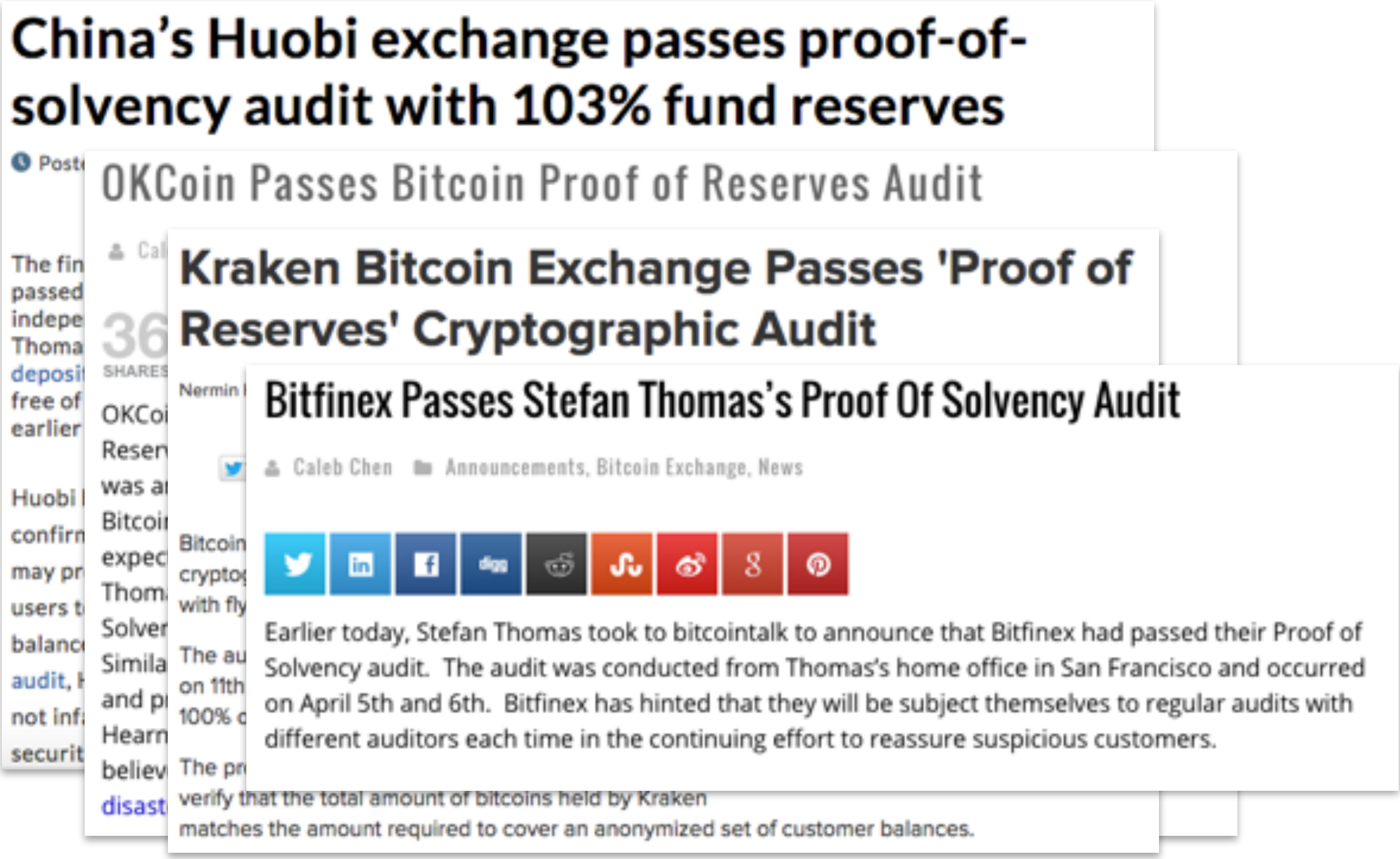
The pr
verify that the total amount of bitcoins held by Kraken matches the amount required to cover an anonymized set of customer balances.

Bitfinex Passes Stefan Thomas's Proof Of Solvency Audit

Caleb Chen Announcements, Bitcoin Exchange, News

Earlier today, Stefan Thomas took to bitcointalk to announce that Bitfinex had passed their Proof of Solvency audit. The audit was conducted from Thomas's home office in San Francisco and occurred on April 5th and 6th. Bitfinex has hinted that they will be subject themselves to regular audits with different auditors each time in the continuing effort to reassure suspicious customers.

Legitimacy of Bitcoin Exchanges



China's Huobi exchange passes proof-of-solvency audit with 103% fund reserves

Post

The fin
passed
indepe
Thoma
deposi
free of
earlier

Huobi
confirn
may pr
users t
balanc
audit,
not inf
securit

OKCoin Passes Bitcoin Proof of Reserves Audit

Cal

36 SHARES

OKCoi
Reser
was a
Bitcoi
expec
Thom
Solver
Simila
and p
Hearn
believ
disast

Kraken Bitcoin Exchange Passes 'Proof of Reserves' Cryptographic Audit

Nermin

Bitcoin
cryptog
with fly

The au
on 11th
100% c

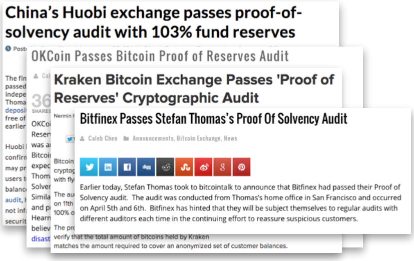
The pr
verify that the total amount of bitcoins held by Kraken matches the amount required to cover an anonymized set of customer balances.

Bitfinex Passes Stefan Thomas's Proof Of Solvency Audit

Caleb Chen   Announcements, Bitcoin Exchange, News

Earlier today, Stefan Thomas took to bitcointalk to announce that Bitfinex had passed their Proof of Solvency audit. The audit was conducted from Thomas's home office in San Francisco and occurred on April 5th and 6th. Bitfinex has hinted that they will be subject themselves to regular audits with different auditors each time in the continuing effort to reassure suspicious customers.

Legitimacy of Bitcoin Exchanges



China’s Huobi exchange passes proof-of-solvency audit with 103% fund reserves

OKCoin Passes Bitcoin Proof of Reserves Audit

Kraken Bitcoin Exchange Passes 'Proof of Reserves' Cryptographic Audit

verify that the total amount of bitcoins held by Kraken matches the amount required to cover an anonymized set of customer balances.

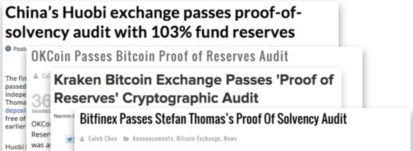
Bitfinex Passes Stefan Thomas’s Proof Of Solvency Audit

Caleb Chen Announcements, Bitcoin Exchange, News

Earlier today, Stefan Thomas took to bitcointalk to announce that Bitfinex had passed their Proof of Solvency audit. The audit was conducted from Thomas’s home office in San Francisco and occurred on April 5th and 6th. Bitfinex has hinted that they will be subject themselves to regular audits with different auditors each time in the continuing effort to reassure suspicious customers.

Third-party audit

Legitimacy of Bitcoin Exchanges



China's Huobi exchange passes proof-of-solvency audit with 103% fund reserves

OKCoin Passes Bitcoin Proof of Reserves Audit

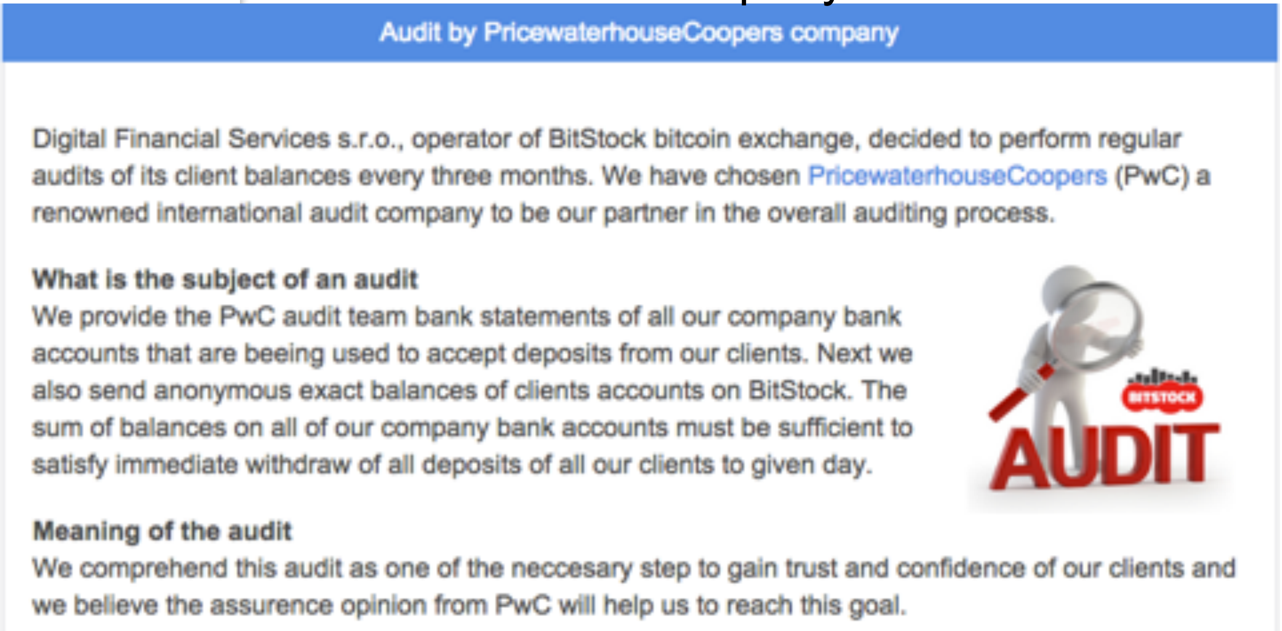
Kraken Bitcoin Exchange Passes 'Proof of Reserves' Cryptographic Audit

Bitfinex Passes Stefan Thomas's Proof Of Solvency Audit

Caleb Chen Announcements, Bitcoin Exchange, News

Earlier today, Stefan Thomas
Solvency audit. The audit wa
on April 5th and 6th. Bitfine
different auditors each time

Third-party audit



Audit by PricewaterhouseCoopers company

Digital Financial Services s.r.o., operator of BitStock bitcoin exchange, decided to perform regular audits of its client balances every three months. We have chosen PricewaterhouseCoopers (PwC) a renowned international audit company to be our partner in the overall auditing process.

