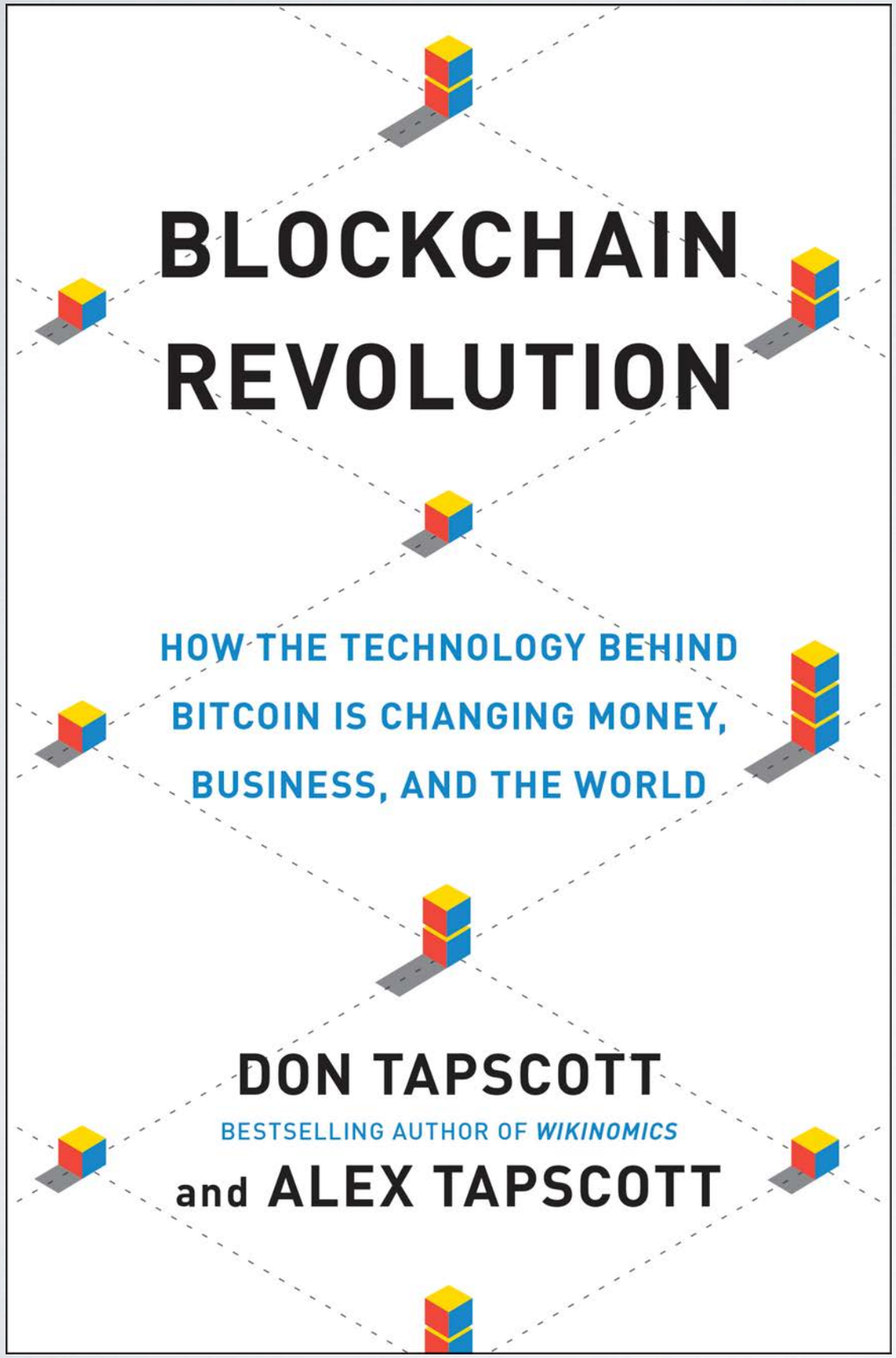
Blockchain Technology: Landscape & Future Directions

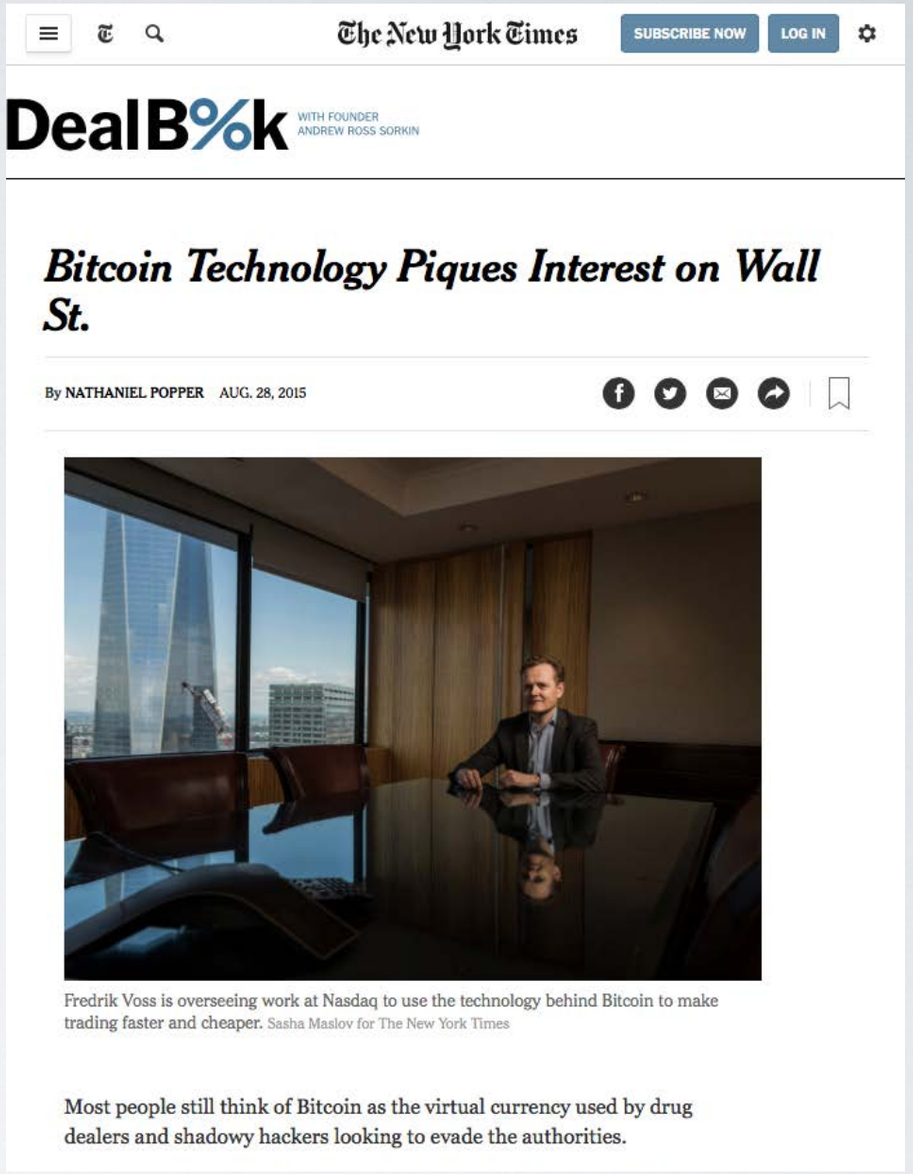
Jeremy Clark

Where I Am

Jeremy Clark

- Assistant Professor at the Concordia Institute for Information Systems Engineering (CIISE) in Montreal
- PhD from the University of Waterloo (2009)
- Team of eight graduate students
- Numerous academic papers on Bitcoin/Blockchain, including one of the earliest
- Contributed to courses (Princeton, MIT) & textbook on Bitcoin/blockchain
- Testified to Senate and House committees on Bitcoin/blockchain


BLOCKCHAIN
REVOLUTION
HOW THE TECHNOLOGY BEHIND
BITCOIN IS CHANGING MONEY,
BUSINESS, AND THE WORLD
DON TAPSCOTT
BESTSELLING AUTHOR OF WIKINOMICS
and ALEX TAPSCOTT


The New York Times
SUBSCRIBE NOW
LOG IN
DealB%k
WITH FOUNDER
ANDREW ROSS SORKIN
Bitcoin Technology Piques Interest on Wall St.
By NATHANIEL POPPER AUG. 28, 2015
Fredrik Voss is overseeing work at Nasdaq to use the technology behind Bitcoin to make trading faster and cheaper. Sasha Maslov for The New York Times
Most people still think of Bitcoin as the virtual currency used by drug dealers and shadowy hackers looking to evade the authorities.

TED

Digital Asset

HITACHI
Inspire the Next

accenture
High performance. Delivered.

AIRBUS

CME Group

DTCC
Securing Today. Shaping Tomorrow.

ANZ

DEUTSCHE BÖRSE GROUP

FUJITSU

IBM

intel

J.P.Morgan

R

万达·飞凡科技
WANDA FFAN TECHNOLOGY

ABN·AMRO

AESTHETIC INTEGRATION

博图纵横
BOTUZONGHENG

ALTOROS

CONSENSYS

Cuscal
The complete payments partner

coinplug

Eurostep
Digital

CREDITS

众享比特
PeerSafe

HUNDSUN

INVESHARE
Intelligent solutions for shareholder communications

KSD
Korea Securities Depository

Milligan Partners

intellect EU

Libra

guardtime

33.复杂美.CN

HUAWEI

趣链科技
Hyperchain

intuit

IROOTECH

JM

bitse

belink

BLOCKCHAIN

blocko

bloq

BNY MELLON

Blockstream

CLS
Fundamental to FX

BNP PARIBAS

ENERGY BLOCKCHAIN LABS

bubi.cn 布比

Broadridge

Calastone

cloudsoft

CISCO

colu.

Gem

MonetaGo

MIRACL

MURPHY & McGONIGLE
A Professional Corporation

ML

MOSCOW EXCHANGE

中国印钞造币
中钞信用卡产业发展有限公司

NSE

NETKI

Orchestrating a brighter world
NEC

norbloc

NOKIA

云象
YUNPHANT

NTT DATA
Global IT Innovator

橙色魔方
Orange Magic Cube

PAXOS

onchain

PDX
全息互信

CHAMBER OF DIGITAL COMMERCE

CSA cloud security alliance®

redhat

SAMSUNG
SAMSUNG SDS

vmware

梧桐树
wutongtree.com

tequa creek
information evolved

Ribbit.me

Investrata Foundation

WELLS FARGO

SANY

SBERBANK

S.W.I.F.T.

NXT FOUNDATION

TMX

fondazione INUIT
Università di Roma Tor Vergata

UMP

太一
TAI

保全网
BaoQuan.com

GINGKOO
金丘股份 (837901)

NEXGO

STATE STREET

Skry

点融网
Dianrong.com

SORAMITSU
ソラミツ

symbiont

THOMSON REUTERS

Digital Revolution

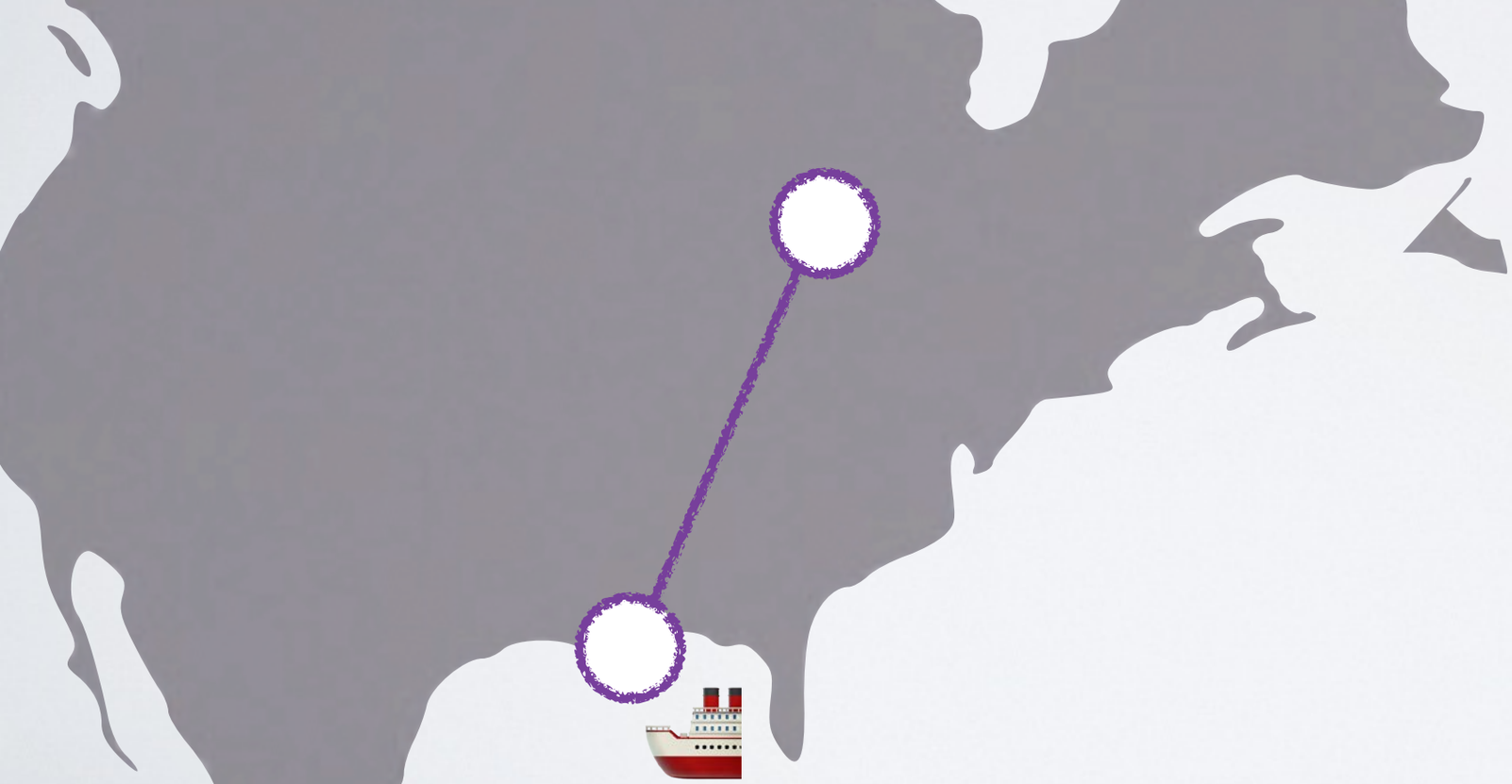
Blockchain

Digital Revolution

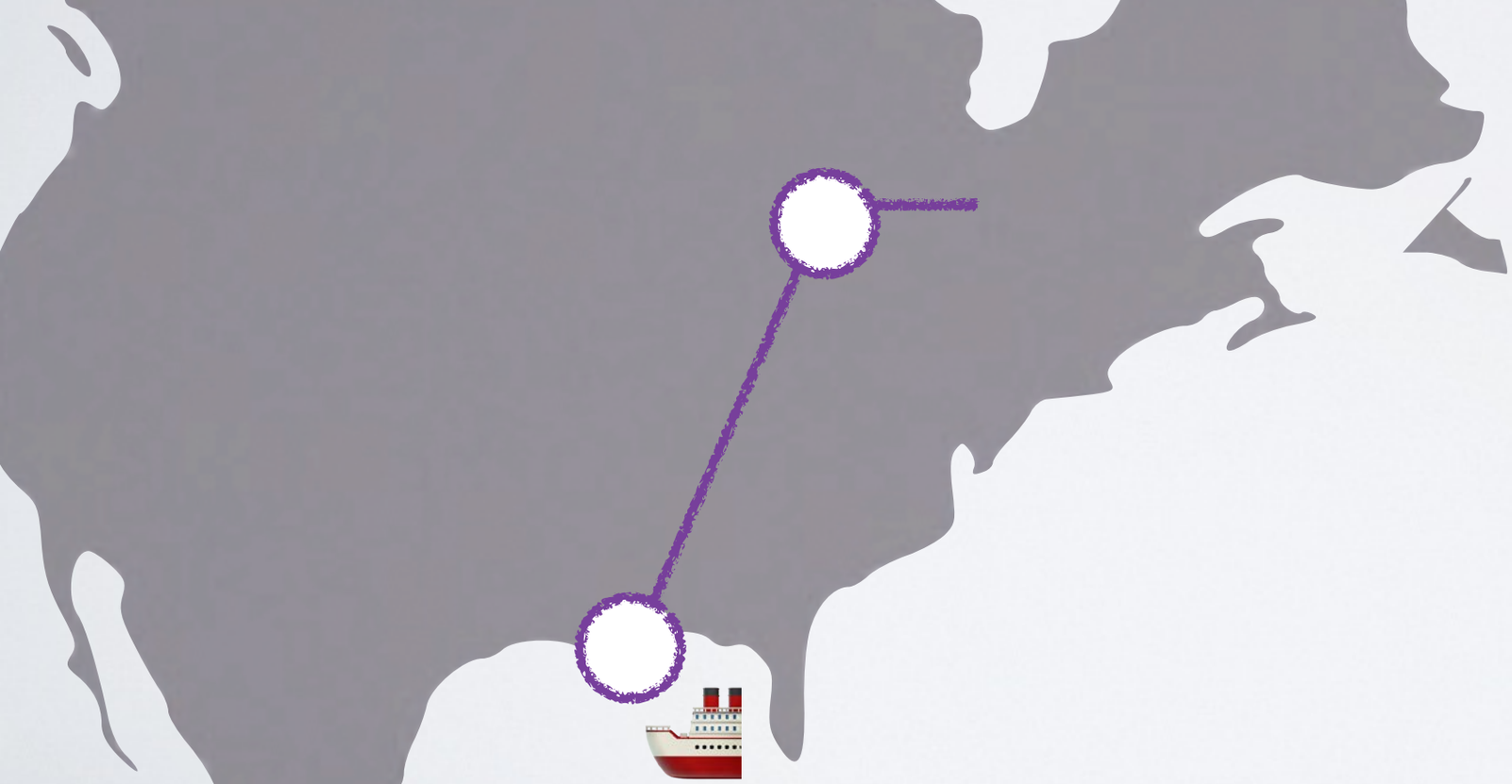
For business processes based on paper records, digitization increases efficiency