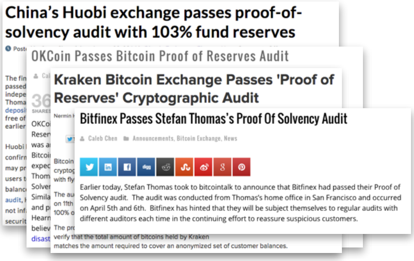
What is the subject of an audit

We provide the PwC audit team bank statements of all our company bank accounts that are beeing used to accept deposits from our clients. Next we also send anonymous exact balances of clients accounts on BitStock. The sum of balances on all of our company bank accounts must be sufficient to satisfy immediate withdraw of all deposits of all our clients to given day.

Meaning of the audit

We comprehend this audit as one of the neccesary step to gain trust and confidence of our clients and we believe the assurence opinion from PwC will help us to reach this goal.

Legitimacy of Bitcoin Exchanges



China's Huobi exchange passes proof-of-solvency audit with 103% fund reserves

OKCoin Passes Bitcoin Proof of Reserves Audit

Kraken Bitcoin Exchange Passes 'Proof of Reserves' Cryptographic Audit

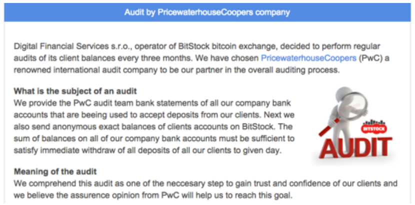
verify that the total amount of bitcoins held by Kraken matches the amount required to cover an anonymized set of customer balances.

Bitfinex Passes Stefan Thomas's Proof Of Solvency Audit

Caleb Chen Announcements, Bitcoin Exchange, News

Earlier today, Stefan Thomas took to bitcointalk to announce that Bitfinex had passed their Proof of Solvency audit. The audit was conducted from Thomas's home office in San Francisco and occurred on April 5th and 6th. Bitfinex has hinted that they will be subject themselves to regular audits with different auditors each time in the continuing effort to reassure suspicious customers.

Third-party audit



Audit by PricewaterhouseCoopers company

Digital Financial Services s.r.o., operator of BitStock bitcoin exchange, decided to perform regular audits of its client balances every three months. We have chosen PricewaterhouseCoopers (PwC) a renowned international audit company to be our partner in the overall auditing process.

What is the subject of an audit
We provide the PwC audit team bank statements of all our company bank accounts that are beeing used to accept deposits from our clients. Next we also send anonymous exact balances of clients accounts on BitStock. The sum of balances on all of our company bank accounts must be sufficient to satisfy immediate withdraw of all deposits of all our clients to given day.

Meaning of the audit
We comprehend this audit as one of the neccesary step to gain trust and confidence of our clients and we believe the assurence opinion from PwC will help us to reach this goal.

Renowned third-party audit (PwC)