Tufnel-St. Hubbens Company
Clinical Research
Protocol
Study
A 15743
Patient Number
Patient Initials
Week 52 / 54
Early termination
Visit 1
Screening
Day 0
Page 3/47
DEMOGRAPHY
Date of Birth
Gender
[M] Male
[F] Female
Race [C] White
[B] Black
[E] Oriental
[O] Other
VITAL SIGNS
Weight (kg)
Height (cm)
Temperature °C
Oral
Rectal
Tympanic
Pulse Rate
PREVIOUS STUDY PARTICIPATION
Has the patient ever taken part in another
No
Yes
if "Yes" please provid
the answer to be above is not relevant to mot
Investigator's signature
X
(must be signed
Date


DEPARTMENT OF HOMELAND SECURITY
U.S. Customs and Border Protection
CERTIFICATE OF DISPOSITION
OF IMPORTED MERCHANDISE




Tufnel-St. Hubbens Company
Clinical Research
DEMOGRAPHY
Date of Birth
Gender
VITAL SIGNS
Weight (kg)
Height (cm)
Temperature °C
Oral
Rectal
Tympanic
Pulse Rate
PREVIOUS STUDY PARTICIPATION
No
Yes
Investigator's signature




DEPARTMENT OF HOMELAND SECURITY
U.S. Customs and Border Protection
CERTIFICATE OF DISPOSITION
OF IMPORTED MERCHANDISE


Tufnel-St. Hubbens Company
Clinical Research

Digital Revolution

Digital Revolution

Created by Creative Stall
from Noun Project

Database

Created by To Uyen
from Noun Project

Created by To Uyen
from Noun Project

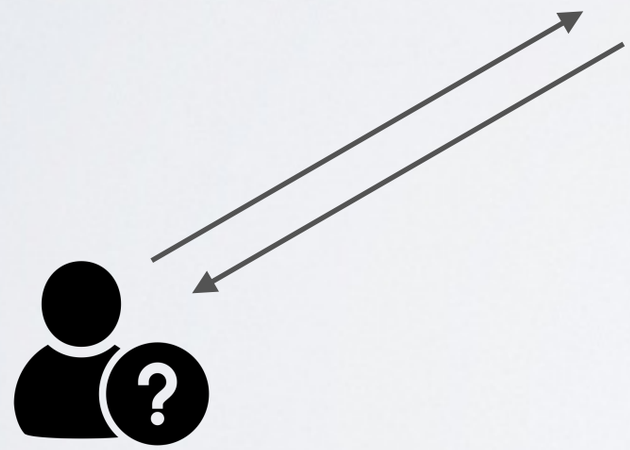
T-2351

T-4528

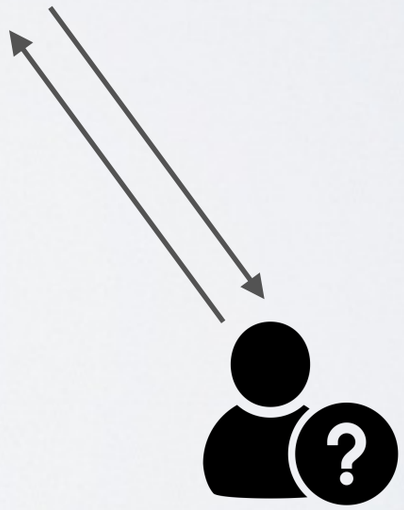
T-9636

T-9833

Created by Creative Stall
from Noun Project



Created by To Uyen
from Noun Project



Created by To Uyen
from Noun Project

Created by To Uyen
from Noun Project

Created by To Uyen
from Noun Project

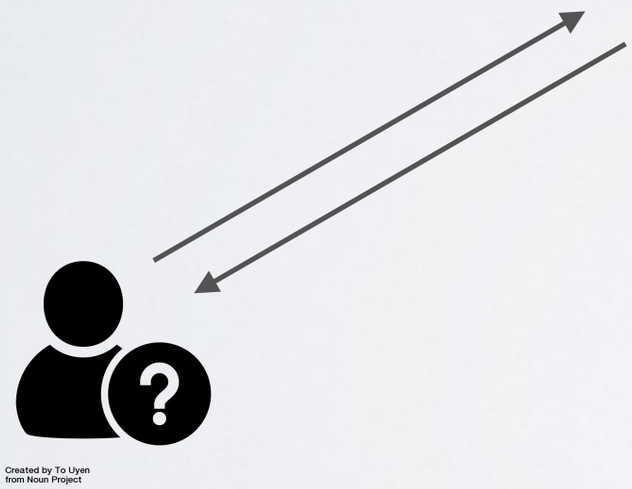
T-2351

T-4528

T-9636

T-9833

Created by Creative Stall
from Noun Project



Created by To Uyen
from Noun Project

Who Owns the Database?

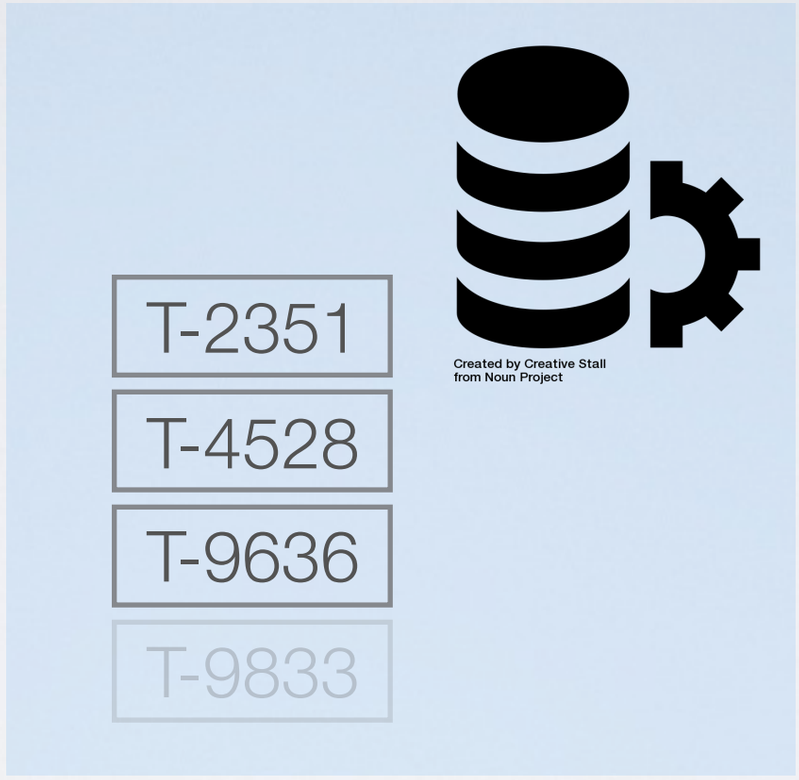
Privileged Position

Availability

Manage Access

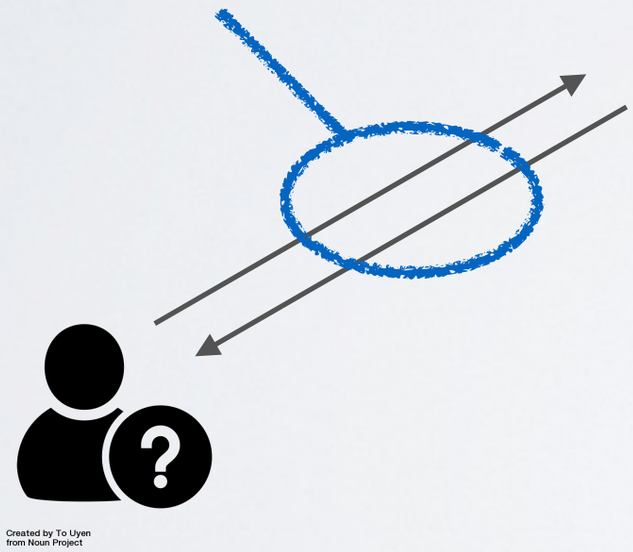
Created by To Uyen
from Noun Project

Created by To Uyen
from Noun Project



Created by Creative Stall
from Noun Project

Reconciliation



Created by To Uyen
from Noun Project

Who Owns the Database?

Privileged Position

Availability

Manage Access

Created by To Uyen
from Noun Project

Created by To Uyen
from Noun Project

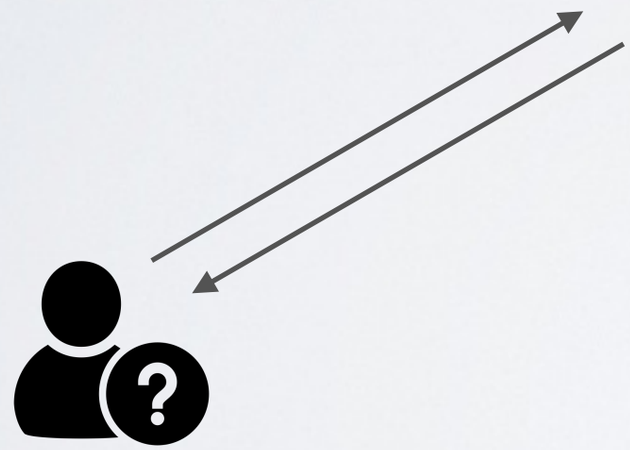
T-2351

T-4528

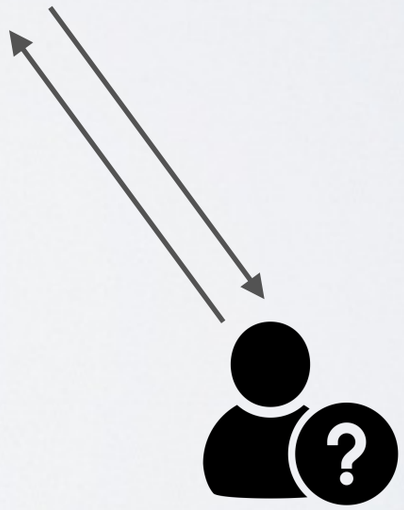
T-9636

T-9833

Created by Creative Stall
from Noun Project



Created by To Uyen
from Noun Project



Created by To Uyen
from Noun Project

Created by To Uyen
from Noun Project

T-2351

T-4528

T-9636

T-9833

Created by Creative Stall
from Noun Project

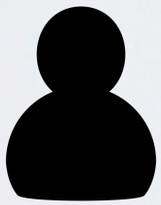
Created by To Uyen
from Noun Project

T-2351

T-4528

T-9636

T-9833



Created by To Uyen
from Noun Project

T-2351

T-4528

T-9636

T-9833

T-2351

T-4528

T-9636

T-9833

Created by To Uyen
from Noun Project

Created by To Uyen
from Noun Project

T-2351

T-4528

T-9636

T-9833

Disintermediation

Created by Creative Stall
from Noun Project

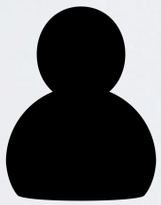
Created by To Uyen
from Noun Project

T-2351

T-4528

T-9636

T-9833



Created by To Uyen
from Noun Project

T-2351

T-4528

T-9636

T-9833

T-2351

T-4528

T-9636

T-9833

Created by To Uyen
from Noun Project

Blockchain

T-2351
T-4528
T-9636
T-9833

Created by To Uyen
from Noun Project

Created by To Uyen
from Noun Project

T-2351
T-4528
T-9636
T-9833

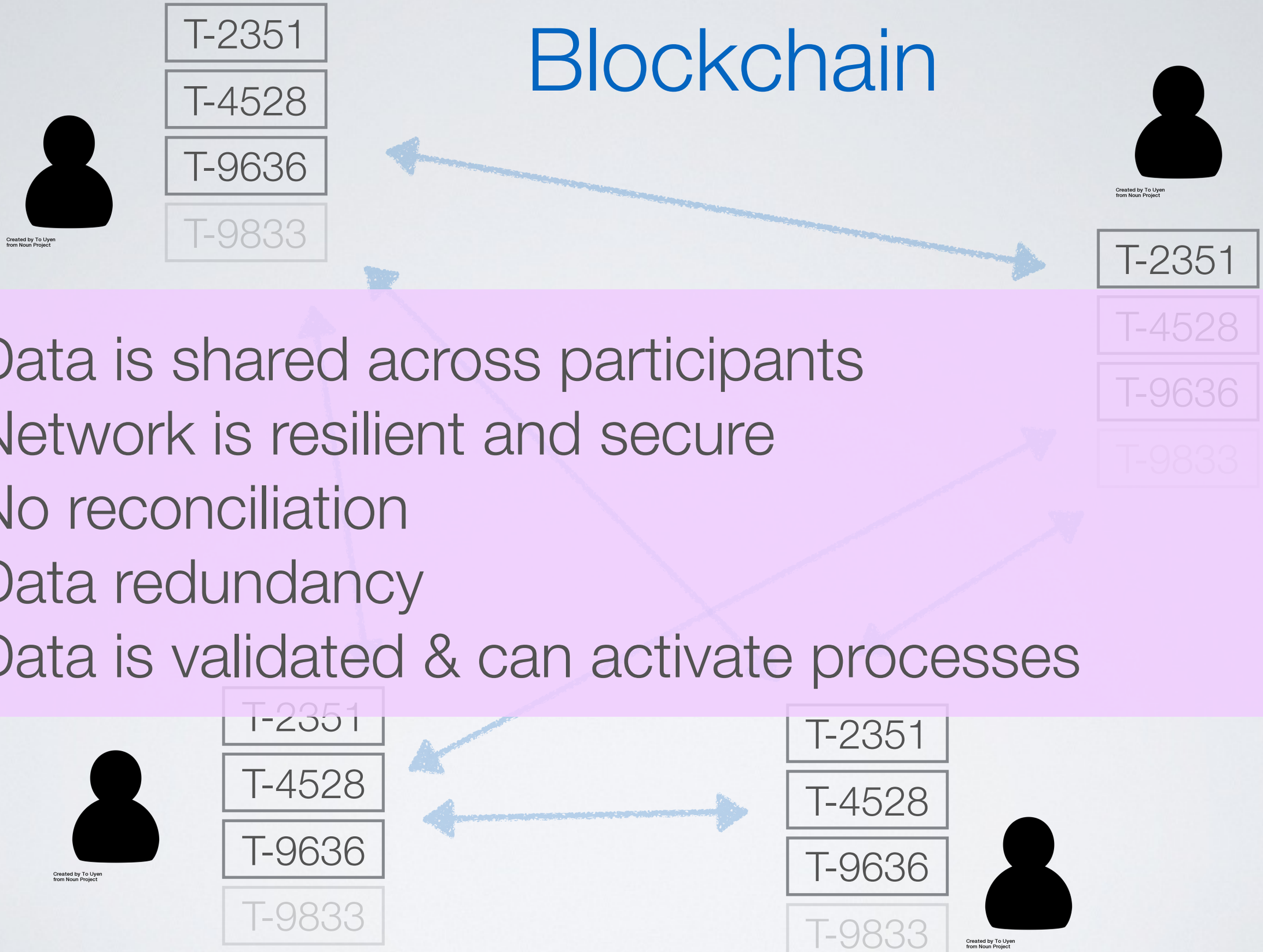
T-2351
T-4528
T-9636
T-9833

Created by To Uyen
from Noun Project

T-2351
T-4528
T-9636
T-9833

Created by To Uyen
from Noun Project

Blockchain



Data is shared across participants
Network is resilient and secure
No reconciliation
Data redundancy
Data is validated & can activate processes

Use Cases

- Securities: stocks, bonds, derivatives, swaps, repos and post-trade settlement
- Markets: land deeds, carbon credits
- Banking: inter-bank settlement, international payments, remittances, micropayments, loyalty
- Provenance: luxury goods, organic certifications, supply chain management
- Government: voting, registries
- Coordination: internet of things
- Identity management: KYC, PKI
- Fun: gambling, prediction markets

Use Cases

- Securities: stocks, bonds, derivatives, swaps, repos and post-trade settlement
- Markets: land deeds, carbon credits
- Banking: inter-bank settlement, international payments, remittances, micropayments, loyalty
- Provenance: luxury goods, organic certifications, supply chain management
- Gaming: betting, gambling
- Coordination: internet of things
- Identity management: KYC, PKI
- Fun: gambling, prediction markets

Blockchain systems can interact

Frequently Asked Questions

& common misconceptions

Relation to Bitcoin

Bitcoin is designed to be a currency (BTC)

Bitcoin is not a digital form of an existing currency

Thus not like Paypal, EFTs, interact-by-email

Bitcoin is decentralized: no central bank

The term blockchain

1) Bitcoin's protocol for achieving a distributed ledger maintained by an open network of profit-seeking nodes

2) Any distributed ledger

3) The philosophy behind Bitcoin: digitizing commodities, securities, deeds, contracts…

Blockchain v. Database

- Blockchains and (distributed) databases are similar and somewhat interchangeable
- The emphasis is on different things
- Blockchains are for small data (1MB every 10 min)
- Blockchains are for validated data
- Blockchains are not about complex queries (you download everything)
- Blockchains are secure against malicious nodes

Standards

- CAC-ISO-TC307: Blockchain and electronic distributed ledger technologies
- Industry Consortiums: Various

Regulation

- Use-Case Specific: Mostly pertains to Bitcoin
- Taxation: capital gain
- Accounting (IFRS): intangible asset
- KYC/AML: Fintrac given authority
- ICOs/Trusts/Exchanges: Securities authorities

Confidentiality & Privacy

- By default, blockchains have no confidential transactions
- Confidentiality can be added on with encryption but non-trivial
- By default, blockchains have no identities associated to transactions
- Identities can be added (or conversely, anonymity strengthened)

Proof of Work

Consistency?