Trust in third party 👎 Cost 👎 Frequency 👎 Privacy 👎

Automated Software-Based Audit

≥

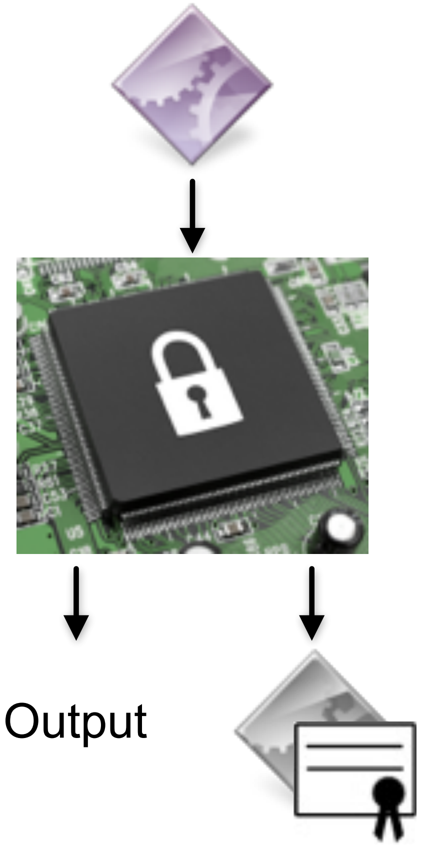
Solvency

Assets

Liabilities

Privacy

Trusted Computing

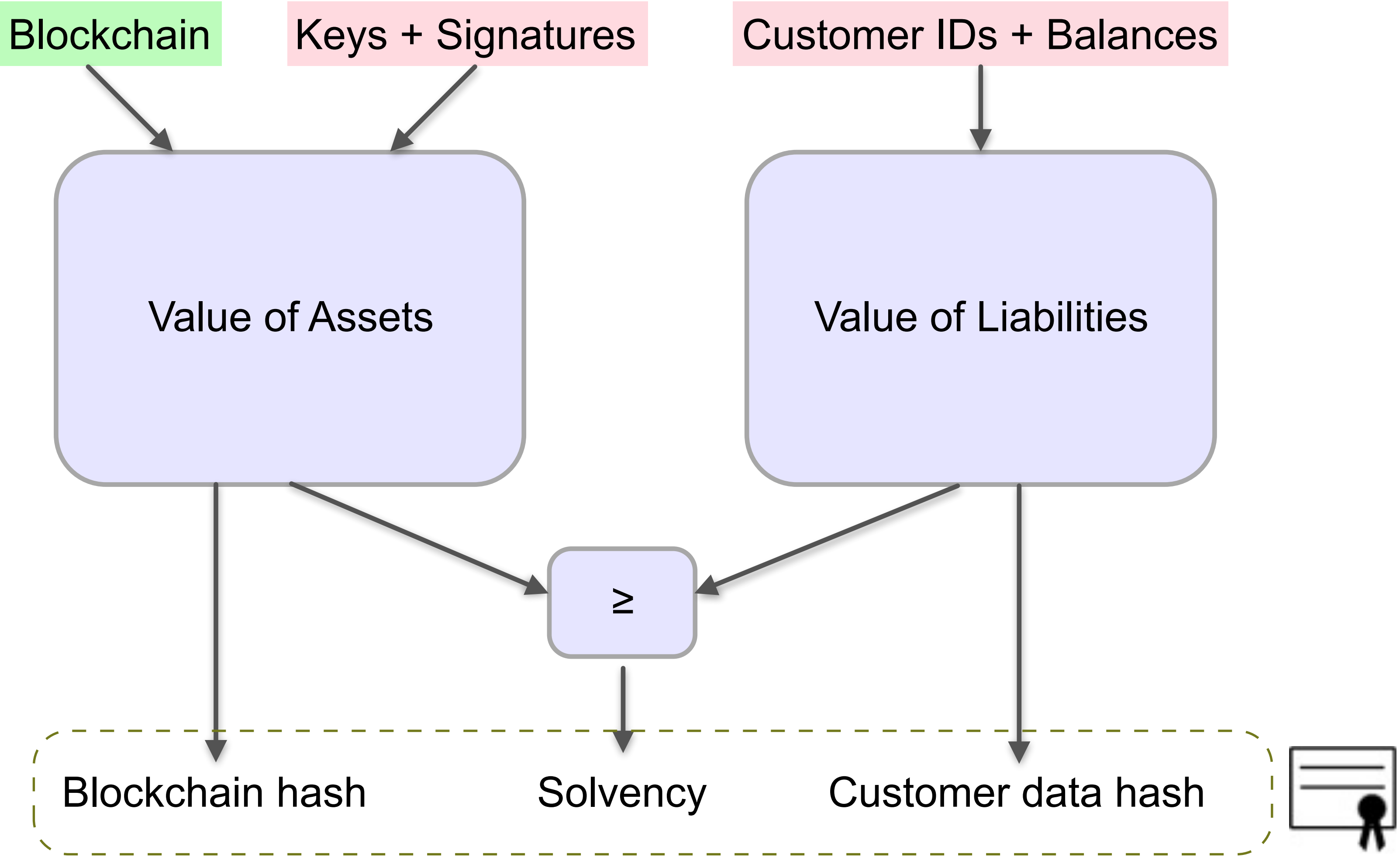


Executable

Trusted Execution

Result + Proof of Execution

Overview of Audit Process



Blockchain

Keys + Signatures

Customer IDs + Balances

Value of Assets

Value of Liabilities

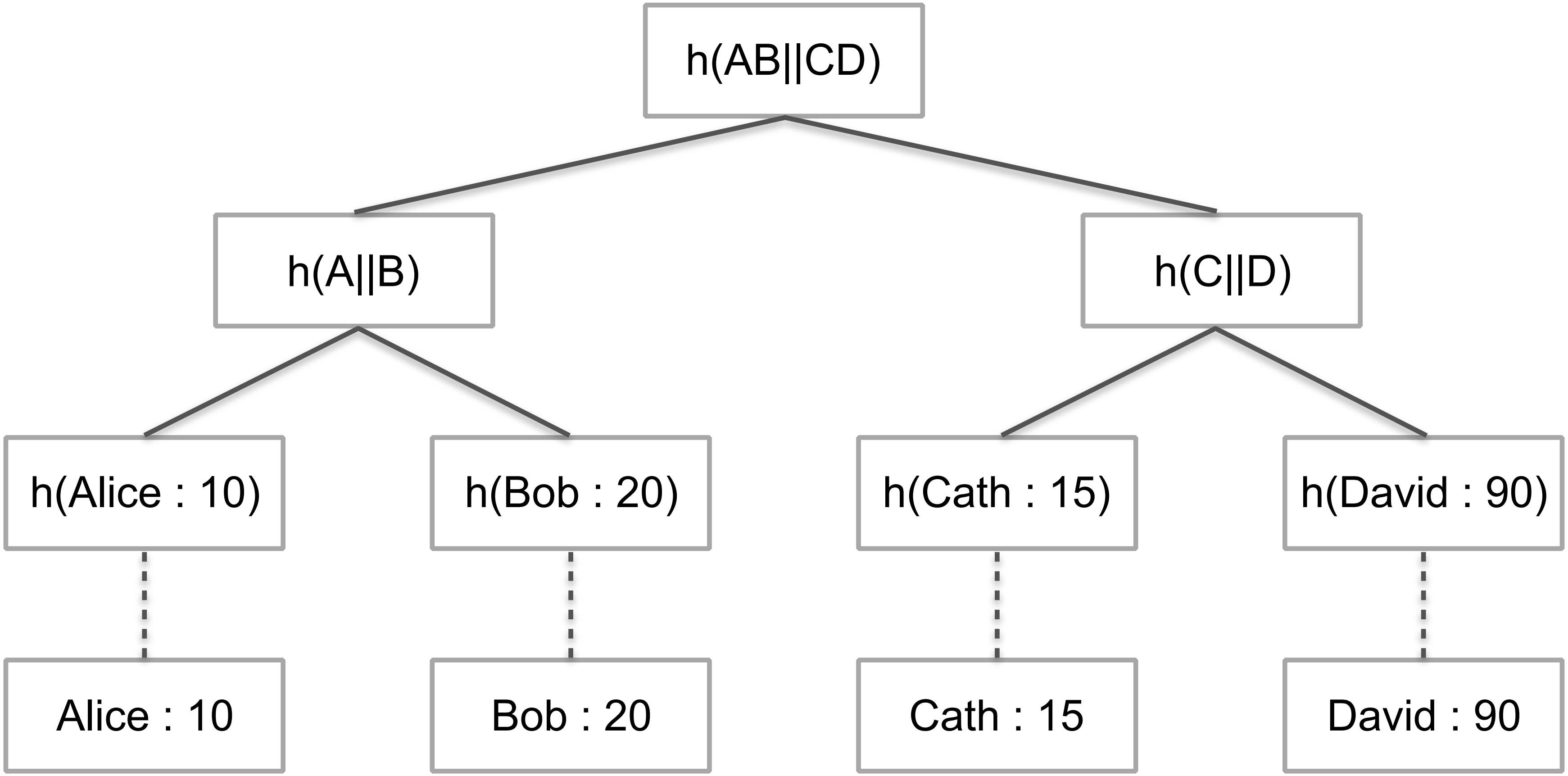
≥

Blockchain hash

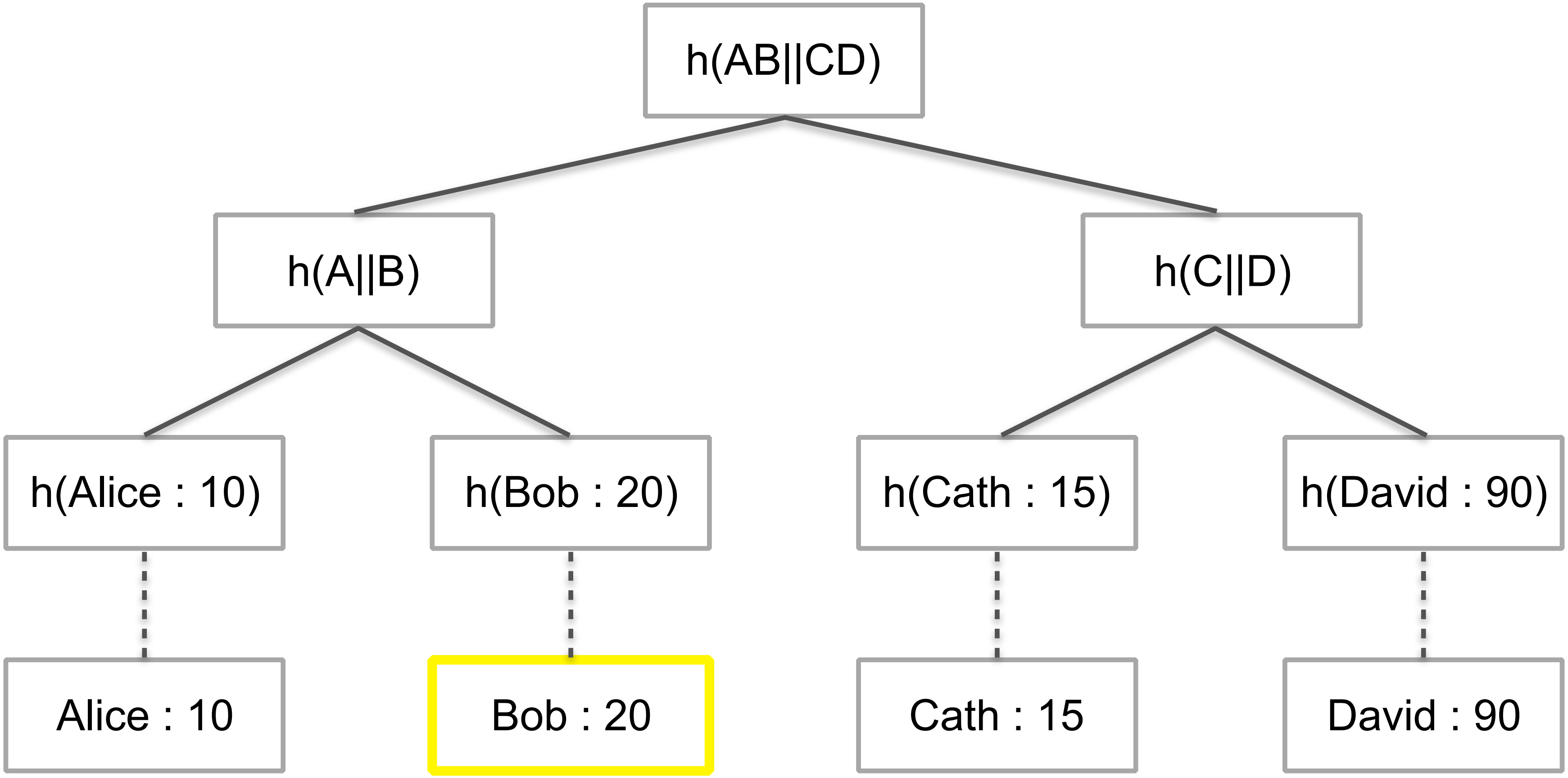
Solvency

Customer data hash

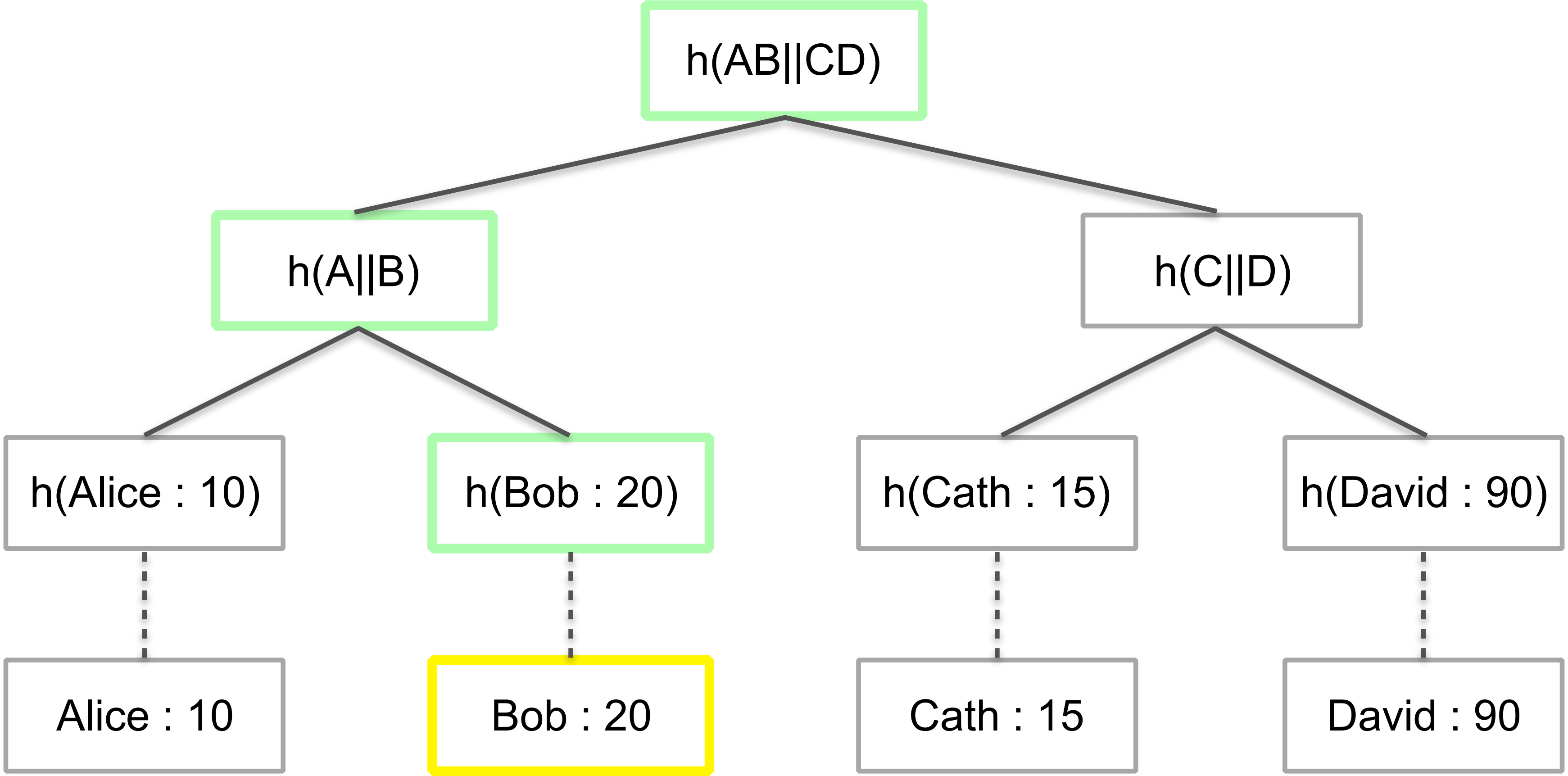
Customer Verification