- Consensus through voting

Honest majority

Consistency?

Consensus through voting

Honest majority

Consistency?

Consensus through voting

One vote per _____?

Honest majority

Consistency?

Consensus through voting

One vote per _____?

1) Entity:

trusted list of entities, closed network

Honest majority

Consistency?

Consensus through voting

One vote per _____?

1) Entity:

trusted list of entities, closed network

2) Unit of computational effort:

Bitcoin's blockchain

No trust, open network

Use cases

real & imagined

Supply chain management	Asset tracking	Payments	Transaction processing
Identity management	Internet of Things / Smart property	Data sharing	Fine-grained access control
Interoperation between systems	Regulation / sanctions	Permanent record storage	Decentralized timestamping
Auctions	Voting	Gambling	Insurance

Data

- Supply Chain
- Voting
- Identity
- IoT

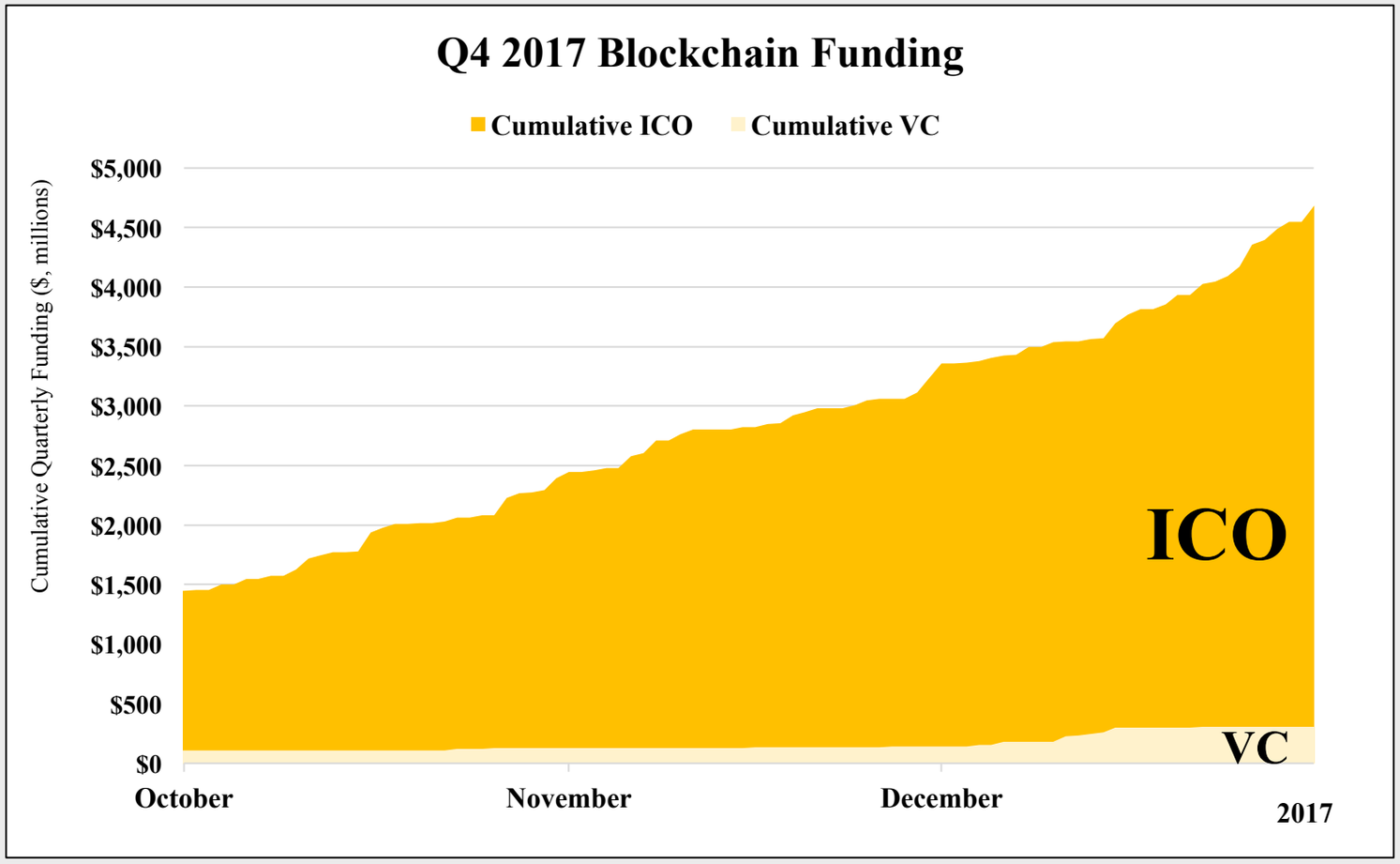
FinTech

- Payments
- Insurance
- Assets

Bitcoin

ICO Funding Raised $3.2bn in Q4

ICOs Exceeded VC by Over 16x



ICO
$3,231mn

VC
$200mn

Top ICO Deals:

Sirin Labs - $157.9mn
Polkadot - $144.6mn
Qash - $107.3mn
COMSA - $95.4mn

Top VC Deals:

BitGo - $42.5mn
BitPay - $30mn
OKCoin - $27.2mn
Abra - $16mn

Q2

ICO	VC
$797mn	$235mn

Q3

ICO	VC
$1,316mn	$156mn

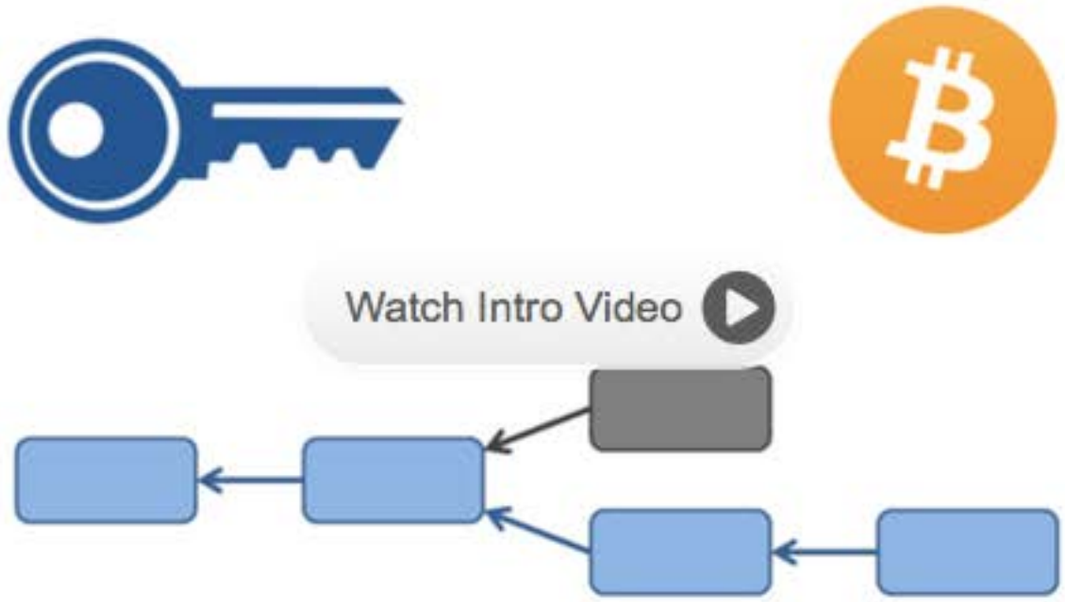
Data Sources: CoinDesk venture capital database, CoinDesk ICO Tracker
Notes: Deals under $100,000 excluded, $ amount at time raised, including only fundraisers ending in 'Q4 2017' (10/1/17 – 12/31/17)

coindesk

PRINCETON UNIVERSITY

Bitcoin and Cryptocurrency Technologies

There's a lot of excitement about Bitcoin, but also a lot of confusion about what Bitcoin is and how it works. We're offering this course focusing on the computer science behind Bitcoin to help cut through the hype and get to the core of what makes Bitcoin unique.



About the Course

To really understand what is special about Bitcoin, we need to understand how it works at a technical level. We'll address the important questions about Bitcoin, such as:

How does Bitcoin work? What makes Bitcoin different? How secure are your Bitcoins? How anonymous are Bitcoin users? What determines the price of Bitcoins? Can cryptocurrencies be regulated? What might the future hold?

After this course, you'll know everything you need to be able to separate fact from fiction when reading claims about Bitcoin and other cryptocurrencies. You'll have the conceptual foundations you need to engineer secure software that interacts with the Bitcoin network. And you'll be able to integrate ideas from Bitcoin in your own

Sessions

September 4, 2015 - April 22, 2016

Go to Course

Course at a Glance

- 7 weeks of study
- 3-6 hours/week
- English

Bitcoin and Cryptocurrency Technologies

Arvind Narayanan, Joseph Bonneau, Edward Felten,
Andrew Miller, Steven Goldfeder

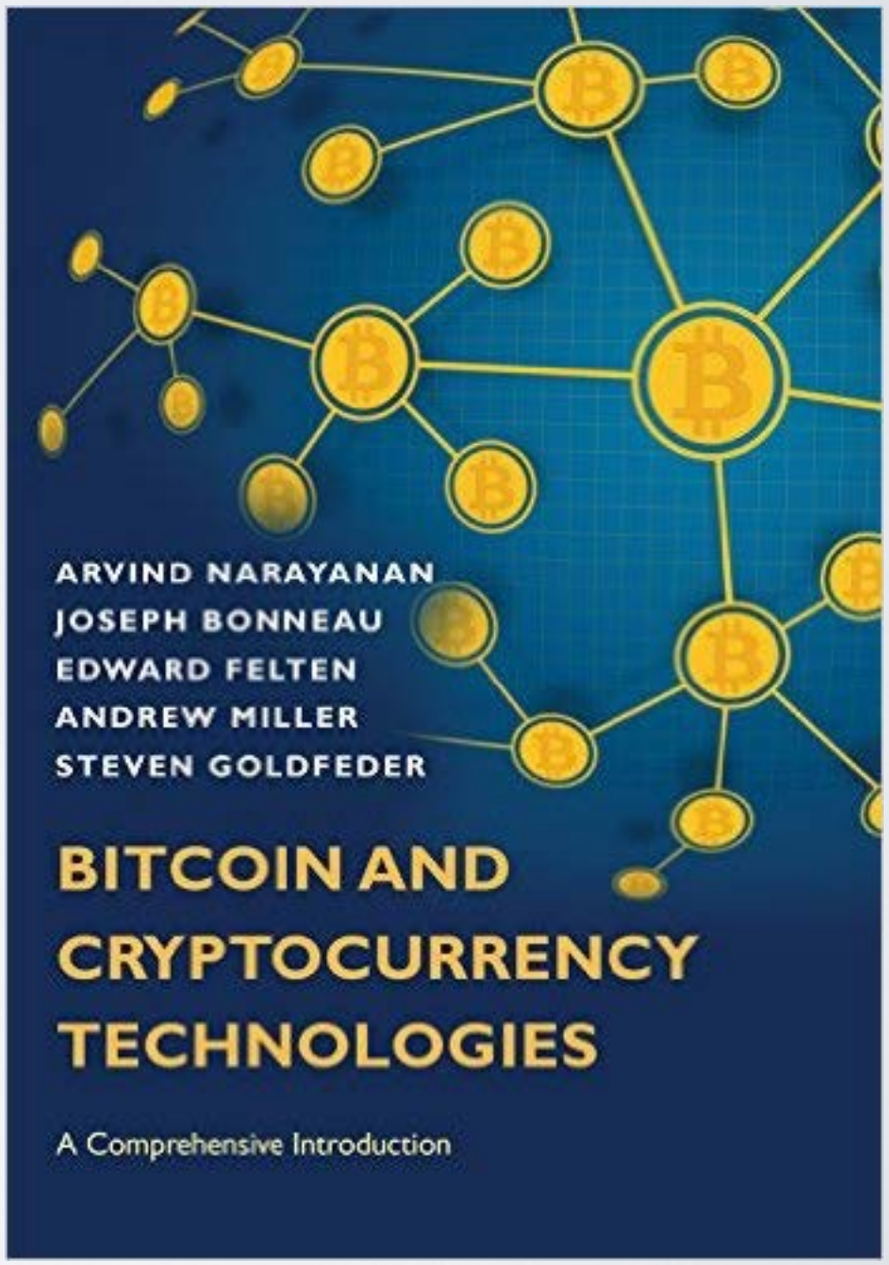
with a preface by Jeremy Clark

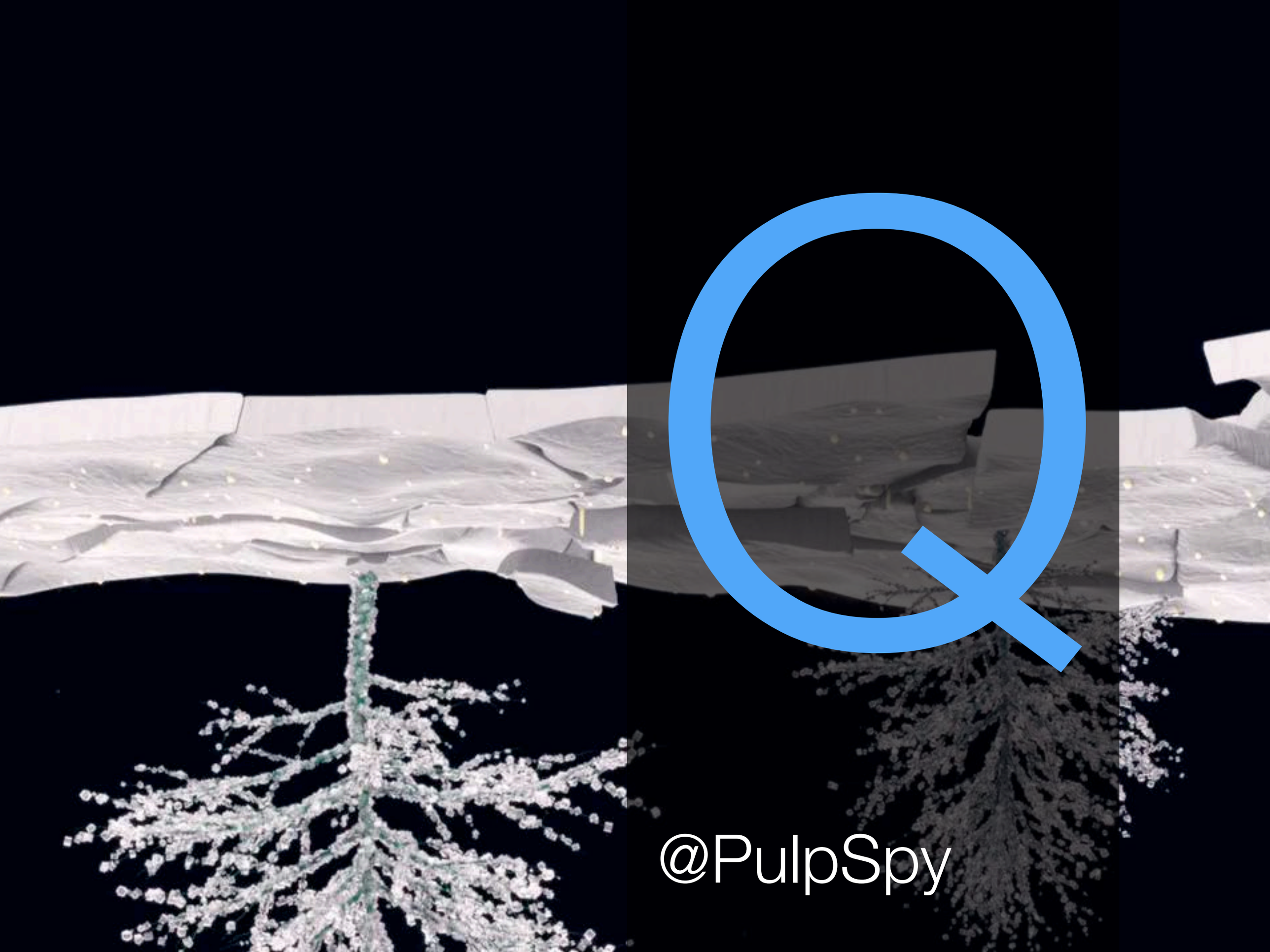
Draft — Feb 9, 2016

Feedback welcome! Email bitcoinbook@lists.cs.princeton.edu

For the latest draft and supplementary materials including programming assignments, see our Coursera course.

The official version of this book will be published by Princeton University Press in 2016. If you'd like to be notified when it's available, please sign up here.




@PulpSpy

How it works

Alice

Bob

Digital Monetary Unit

Bank

Alice

Bob

Issued by Bank

Bank

Spent without Bank

Bank

Alice

Bob

Ledger-based System

Bob	Alice	10 BTC
Carol	Alice	5 BTC
Carol	Bob	18 BTC

Ledger

Alice
15 BTC

Bob
18 BTC

Bob	Alice	10 BTC
Carol	Alice	5 BTC
Carol	Bob	18 BTC

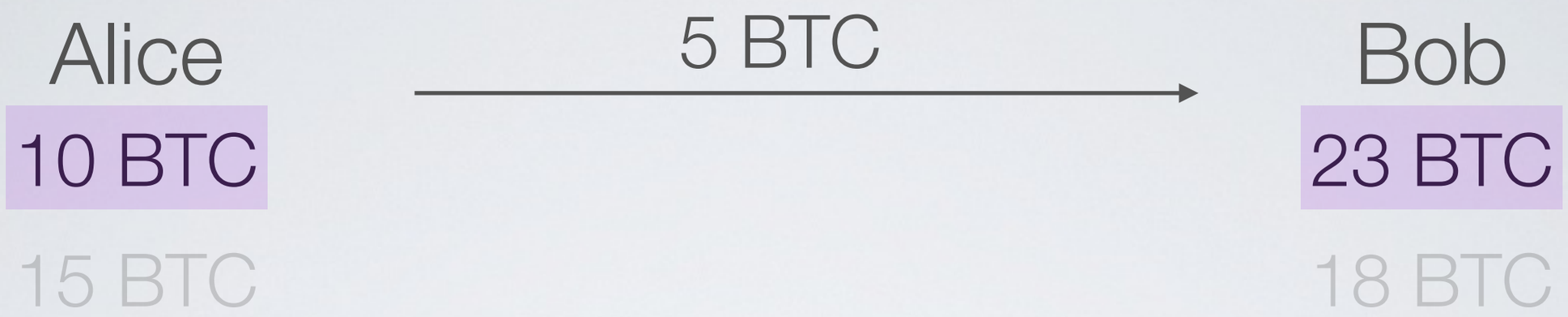
Ledger

Bob	Alice	10 BTC
Carol	Alice	5 BTC
Carol	Bob	18 BTC

Ledger

Bob	Alice	10 BTC
Carol	Alice	5 BTC
Carol	Bob	18 BTC
Alice	Bob	5 BTC

Ledger



Bob	Alice	10 BTC
Carol	Alice	5 BTC
Carol	Bob	18 BTC
Alice	Bob	5 BTC

Ledger

Alice
10 BTC

Bob
23 BTC

Access Control

Bob	Alice	10 BTC
Carol	Alice	5 BTC
Carol	Bob	18 BTC
Alice	Bob	5 BTC

Ledger

{Alice, K_A}
10 BTC

{Bob, K_B}
23 BTC

Bob	Alice	10 BTC
Carol	Alice	5 BTC
Carol	Bob	18 BTC
Alice	Bob	5 BTC

Ledger

Bob	Alice	10 BTC
Carol	Alice	5 BTC
Carol	Bob	18 BTC
Alice	Bob	5 BTC

Ledger

{Alice, K_A}
10 BTC

{Bob, K_B}
23 BTC

PKI

Bob	Alice	10 BTC
Carol	Alice	5 BTC
Carol	Bob	18 BTC
Alice	Bob	5 BTC

Ledger

K_A
10 BTC

K_B
23 BTC

Pseudonymity

K_B	K_A	10 BTC
K_C	K_A	5 BTC
K_C	K_B	18 BTC
K_A	K_B	5 BTC

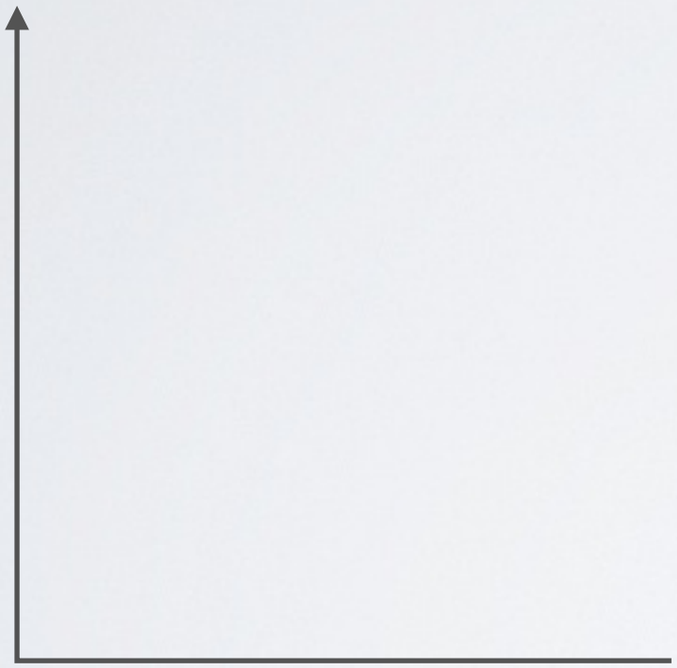
Ledger

Transaction:	T-9833
Inputs:	{T-5292, K_{A1}, 3.5} {T-3928, K_{A2}, 2.5}
Outputs:	{K_{B1}, 5.0} {K_{A3}, 0.99}
Signature:	{Sig_{A1}} {Sig_{A2}}

K_B	K_A	10 BTC
K_C	K_A	5 BTC
K_C	K_B	18 BTC
K_A	K_B	5 BTC

Ledger

Transaction:	T-9833
Inputs:	{T-5292, K_{A1}, 3.5} {T-3928, K_{A2}, 2.5}
Outputs:	{K=Script(In), 5.0} {K=Script(In), 0.99}
Signature:	{Sig_{A1}} {Sig_{A2}}



K_B	K_A	10 BTC
K_C	K_A	5 BTC
K_C	K_B	18 BTC
K_A	K_B	5 BTC

Ledger

K_A
10 BTC

K_B
23 BTC

Decentralize?