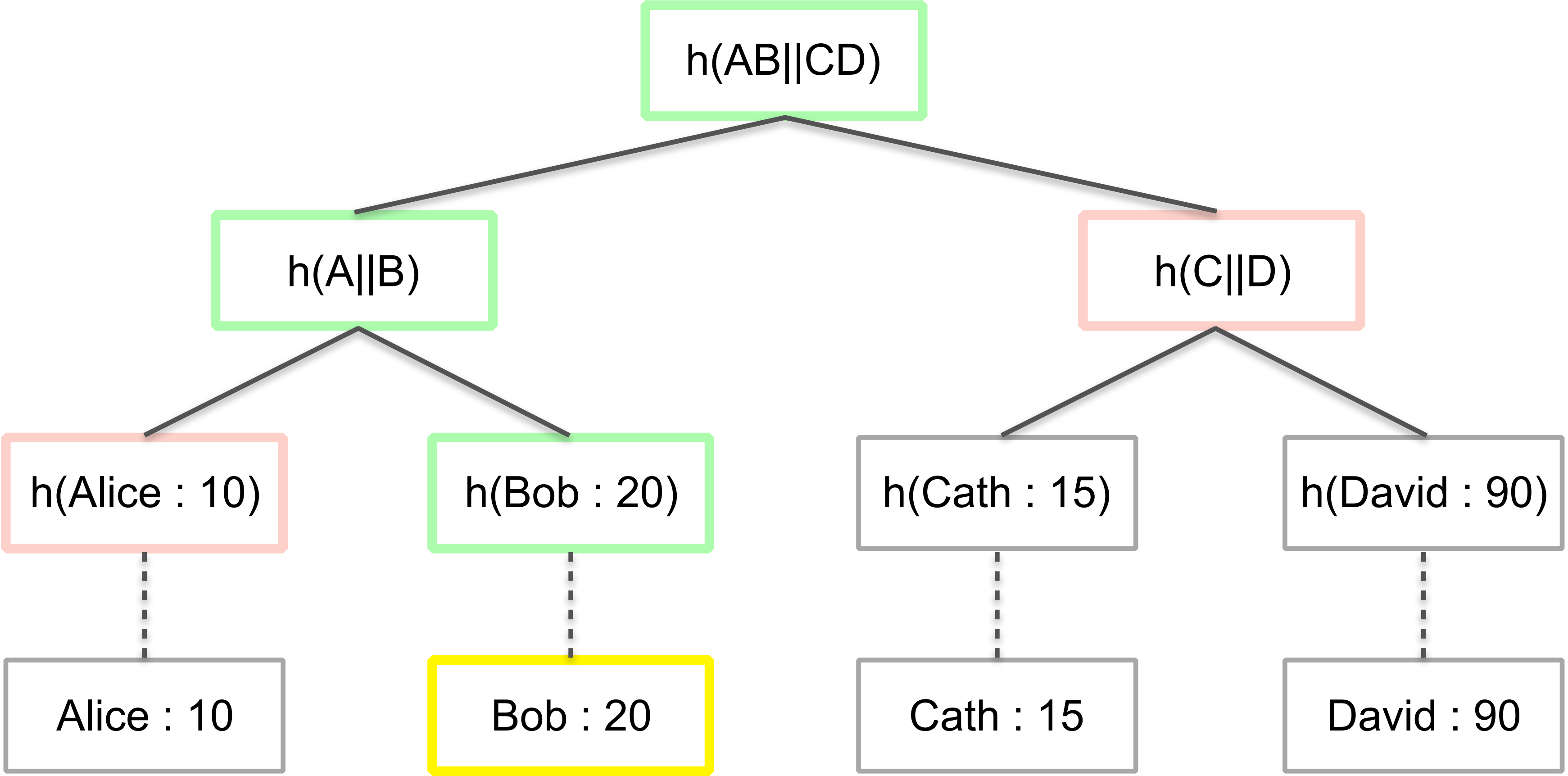
Customer Verification



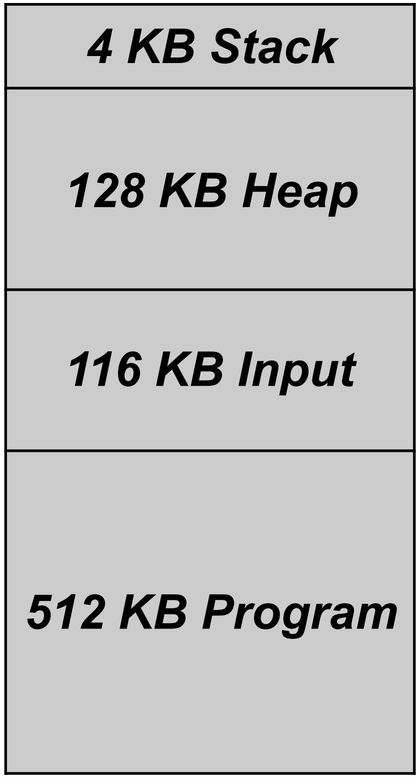
Customer Verification



Customer Verification



Limitations of Trusted Execution Platform



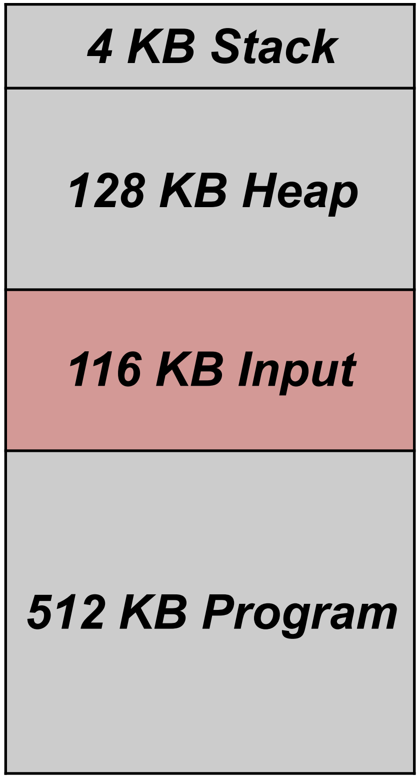
4 KB Stack

128 KB Heap

116 KB Input

512 KB Program

Limitations of Trusted Execution Platform



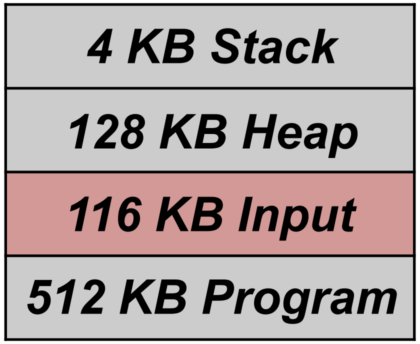
4 KB Stack

128 KB Heap

116 KB Input

512 KB Program

Limitations of Trusted Execution Platform

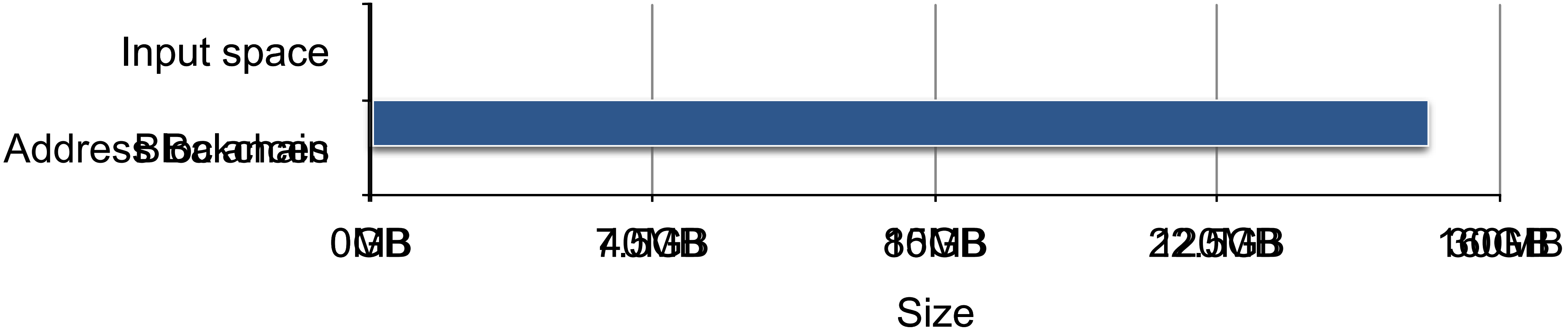


4 KB Stack

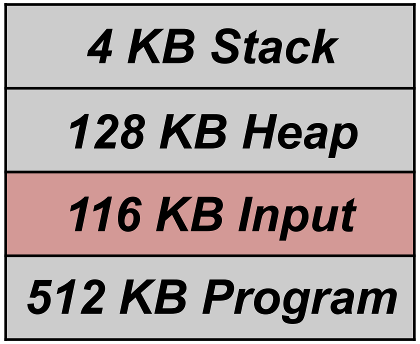
128 KB Heap

116 KB Input

512 KB Program