T-2351
T-4528
T-9636
T-9833

Ledger

K_A → T-9833

10 BTC

K_B

23 BTC

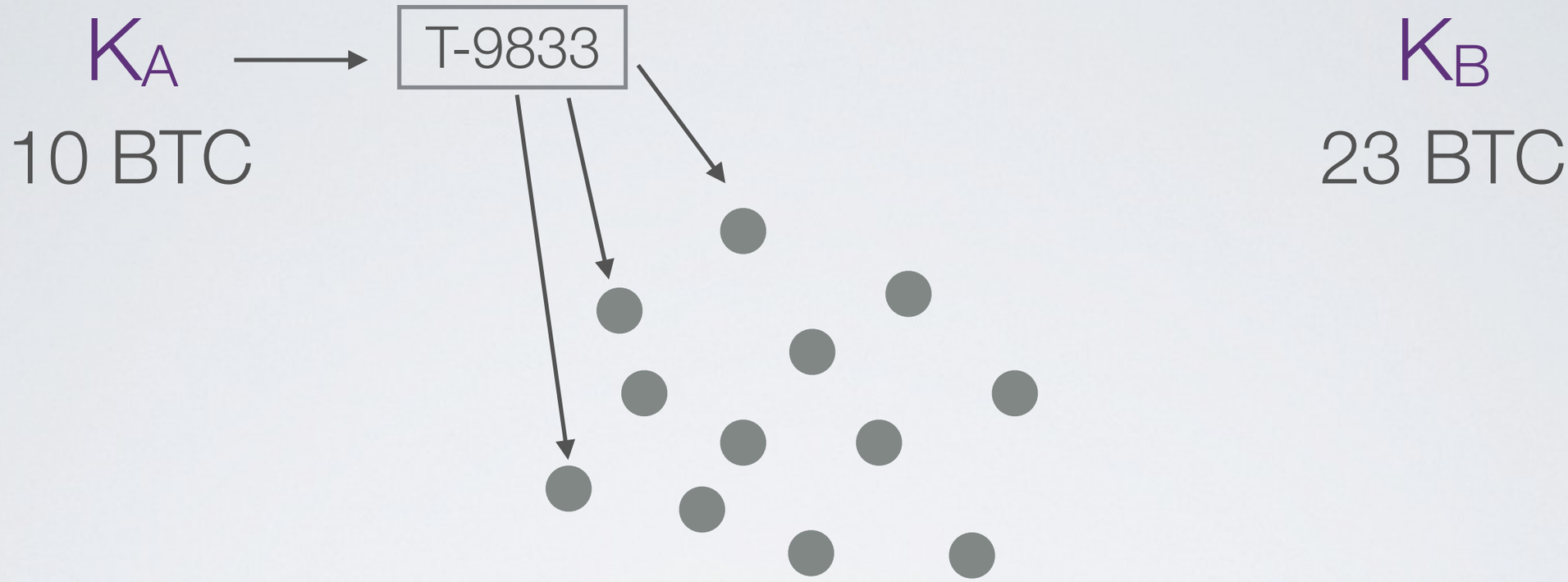
T-2351

T-4528

T-9636

T-9833

Ledger



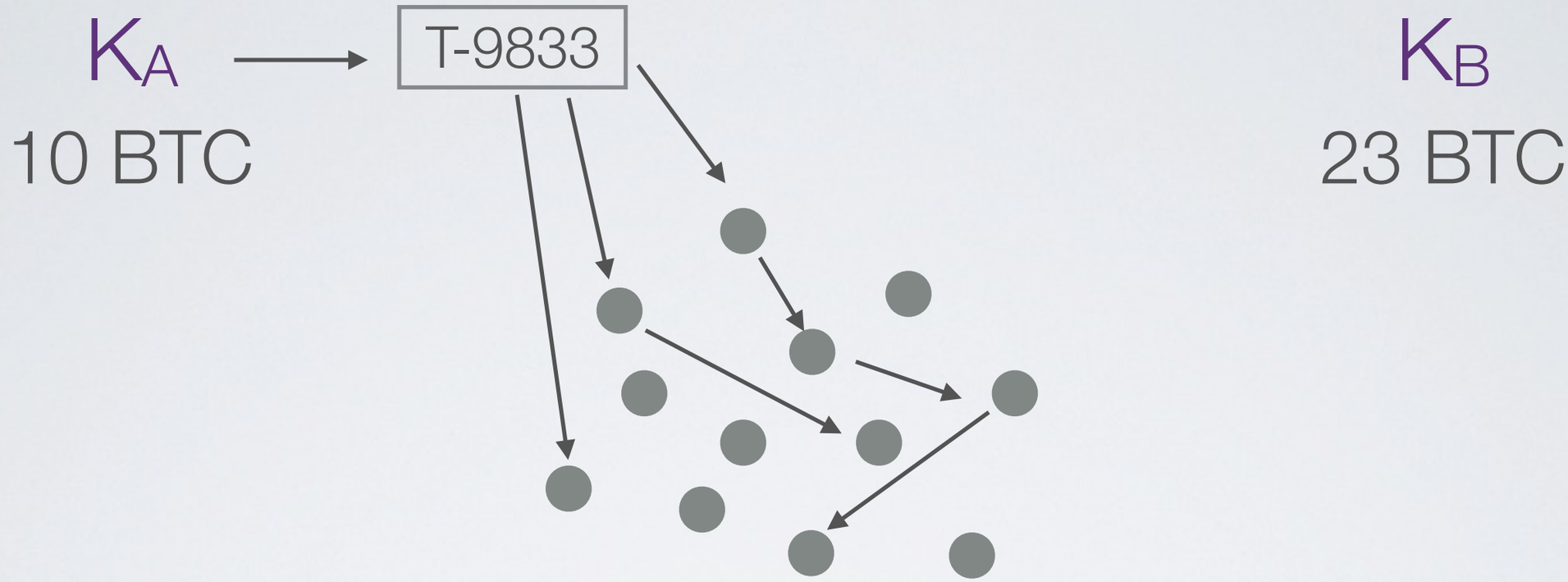
T-2351

T-4528

T-9636

T-9833

Ledger



T-2351

T-4528

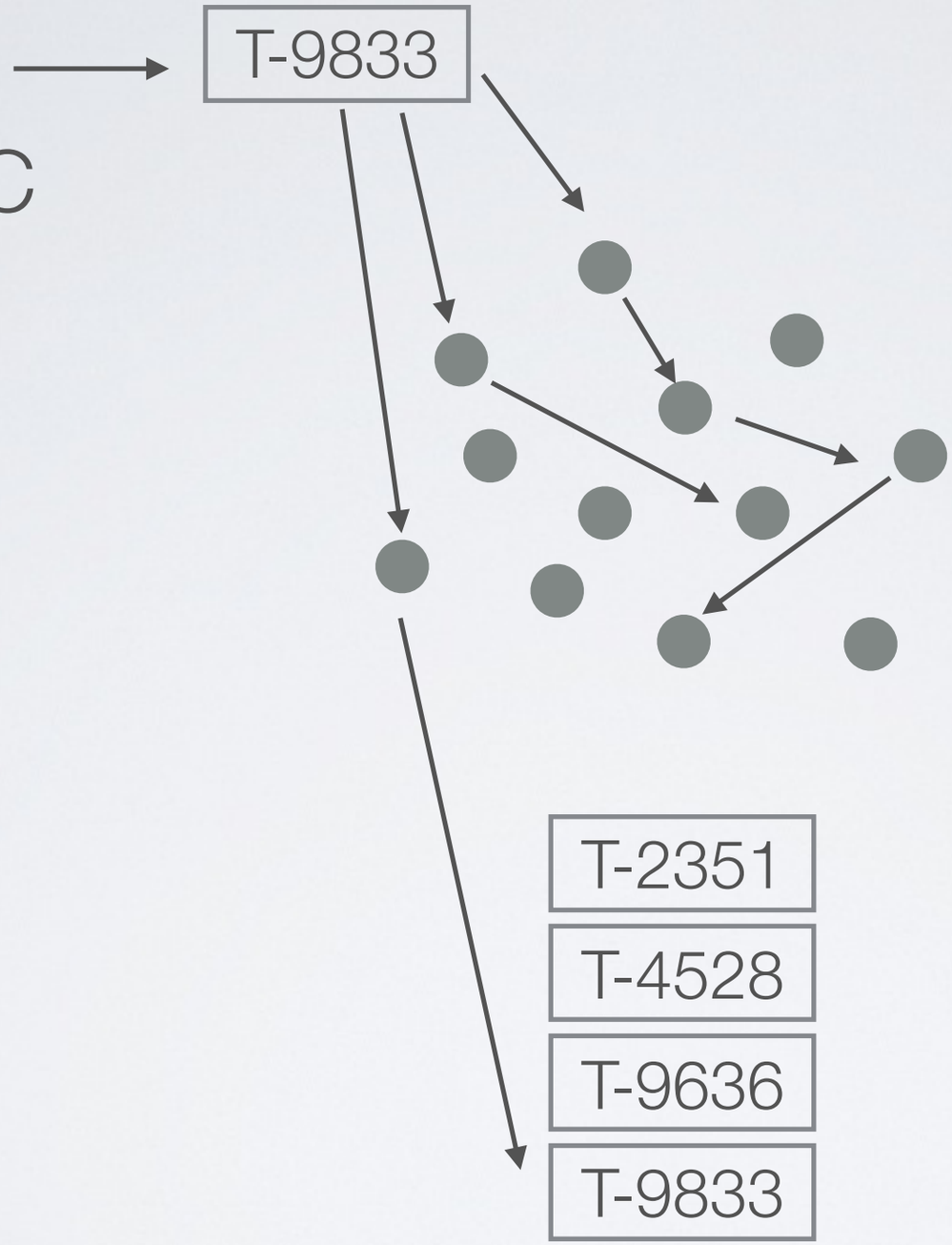
T-9636

T-9833

Ledger

K_A

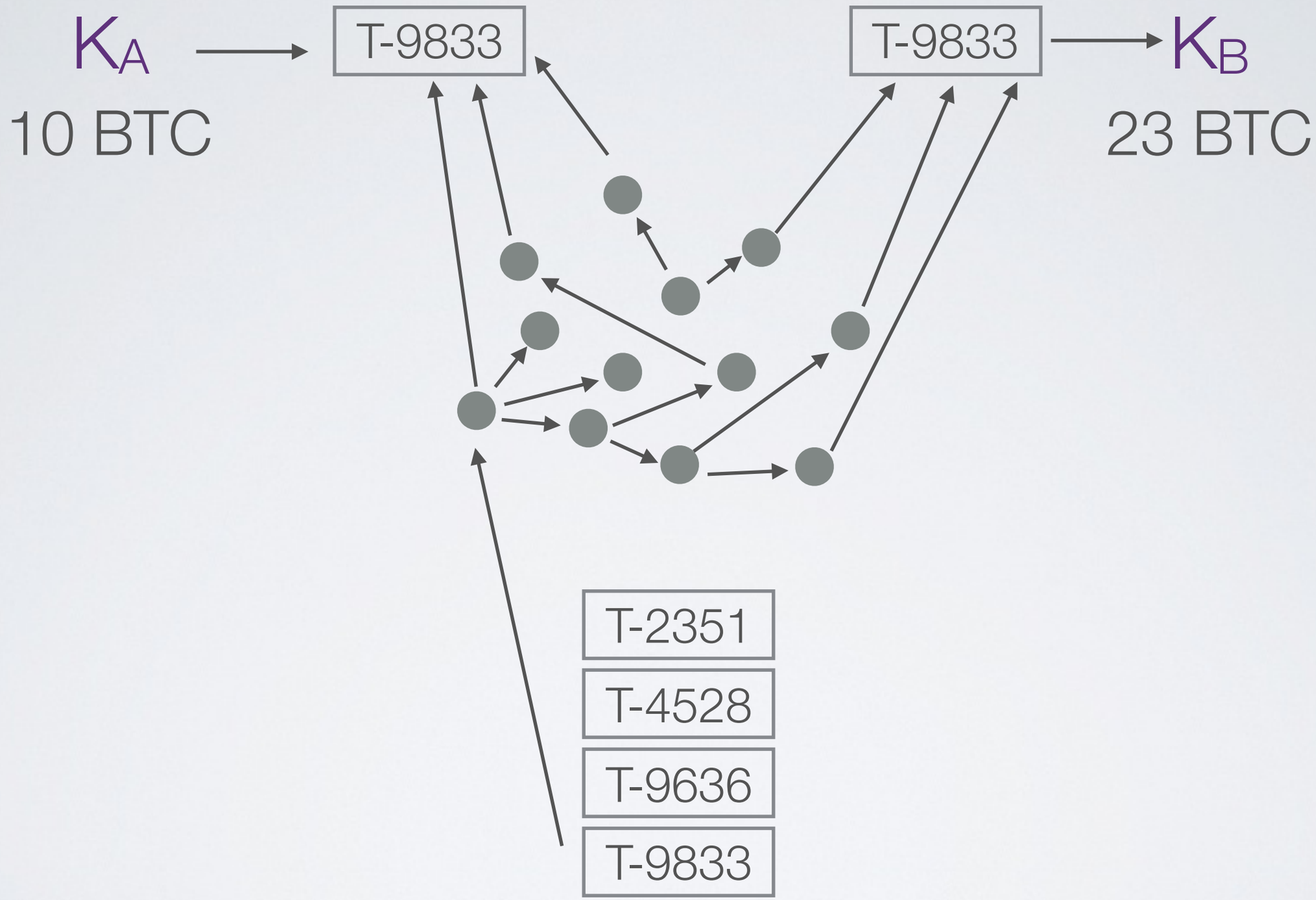
10 BTC



K_B

23 BTC

Ledger


K_A
10 BTC
T-9833
T-9833
K_B
23 BTC
T-2351
T-4528
T-9636
T-9833
Ledger

Agreement & Append-Only

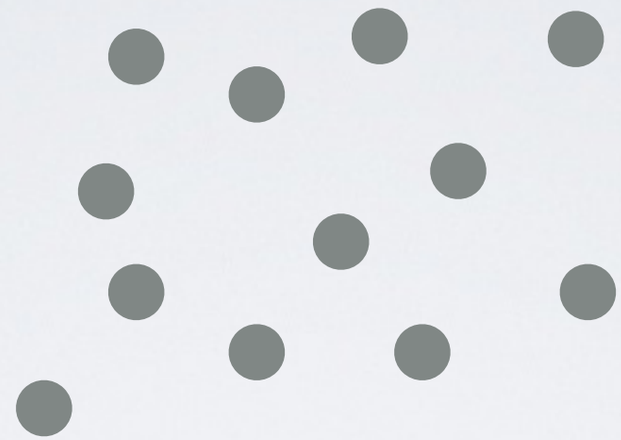
T-2351

T-4528

T-9636

T-9833

Ledger



Block 11

T-2351

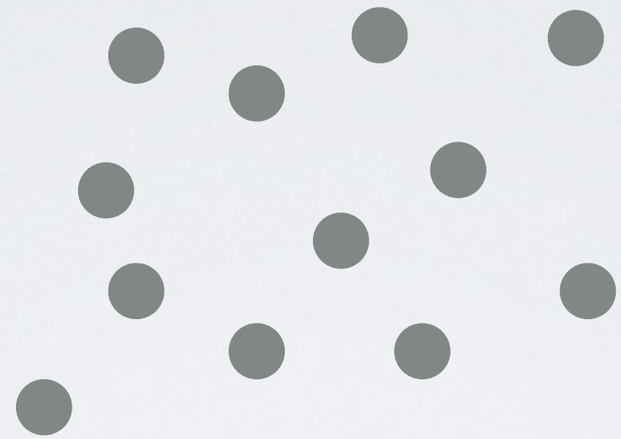
T-4528

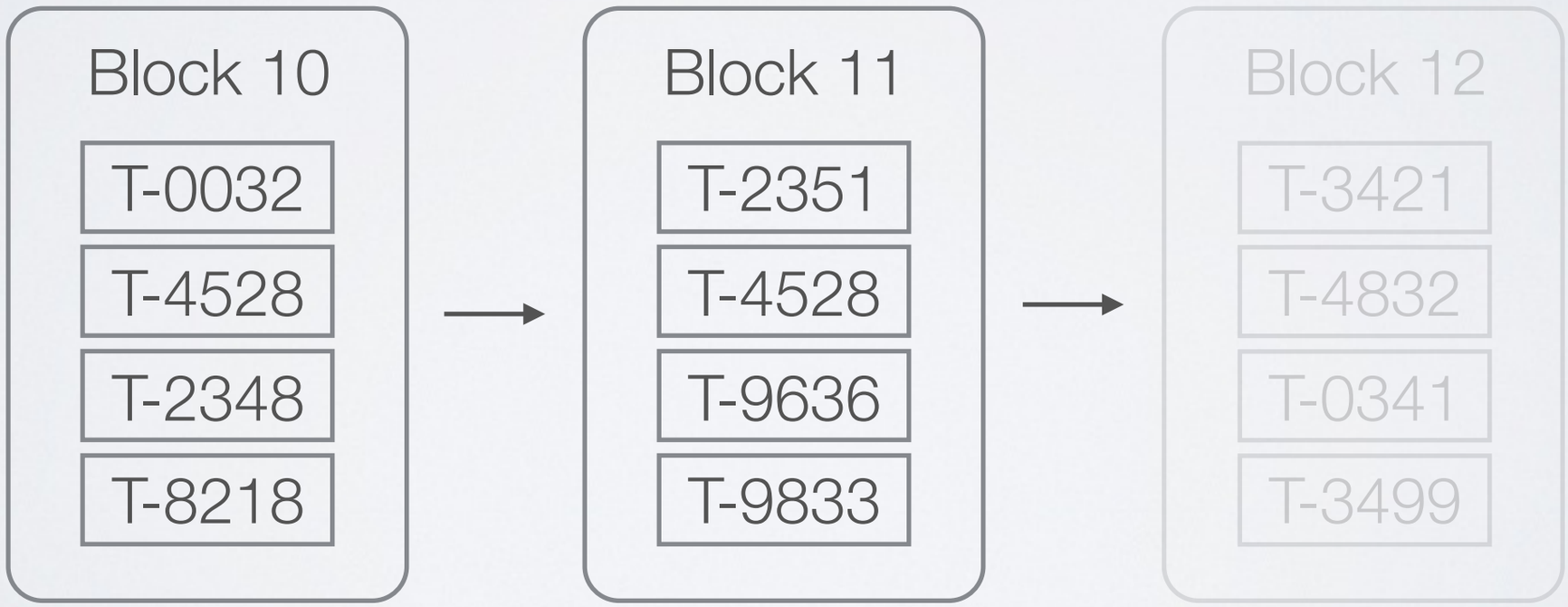
T-9636

T-9833

Ledger

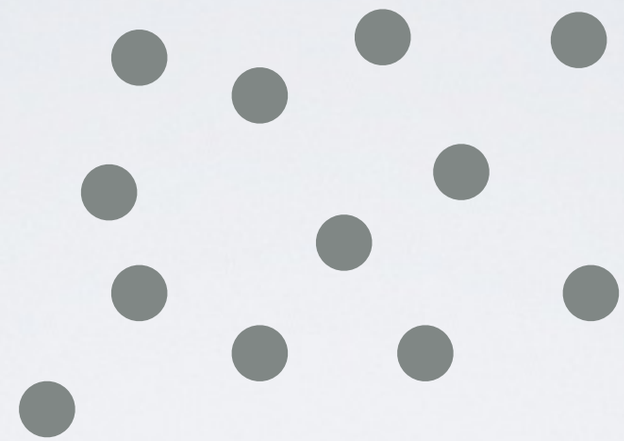
Hash Chain

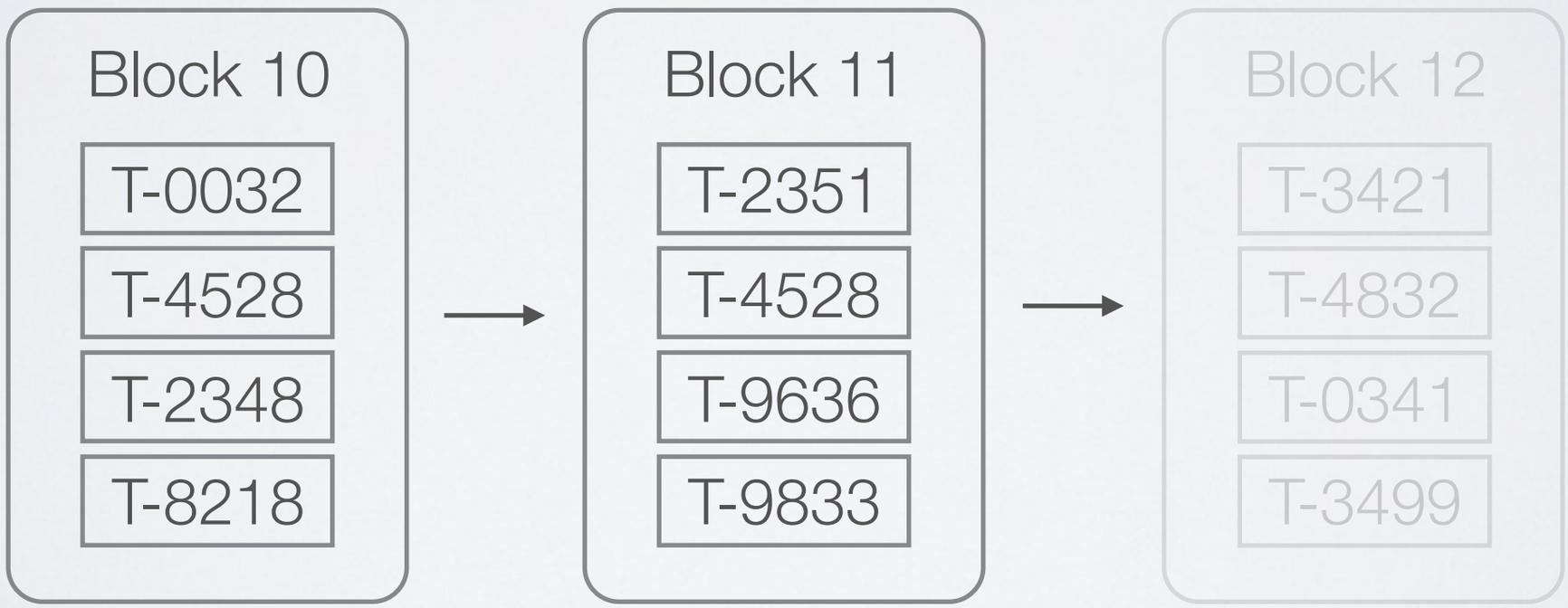


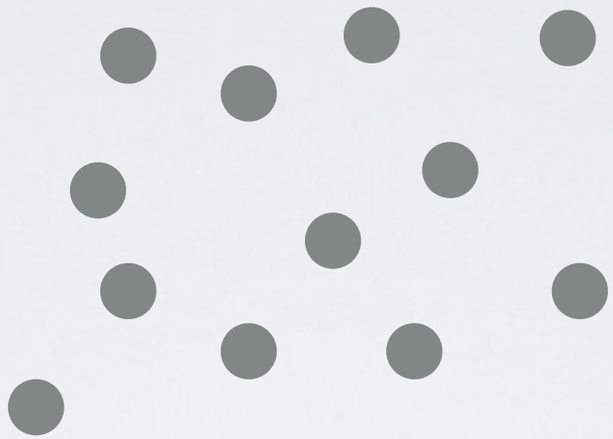


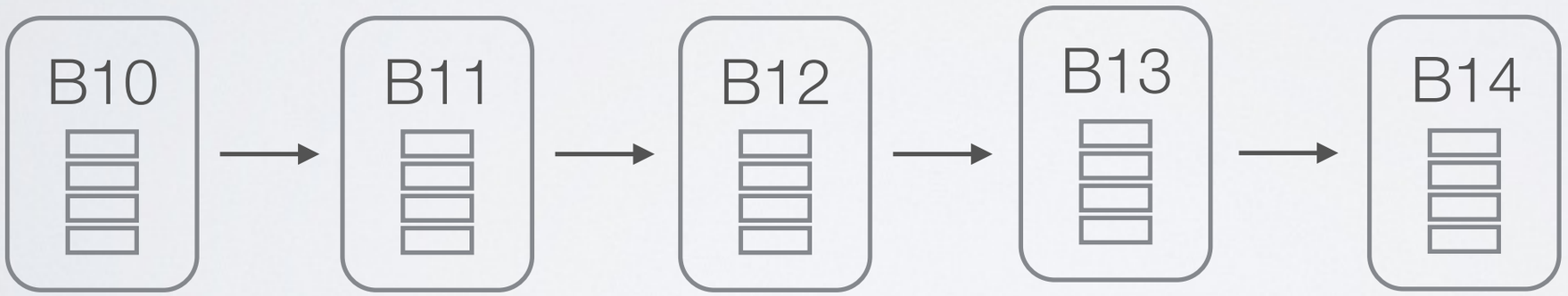
Ledger

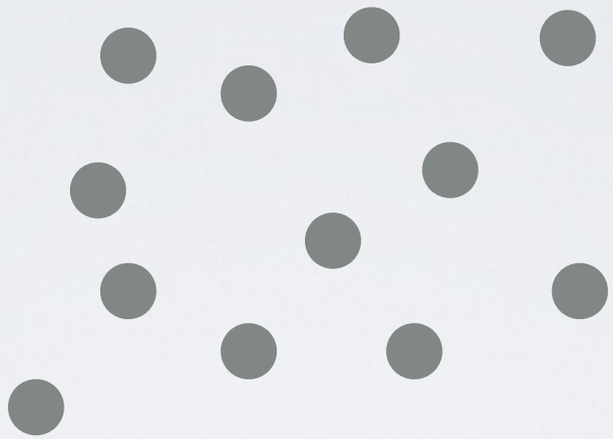
Rate-Limit Block Creation

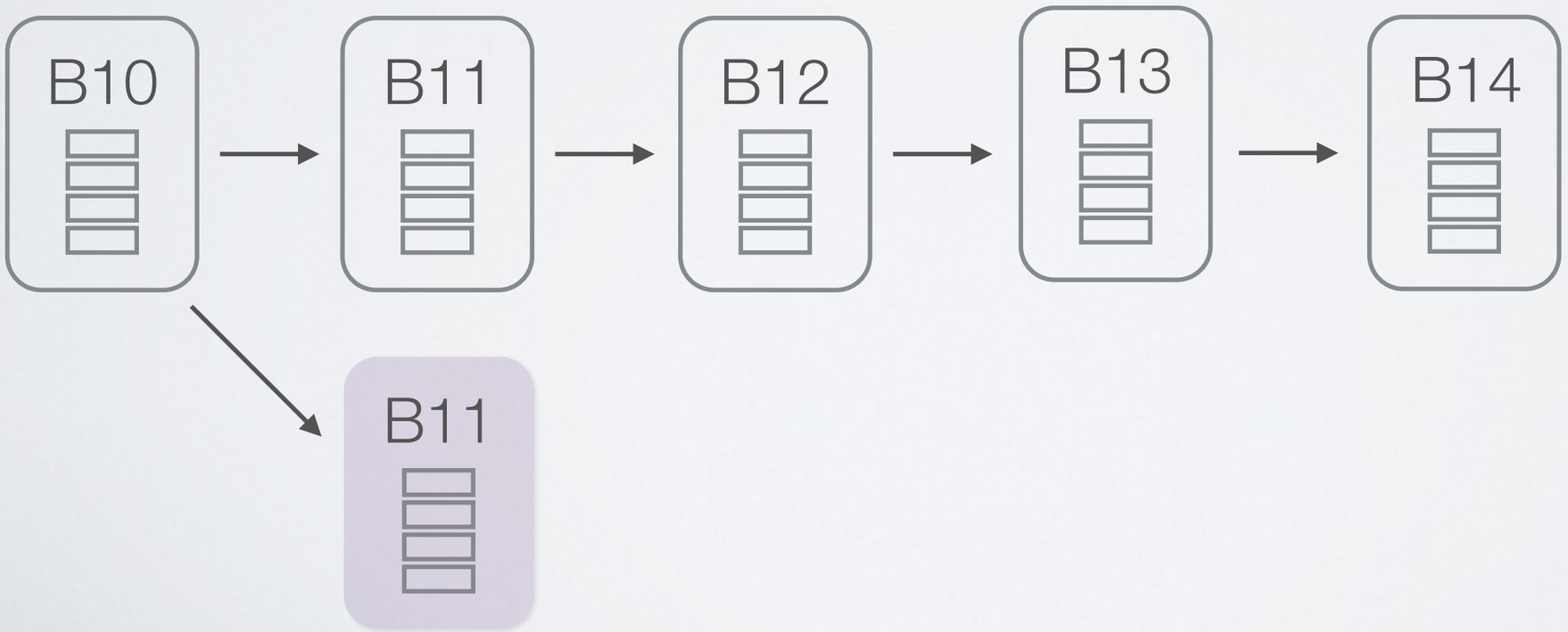


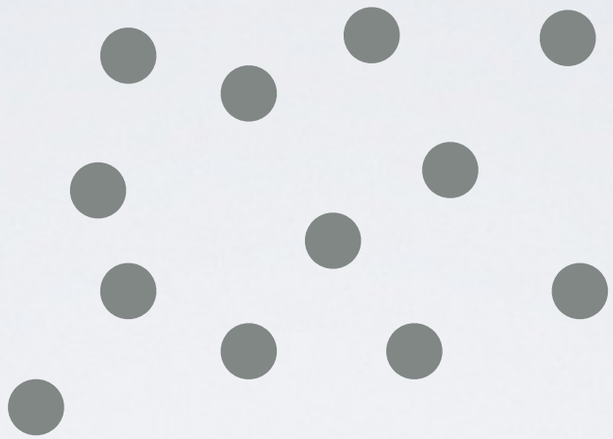


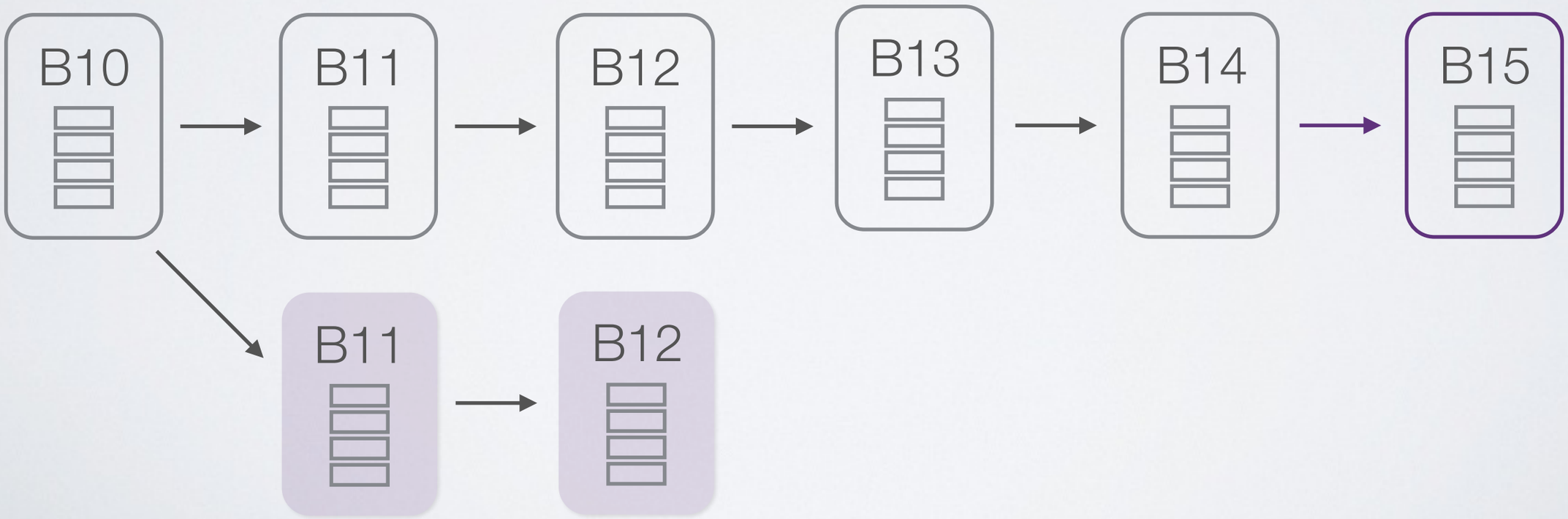


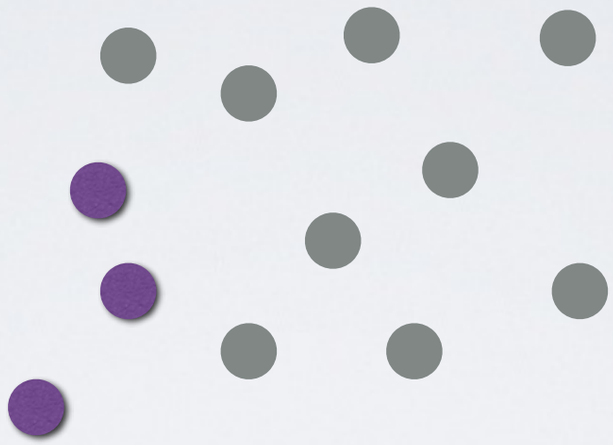

B10
B11
B12
B13
B14

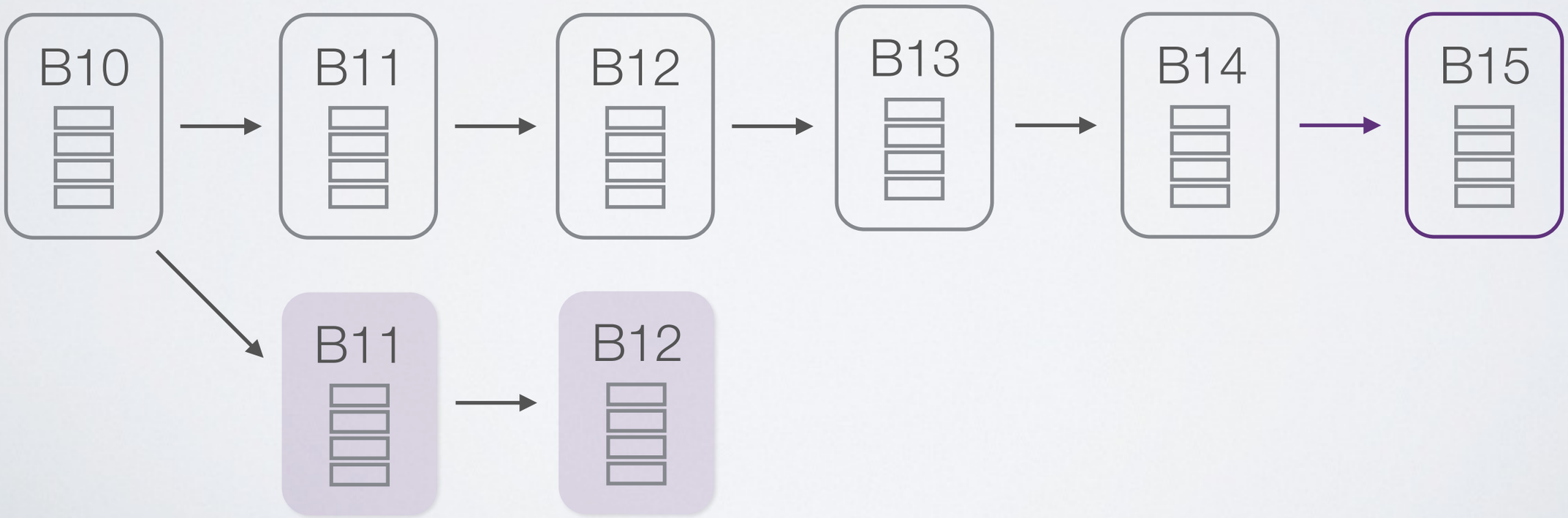


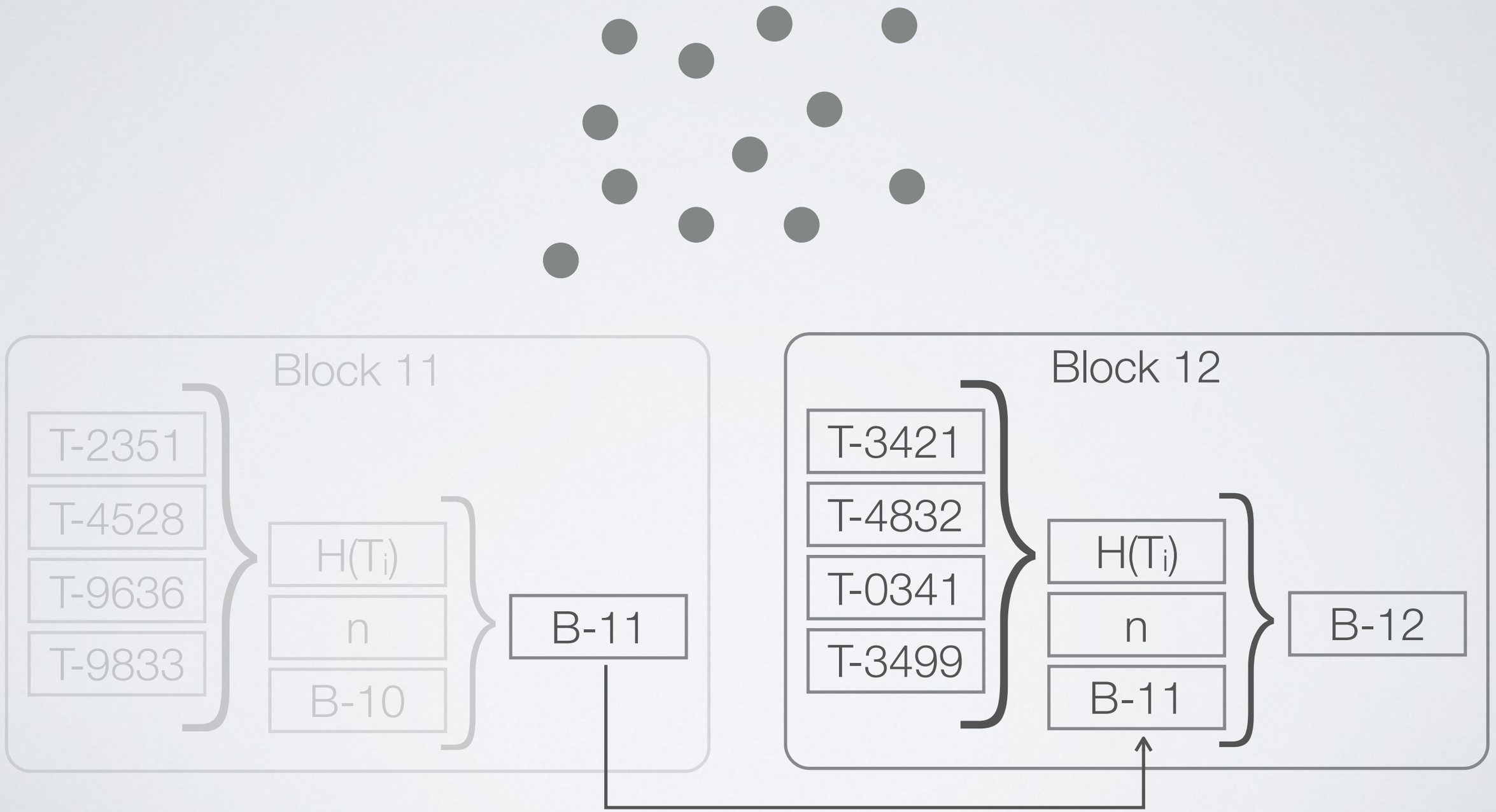

B10
B11
B12
B13
B14
B11




B10
B11
B12
B13
B14
B15
B11
B12



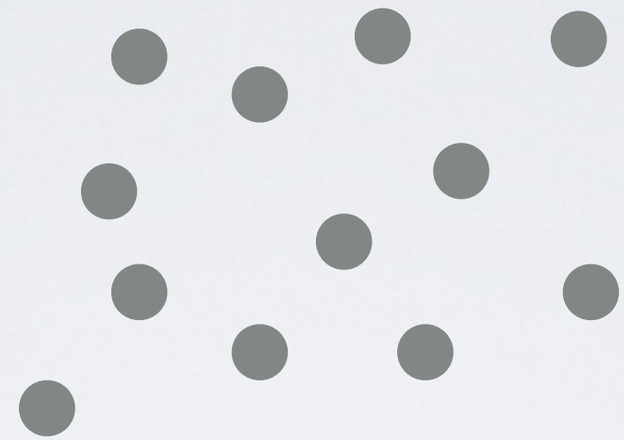

B10
B11
B12
B13
B14
B15
B11
B12

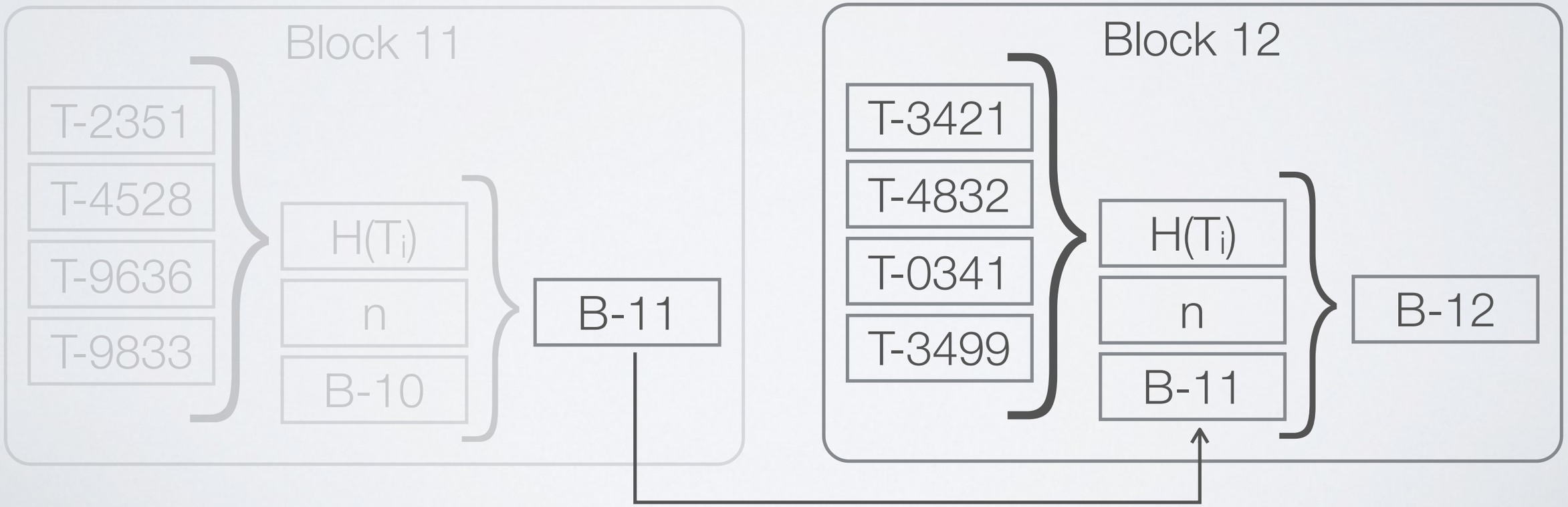

Block 11
T-2351
T-4528
T-9636
T-9833
H(Ti)
n
B-10
B-11
Block 12
T-3421
T-4832
T-0341
T-3499
H(Ti)
n
B-11
B-12

B-12 = H($H(T_i)$ || n || B-11)

= 00000000000XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Work = (2^n)

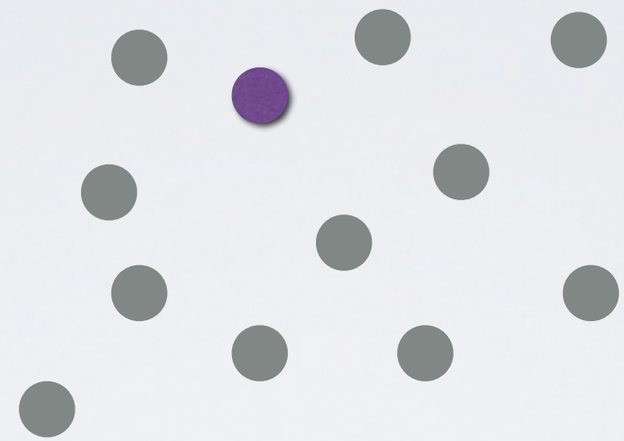


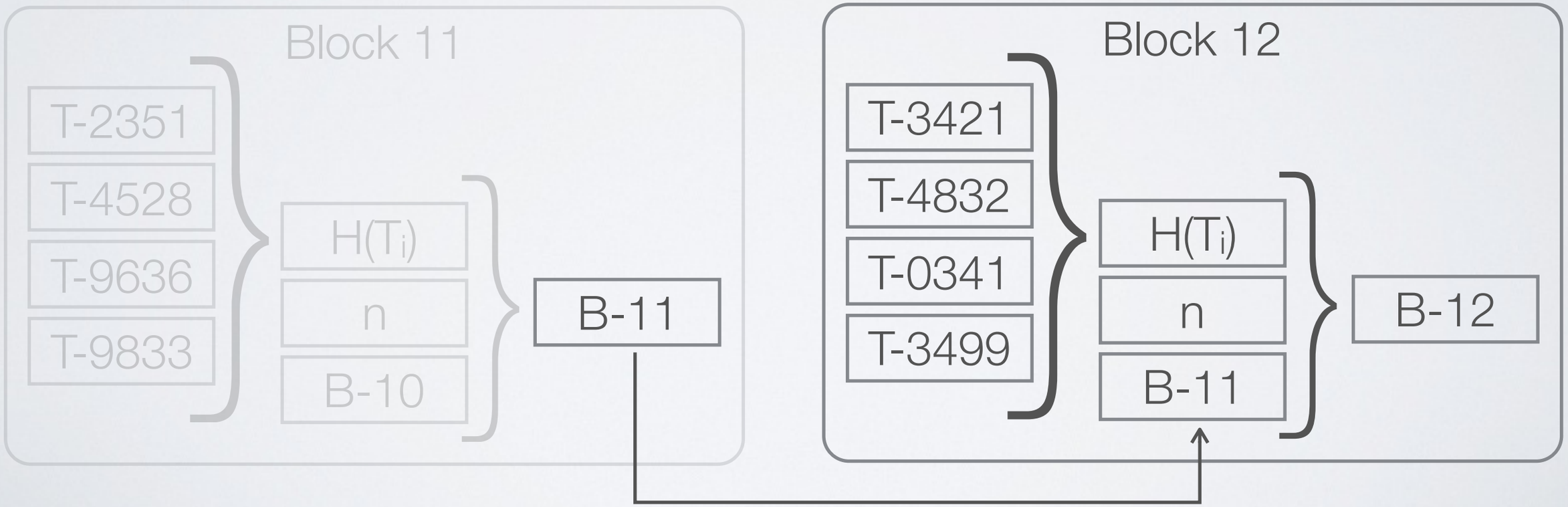


B-12 = H($H(T_i)$ || n || B-11)