Limitations of Trusted Execution Platform



4 KB Stack

128 KB Heap

116 KB Input

512 KB Program

Memory constraints

Limitations of Trusted Execution Platform

4 KB Stack
128 KB Heap
116 KB Input
512 KB Program

aints

Limitations of Trusted Execution Platform

4 KB Stack

128 KB Heap

116 KB Input

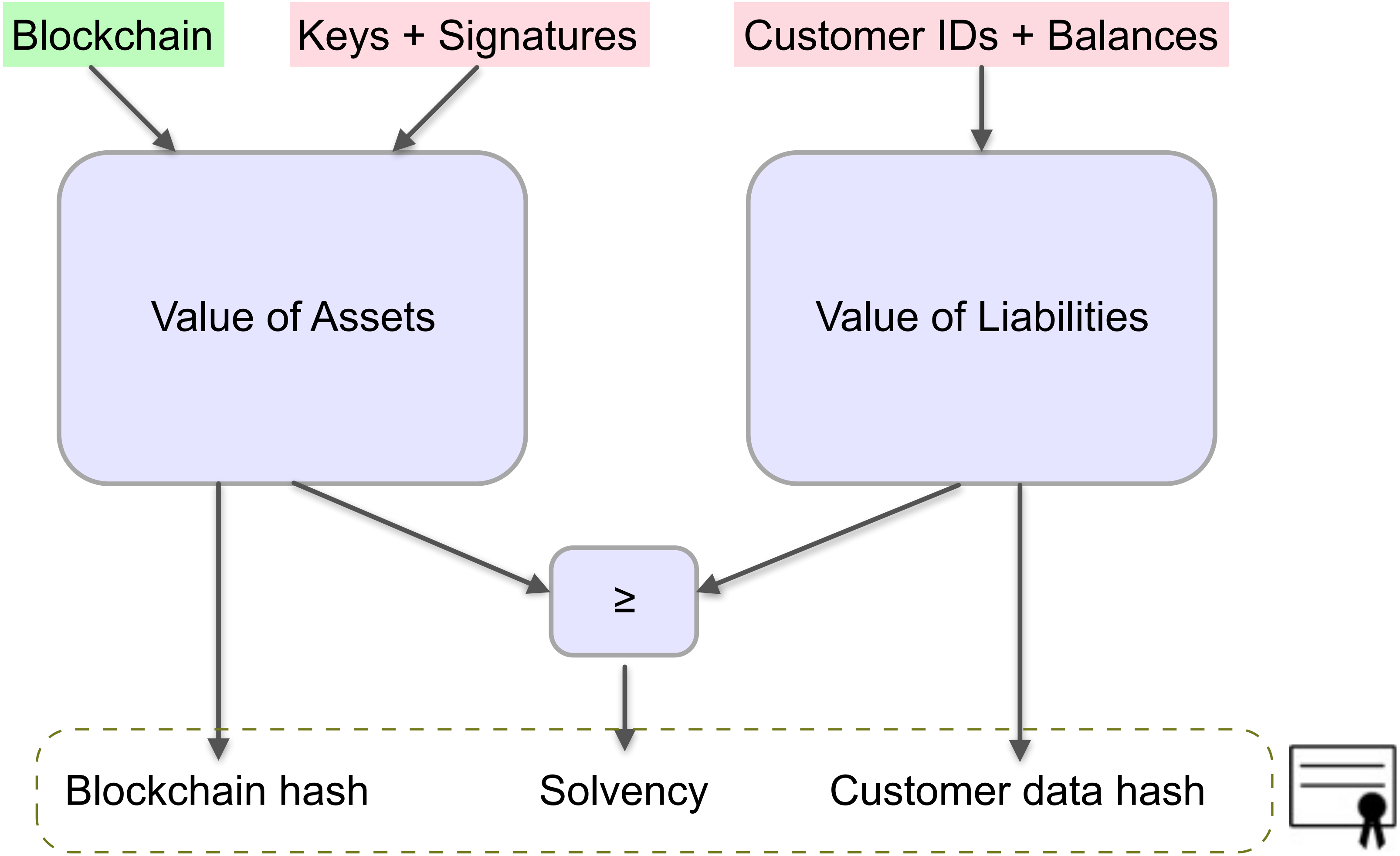
512 KB Program

Memory constraints

Time constraints

- 200ms-1s overhead
- 0.5-1s cooldown

Overview of Audit Process



Blockchain

Keys + Signatures

Customer IDs + Balances

Value of Assets

Value of Liabilities

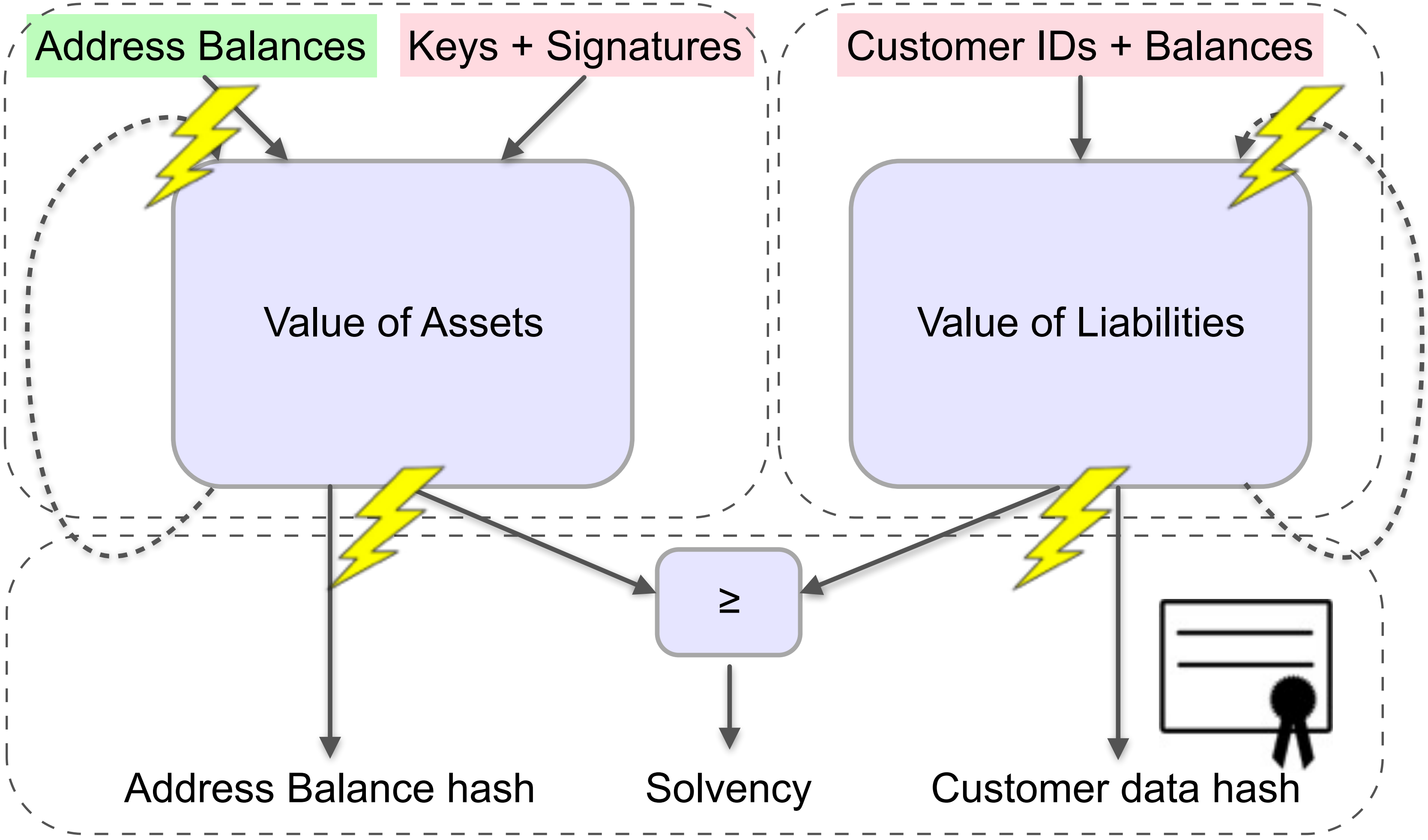
≥