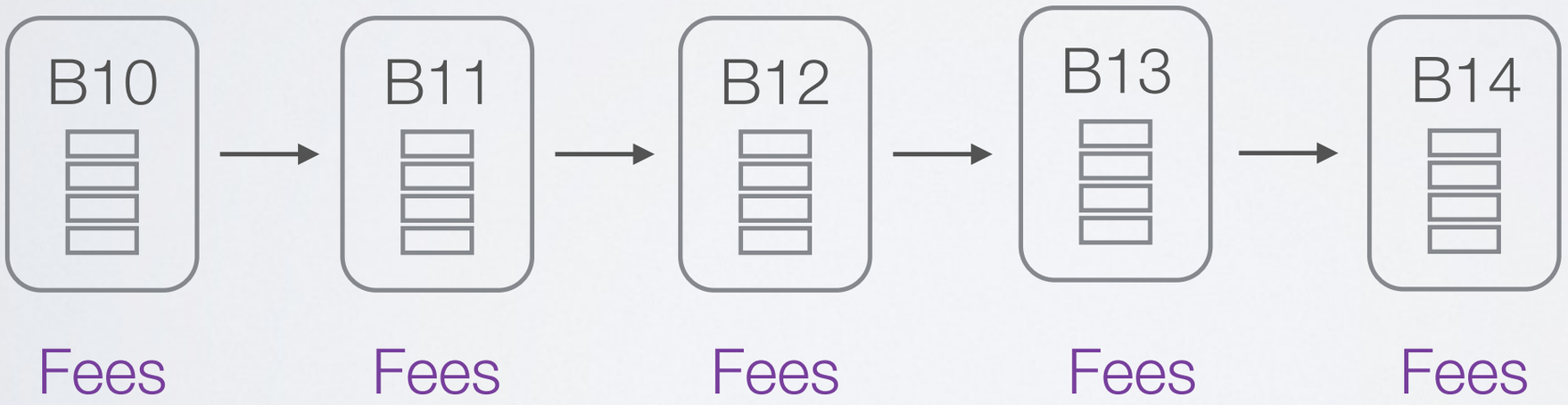
= 00000000000XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