Blockchain hash

Solvency

Customer data hash

Overview of Audit Process



Address Balances

Keys + Signatures

Customer IDs + Balances

Value of Assets

Value of Liabilities

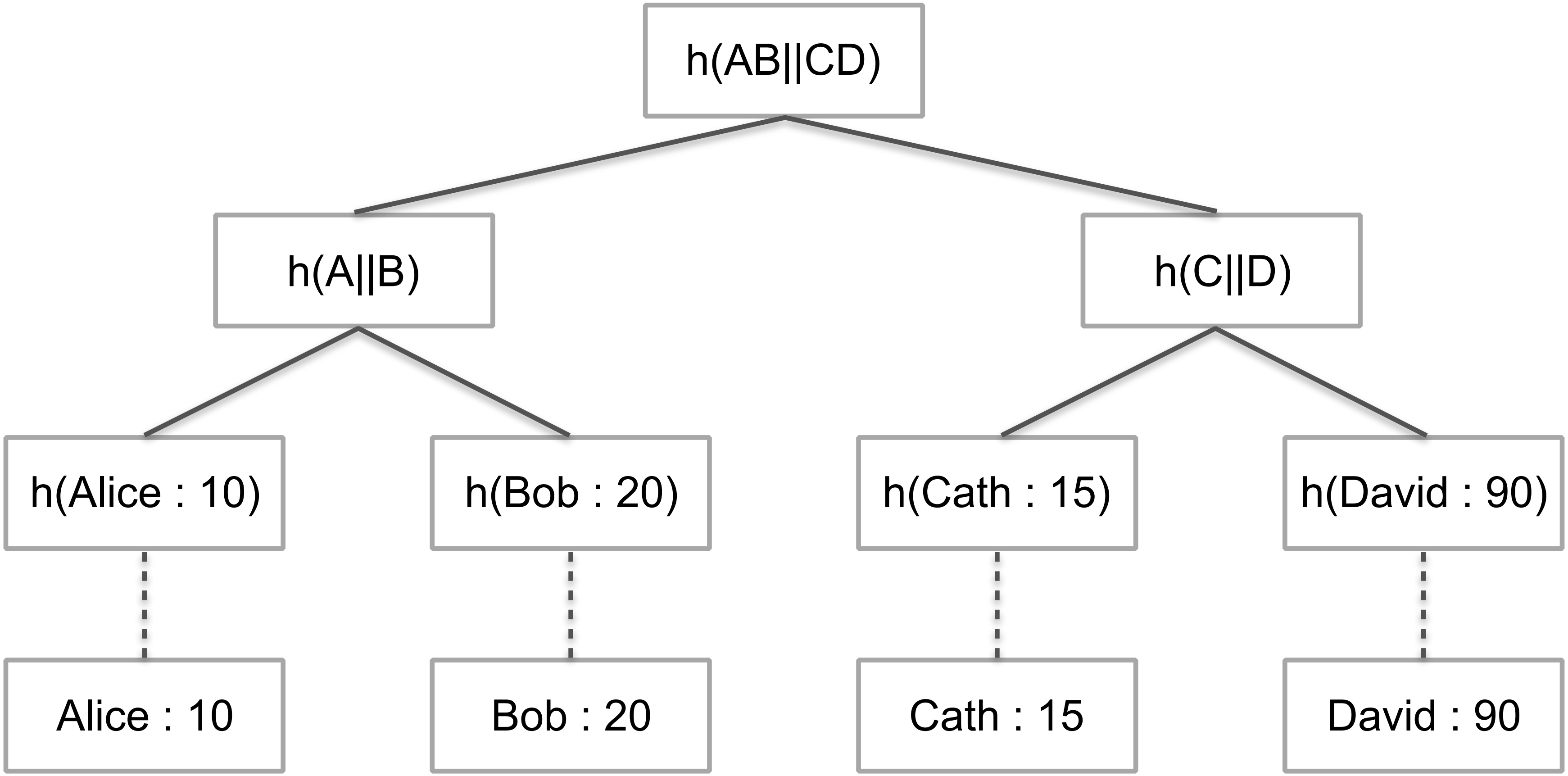
≥

Address Balance hash

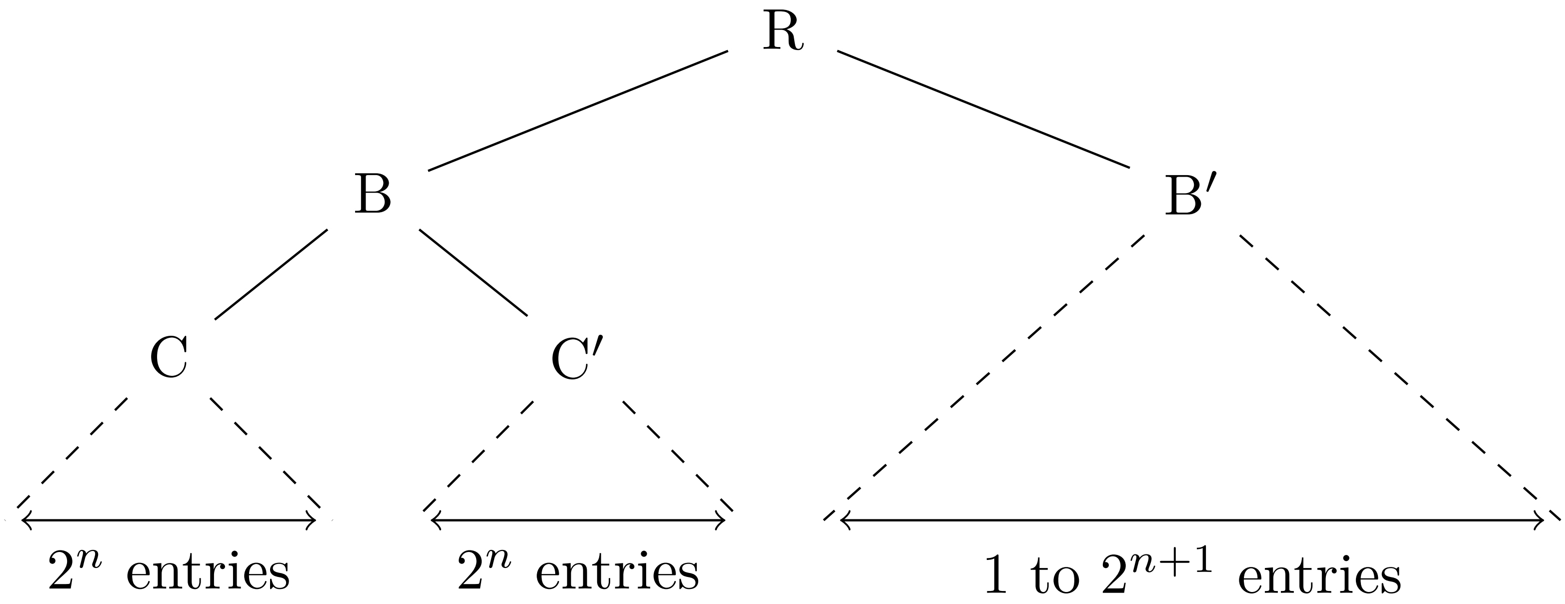
Solvency

Customer data hash

Iterative Customer Verification



Iterative Merkle Tree



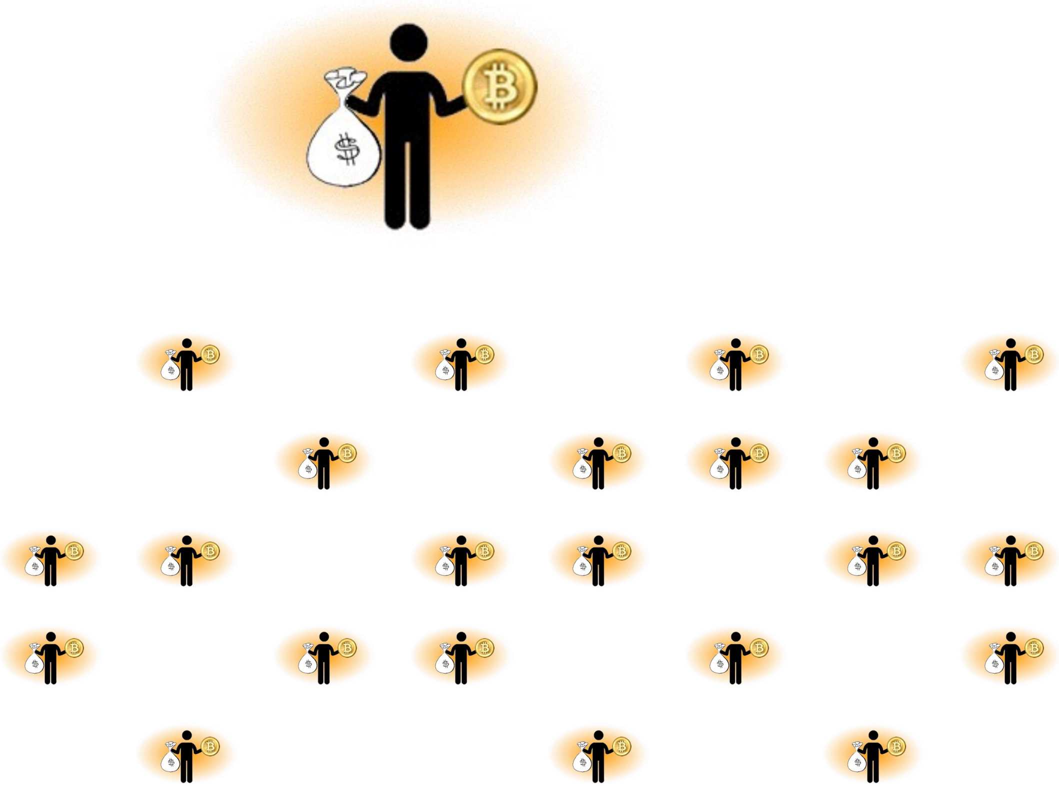
Summary

Summary

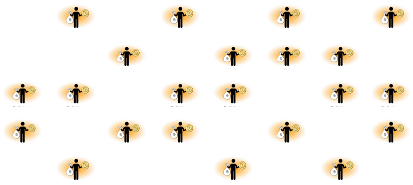
Summary

Summary

Summary



Summary



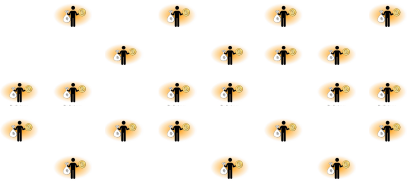
Summary

≥

Assets

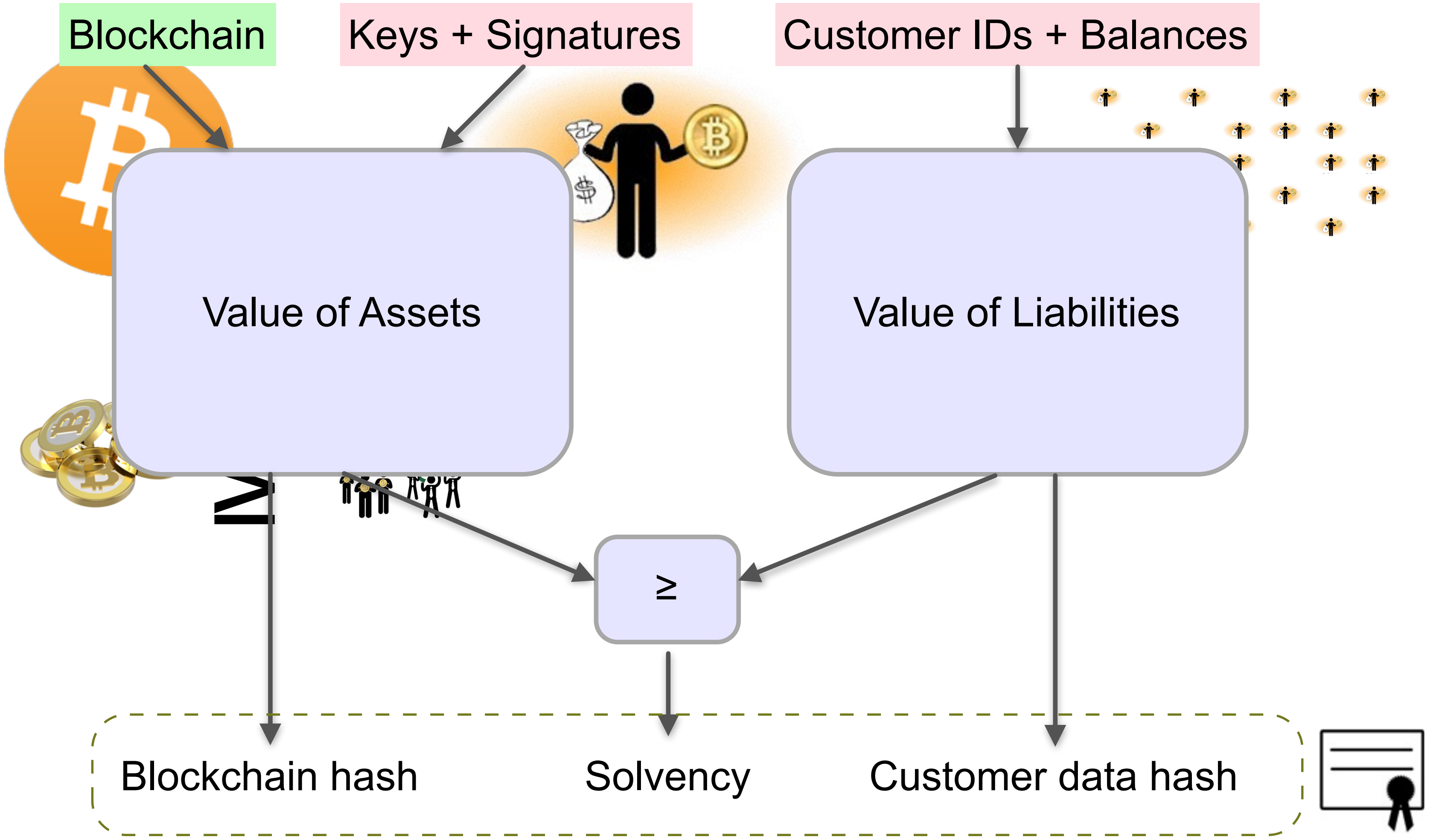
Liabilities

Summary



≥

Summary



Blockchain

Keys + Signatures

Customer IDs + Balances

Value of Assets

Value of Liabilities

≥

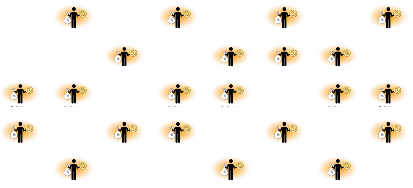
≥

Blockchain hash

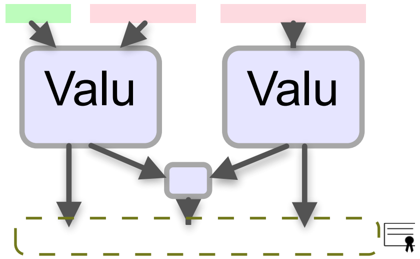
Solvency

Customer data hash

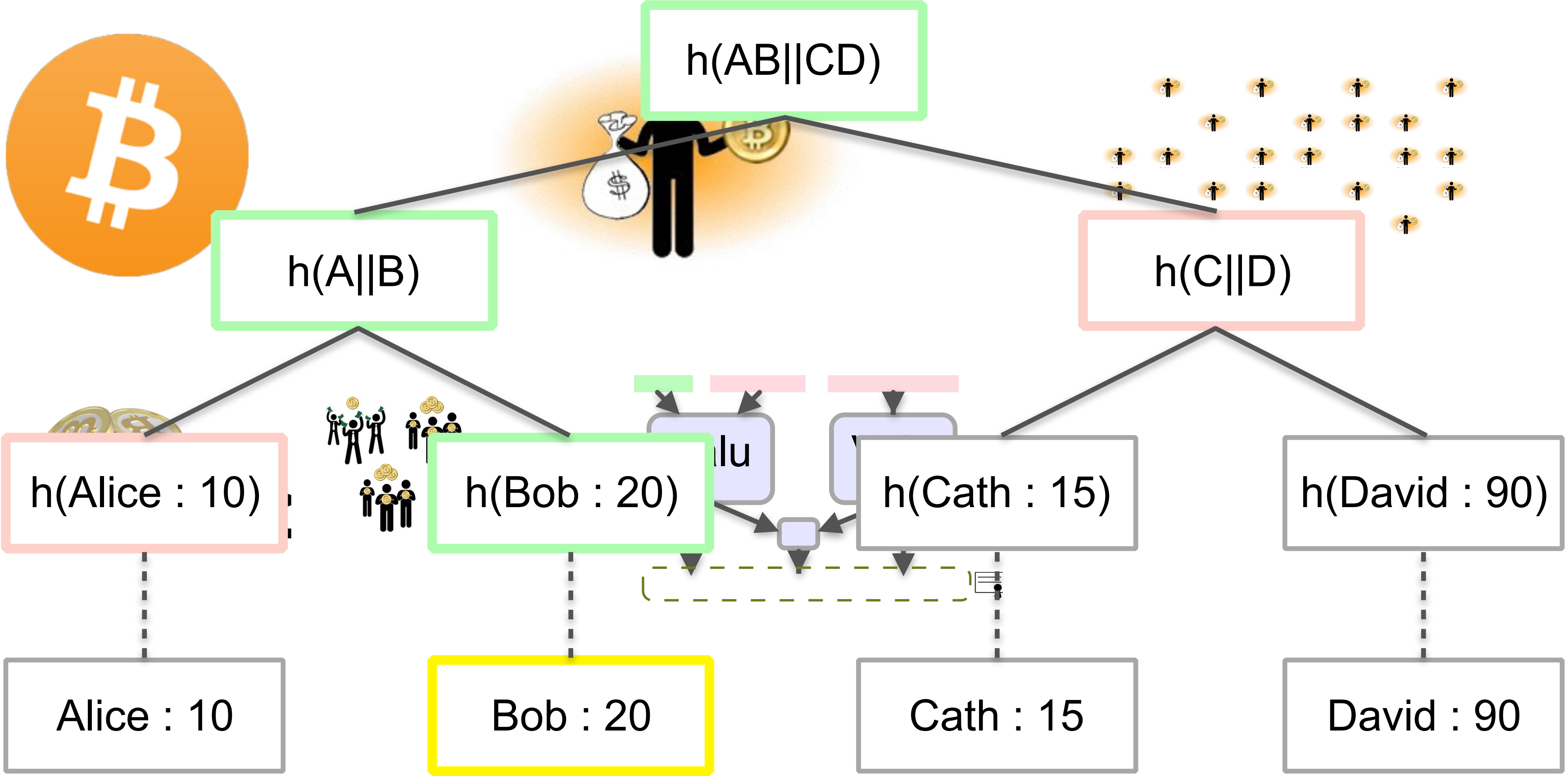
Summary



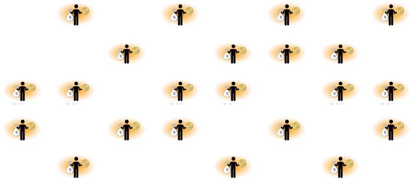
≥

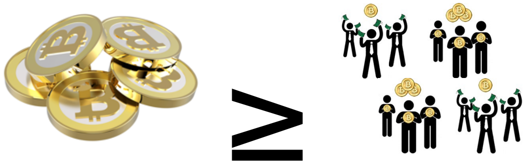


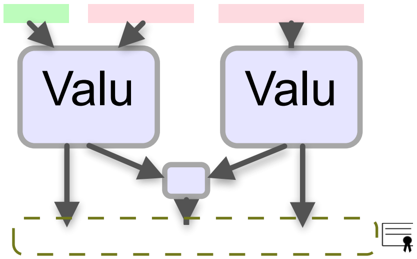
Summary

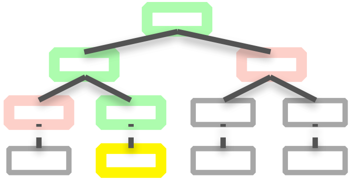

h(AB||CD)
h(A||B)
h(C||D)
lu
h(Alice : 10)
h(Bob : 20)
h(Cath : 15)
h(David : 90)
Alice : 10
Bob : 20
Cath : 15
David : 90

Summary

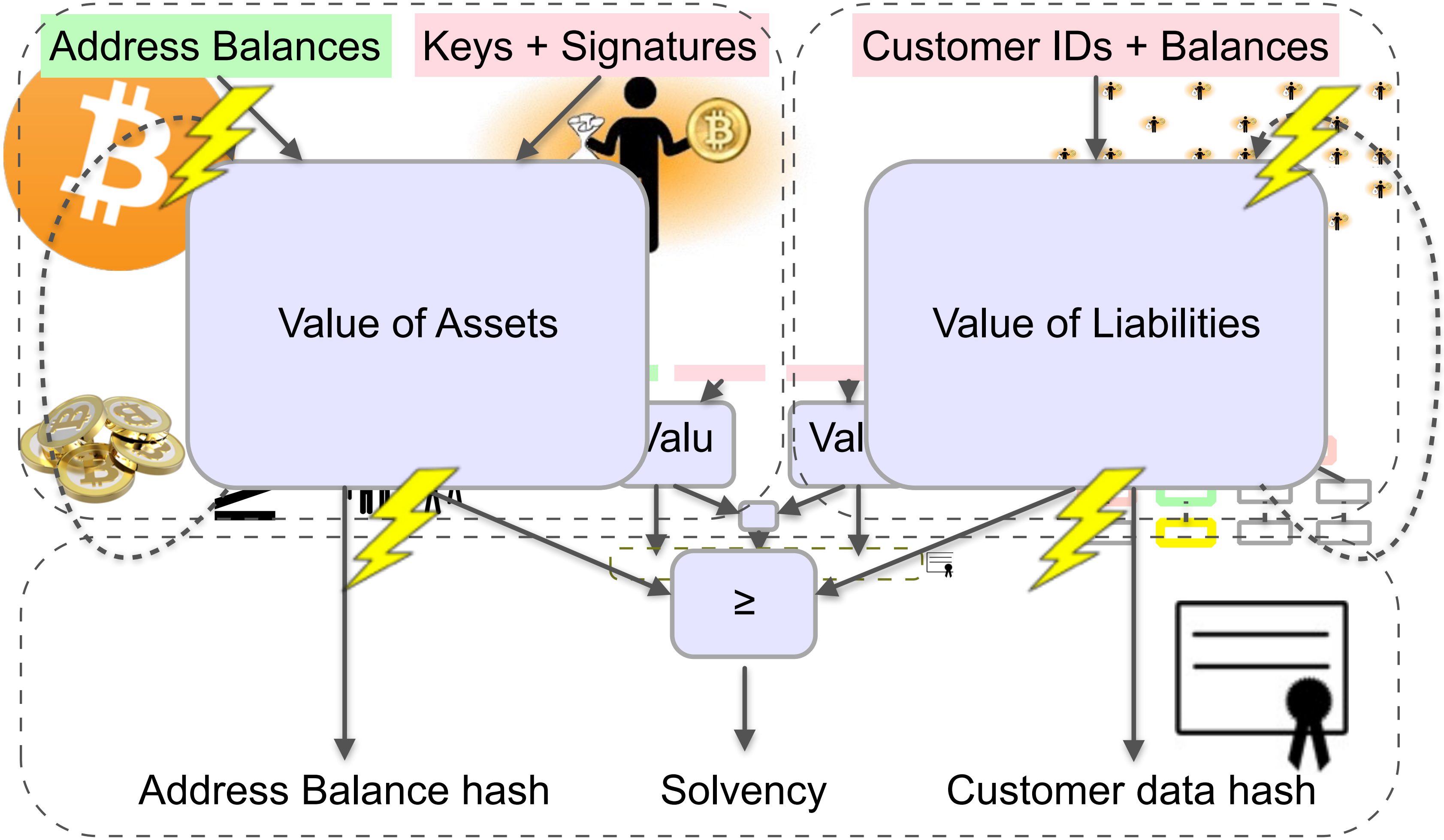




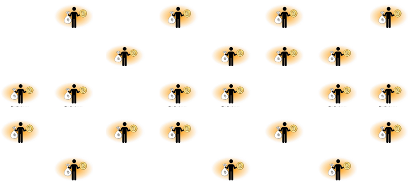


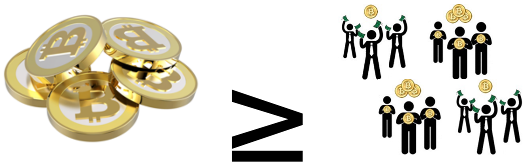


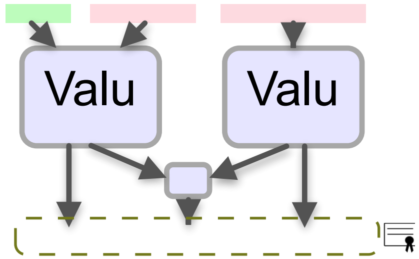
Summary

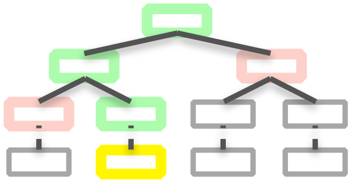

Address Balances
Keys + Signatures
Customer IDs + Balances
Value of Assets
Value of Liabilities
/alu
Val
≥
Address Balance hash
Solvency
Customer data hash

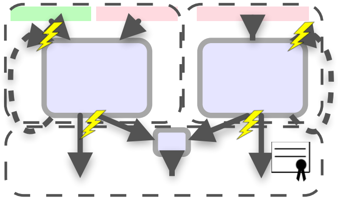
Summary



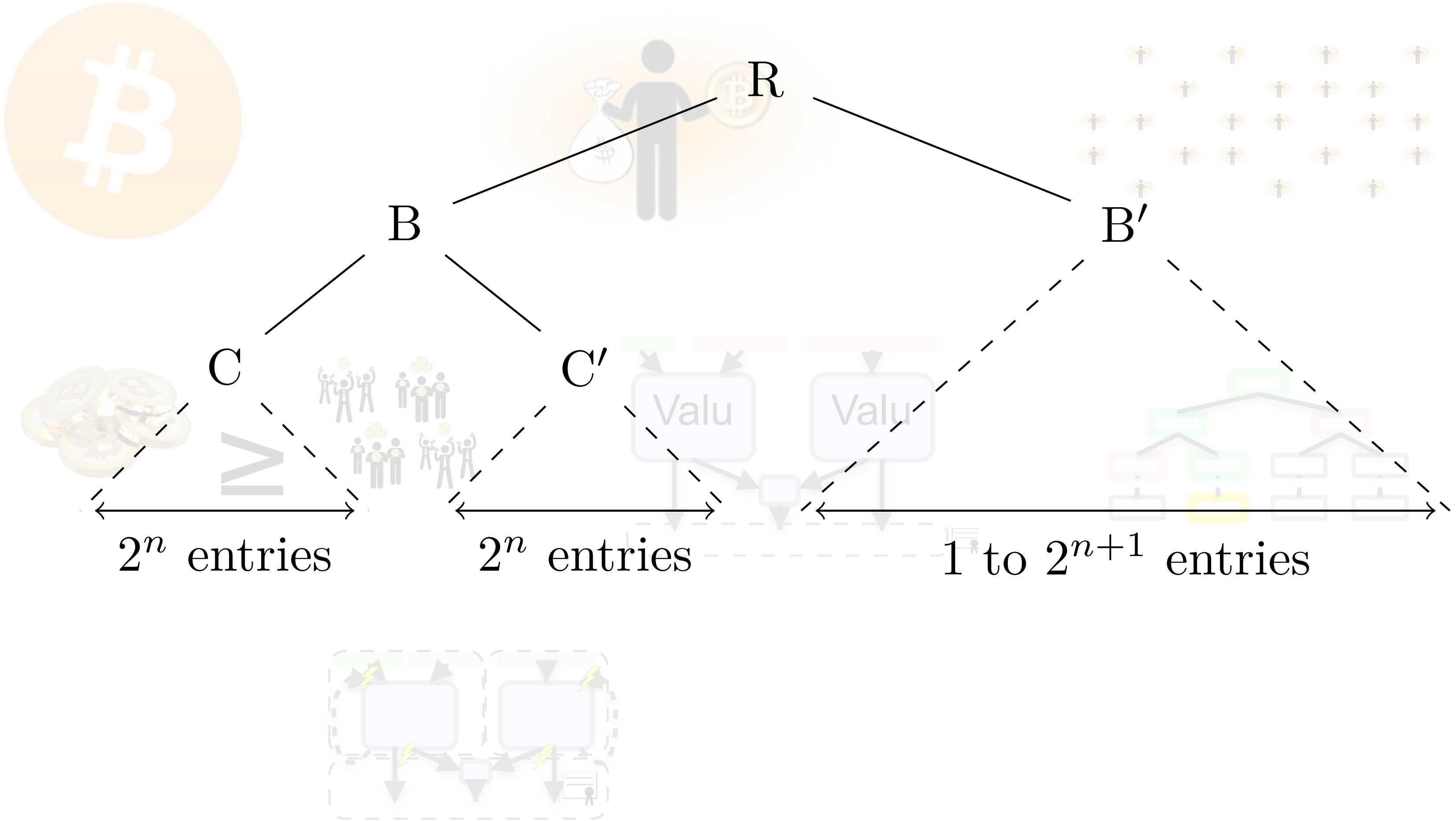




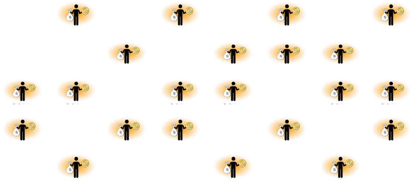




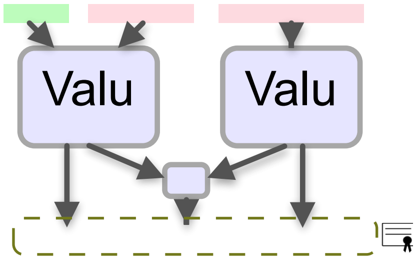
Summary

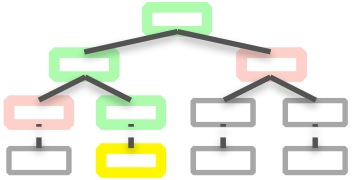


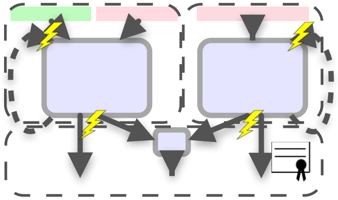
Summary

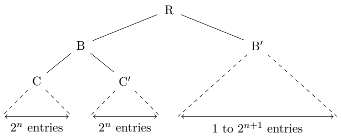


≥









Thank you

Questions?