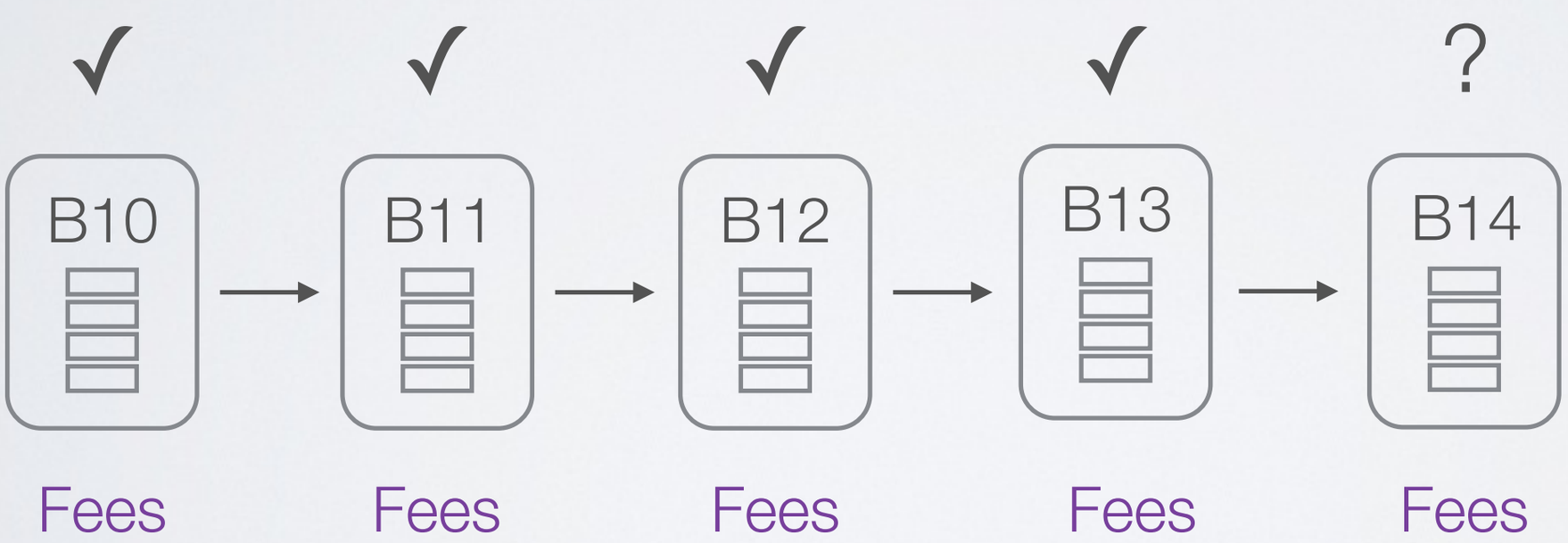
Random Node

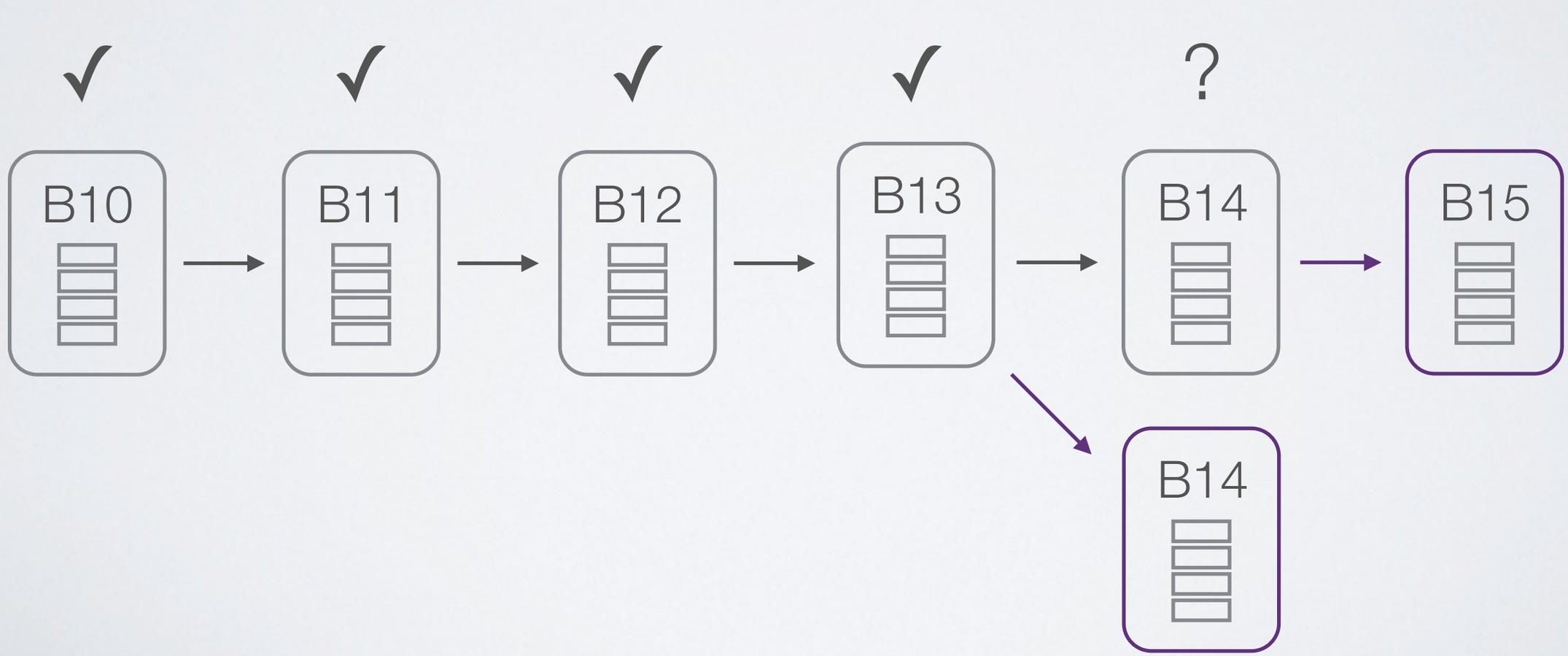


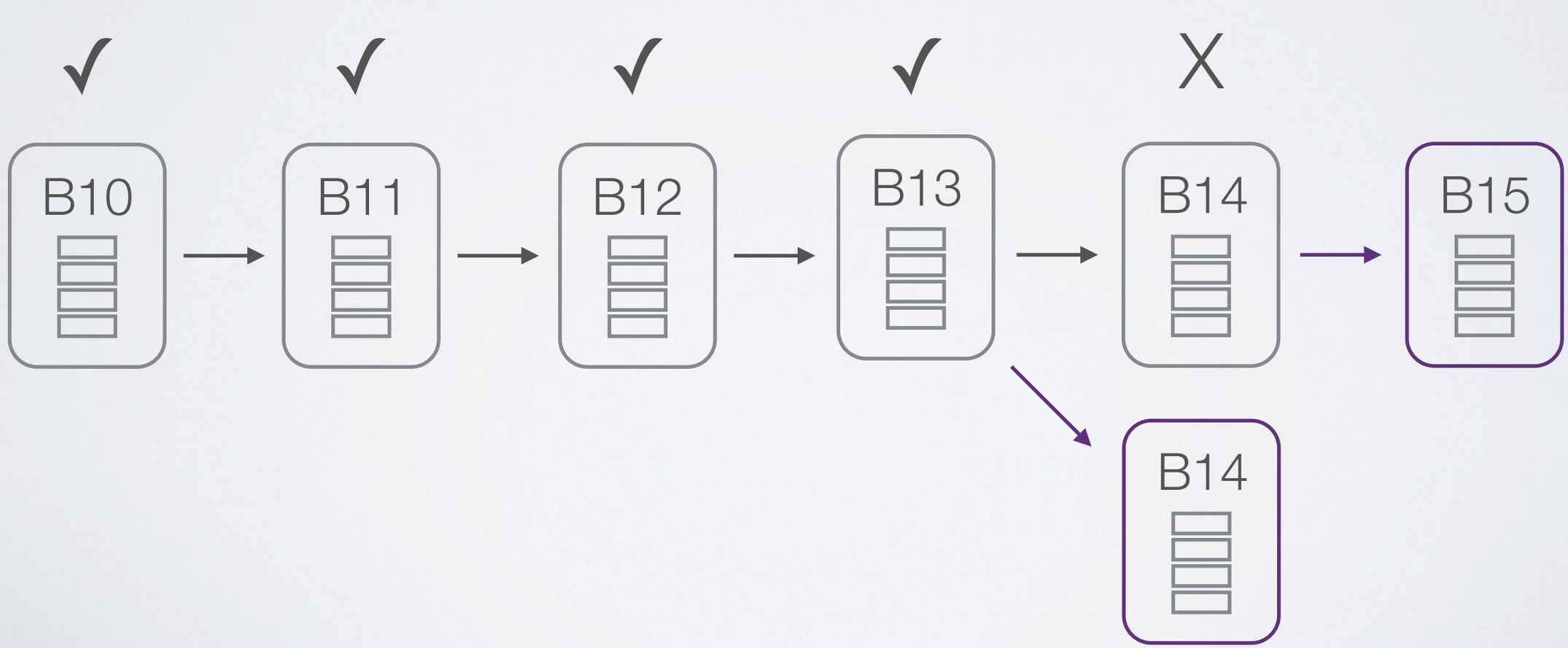


Incentive Compatibility

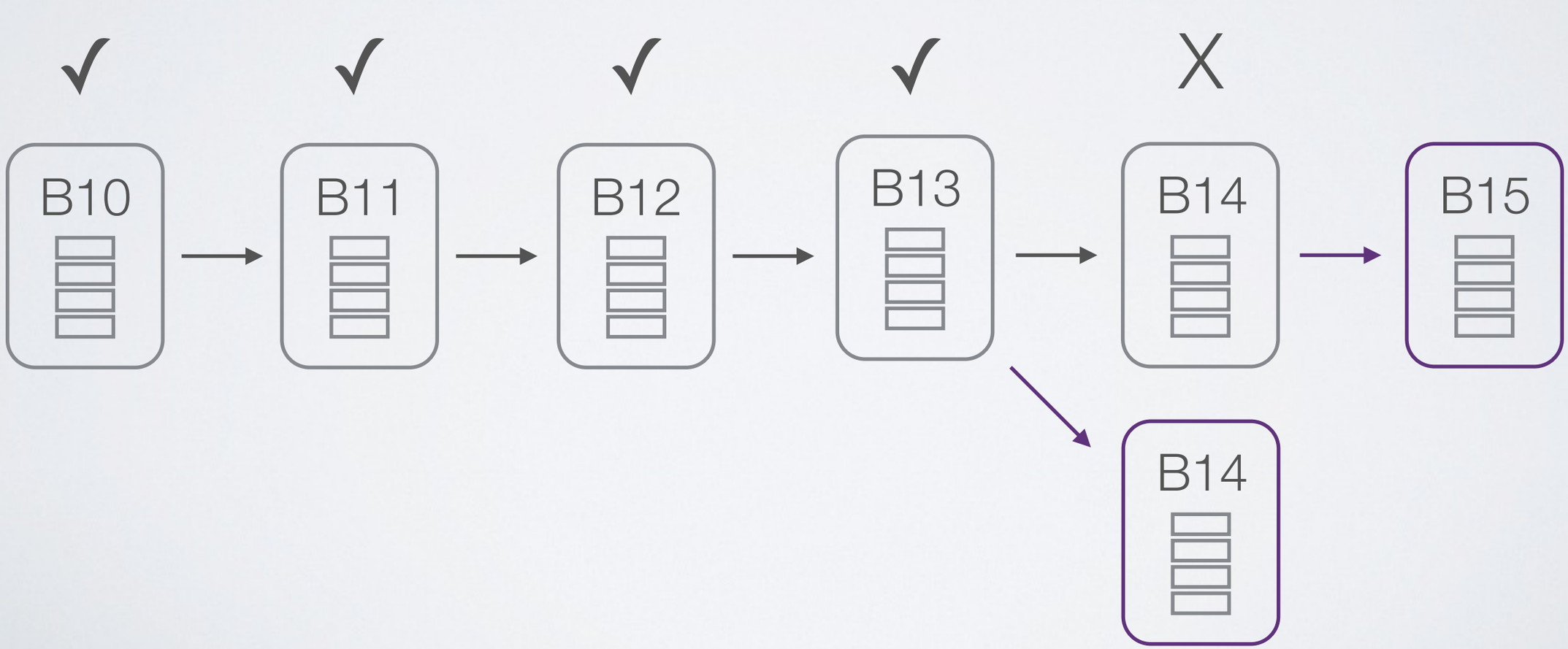



✓
✓
✓
✓
?
B10
B11
B12
B13
B14
Fees
Fees
Fees
Fees
Fees

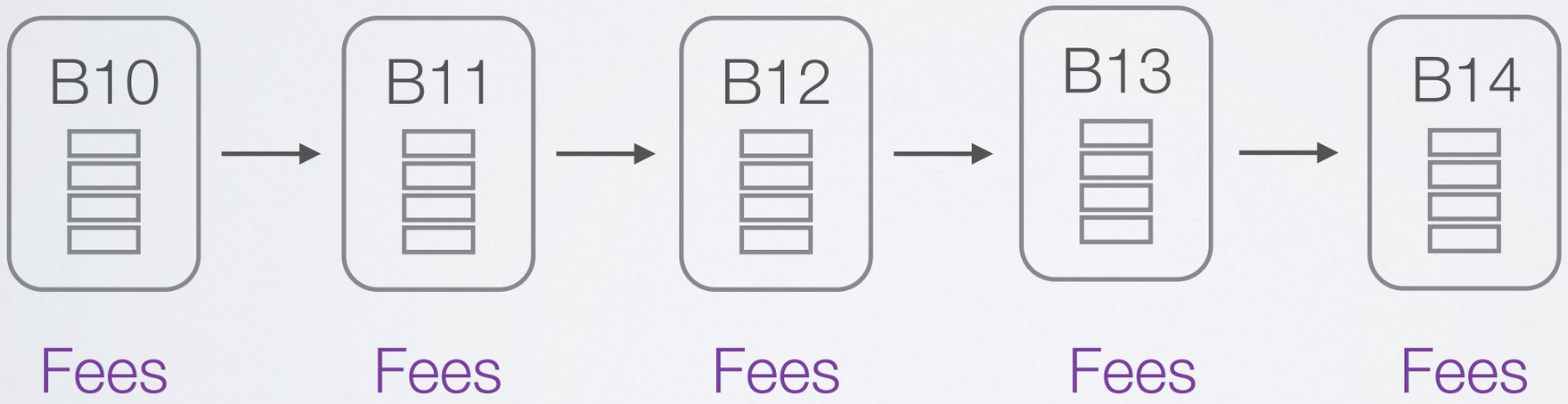

✓
✓
✓
✓
?
B10
B11
B12
B13
B14
B15
B14


✓
✓
✓
✓
X
B10
B11
B12
B13
B14
B15
B14

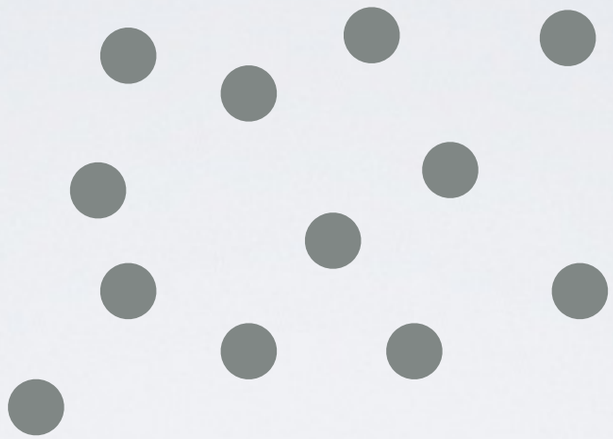
It pays to verify



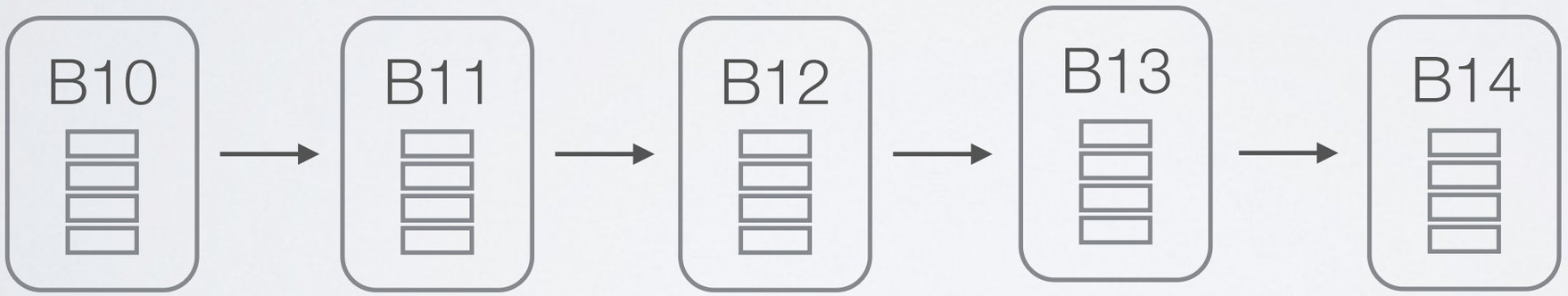
Initial Distribution (Minting)



Initial Distribution (Minting)



Nodes = “Miners”



Fees

Mint

Fees

Mint

Fees

Mint

Fees

Mint

Fees

Mint

Initial Distribution (Minting)

Newly minted coins offset expenses (seignorage)

This allows lower fees

Effectively: minted coins are distributed to the users in the form of lower fees

Circulation limited to 21M BTC (~Year 2140)

Challenge: Double Spend

Consider: two transactions are broadcast & both spend the same BTC

Which one will be included in blockchain?

Consensus will form but will take ~6 blocks (~1 hour) for high assurance. Too long to wait in some cases.

Detailed Use Case:

Decentralized Order Books

Exchanges

Hundreds of projects on decentralized exchanges

Zoom in on core technical component: order book

Goal: understand the landscape of options

An order book is a ledger and blockchains give you distributed ledgers, so easy right?

Original Order Book

Type	*Price*	*Volume*
Offer	155.00	300
Offer	152.50	120
Offer (Best)	152.00	100
Bid (Best)	148.00	75
Bid	147.00	200
Bid	146.60	100
Bid	146.50	50

Digital assets being sold for digital money (both on same blockchain)

Original Order Book

Type	*Price*	*Volume*
Offer	155.00	300
Offer	152.50	120
Offer (Best)	152.00	100
Bid (Best)	148.00	75
Bid	147.00	200
Bid	146.60	100
Bid	146.50	50

New Order

Bid	152.10	500

Updated Order Book

Type	*Price*	*Volume*
Offer	155.00	300
Offer (Best)	152.50	120
Bid (Best)	152.10	400
Bid	148.00	75
Bid	147.00	200
Bid	146.60	100
Bid	146.50	50

Order Book

Goal: continuous, price-time priority

Issues:

Order Book

Goal: continuous, price-time priority

Issues:

- Nodes drop competitive orders

Sent transactions propagate around a P2P network before being added to blockchain

Order Book

Goal: continuous, price-time priority

Issues:

- Nodes drop competitive orders
- No way to establish time

Each node has unsynchronized clock, transactions can enter at different ends of the network

Order Book

Goal: continuous, price-time priority

Issues:

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches and slow

Bitcoin updates every 10m, LiteCoin 2.5m, Ethereum 17s

Order Book

Goal: continuous, price-time priority

Issues:

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches and slow
- Miners drop competitive orders

In a blockchain, miners are free to compose their block any way they want

Order Book

Goal: continuous, price-time priority

Issues:

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches and slow
- Miners drop competitive orders
- Miners front-run well-priced orders

Miners can see the future and have final word

Order Book

Trusted Blockchain (90s)

Order Book

Open Blockchain

~~Order Book~~

Open Blockchain

Functional Equivalent

Order Book

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches
- Miners drop competitive orders
- Miners front-run well-priced orders

Broadcast to all known neighbours

Order Book

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches
- Miners drop competitive orders
- Miners front-run well-priced orders

Call markets: open/closing cross, crossing networks, etc.

Market opens, orders pile up, randomly close (lit) market, match orders

Order Book

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches
- Miners drop competitive orders
- Miners front-run well-priced orders

Matching: Lowest ask matched to highest bid until no more matching possible

Report the market clearing price

Order Book

- Nodes drop competitive orders
- No way to establish time
- Blockchain: updated in batches
- Miners drop competitive orders
- Miners front-run well-priced orders

Miners keep spread: spreads can replace fees & miners can execute at best price

Miners commit to orders before solving and cannot stuff orders into solved block

Detailed Use Case:

Proof of Solvency

Joint Work

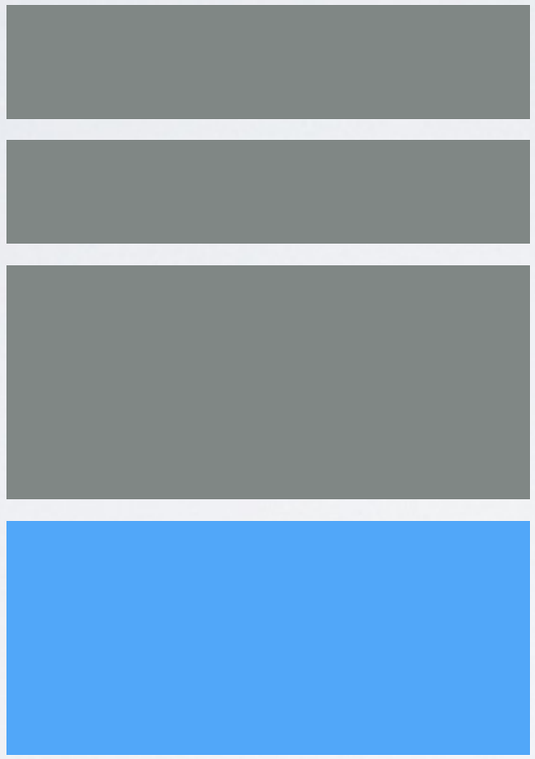
Gaby Dagher - Boise State University
Benedikt Bünz - Stanford
Joe Bonneau - Stanford & EFF
Dan Boneh - Stanford

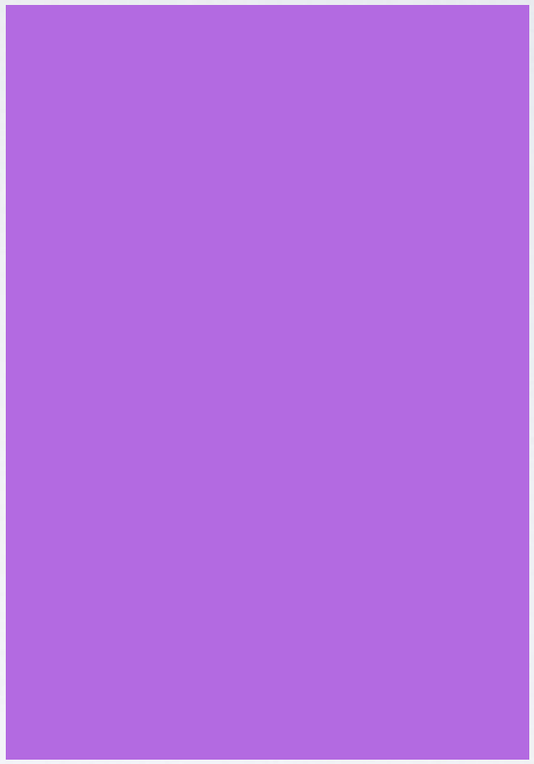
ACM CCS 2015

Balance Sheet

Liabilities

Equity



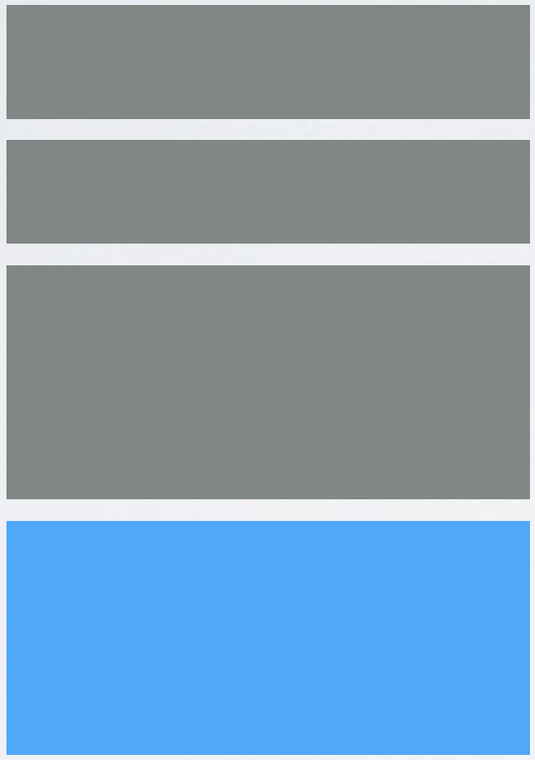


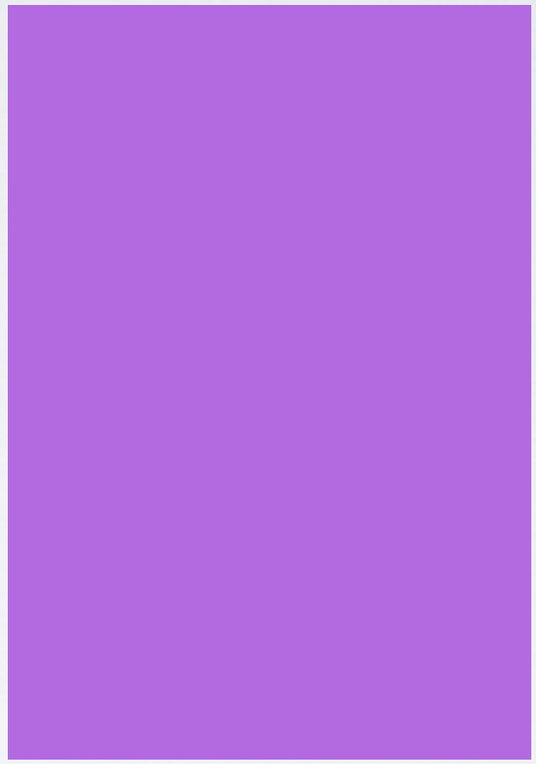
Assets
(on blockchain)

Balance Sheet

Liabilities

Equity





Assets
(on blockchain)

Solvent? Proof for private corporations directly to the customers with no auditors (P2P auditing)

Exchange Services

Provide mechanisms for depositing Bitcoin and fiat currency into an account

Provide an order book where you can buy/sell Bitcoin

Trades are cleared/settled automatically

You can withdrawal at any time, but for Bitcoin, users like keeping money on an exchange

A Recent Headline

FINANCIAL TIMES

Last updated: February 28, 2014 6:35 pm

Bitcoin exchange Mt Gox files for bankruptcy protection

By Ben McLannahan in Tokyo

A Bitcoin trader holds a placard to protest against Mt Gox in Tokyo

The Bitcoin exchange at the centre of a $480m heist has filed for bankruptcy protection, in a move that leaves thousands of virtual-currency investors in limbo.

Events unfolding at Tokyo-based Mt Gox, once the dominant platform for trading and storing Bitcoin, had drawn increasing attention over the past three weeks, as a freeze on withdrawals led to a shutdown of trading and uncertainty over the whereabouts of the company's chief executive, Mark Karpelès.

But on Friday evening Mr Karpelès surfaced to announce that Mt Gox would seek a court-led restructuring, with debts of Y6.5bn ($64m) and assets of Y3.9bn. About 750,000 Bitcoins belonging to customers and 100,000 belonging to the company had been lost, he said, in a theft detected on February 24.

Some virtual currency enthusiasts say that the example set by Mt Gox should encourage authorities to tighten their surveillance of this essentially unregulated landscape.

$480,000,000

FINANCIAL TIMES

Last updated: February 28, 2014 6:35 pm

Bitcoin exchange Mt Gox files for bankruptcy protection

By Ben McLannahan in Tokyo

A Bitcoin trader holds a placard to protest against Mt Gox in Tokyo

The Bitcoin exchange at the centre of a $480m heist has filed for bankruptcy protection, in a move that leaves thousands of virtual-currency investors in limbo.

Events unfolding at Tokyo-based Mt Gox, once the dominant platform for trading and storing Bitcoin, had drawn increasing attention over the past three weeks, as a freeze on withdrawals led to a shutdown of trading and uncertainty over the whereabouts of the company's chief executive, Mark Karpelès.

But on Friday evening Mr Karpelès surfaced to announce that Mt Gox would seek a court-led restructuring, with debts of Y6.5bn ($64m) and assets of Y3.9bn. About 750,000 Bitcoins belonging to customers and 100,000 belonging to the company had been lost, he said, in a theft detected on February 24.

Some virtual currency enthusiasts say that the example set by Mt Gox should encourage authorities to tighten their surveillance of this essentially unregulated landscape.

The New York Times | http://nyti.ms/1fo7M0A

BUSINESS DAY

Apparent Theft at Mt. Gox Shakes Bitcoin World

By NATHANIEL POPPER and RACHEL ABRAMS FEB. 25, 2014

The most prominent Bitcoin exchange appeared to be on the verge of collapse late Monday, raising questions about the future of a volatile marketplace.

On Monday night, a number of leading Bitcoin companies jointly announced that Mt. Gox, the largest exchange for most of Bitcoin's existence, was planning to file for bankruptcy after months of technological problems and what appeared to have been a major theft. A document circulating widely in the Bitcoin world said the company had lost 744,000 Bitcoins in a theft that had gone unnoticed for years. That would be about 6 percent of the 12.4 million Bitcoins in circulation.

Theft Unnoticed for Years

The New York Times | http://nyti.ms/1fo7M0A

BUSINESS DAY

Apparent Theft at Mt. Gox Shakes Bitcoin World

By **NATHANIEL POPPER** and **RACHEL ABRAMS** FEB. 25, 2014

The most prominent Bitcoin exchange appeared to be on the verge of collapse late Monday, raising questions about the future of a volatile marketplace.

On Monday night, a number of leading Bitcoin companies jointly announced that Mt. Gox, the largest exchange for most of Bitcoin's existence, was planning to file for bankruptcy after months of technological problems and what appeared to have been a major theft. A document circulating widely in the Bitcoin world said the company had lost 744,000 Bitcoins in a theft that had gone unnoticed for years. That would be about 6 percent of the 12.4 million Bitcoins in circulation.

Proof of Solvency

We *cannot* stop thefts

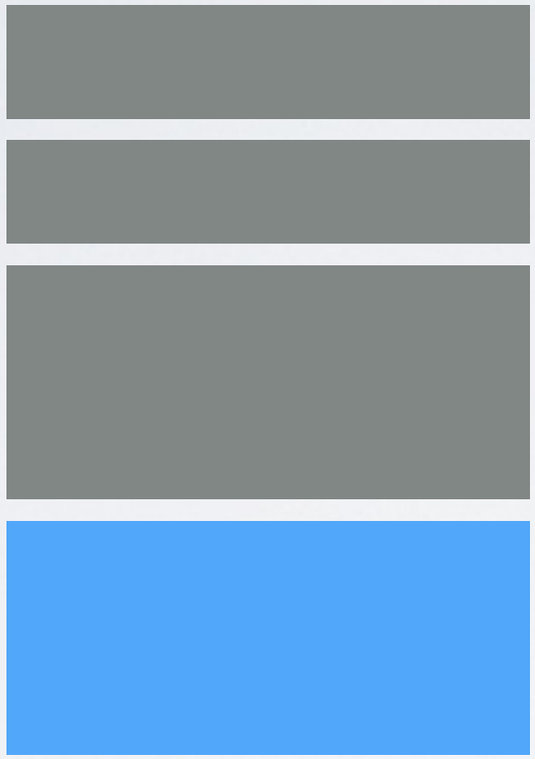
We *can* require exchanges' solvency to be proven

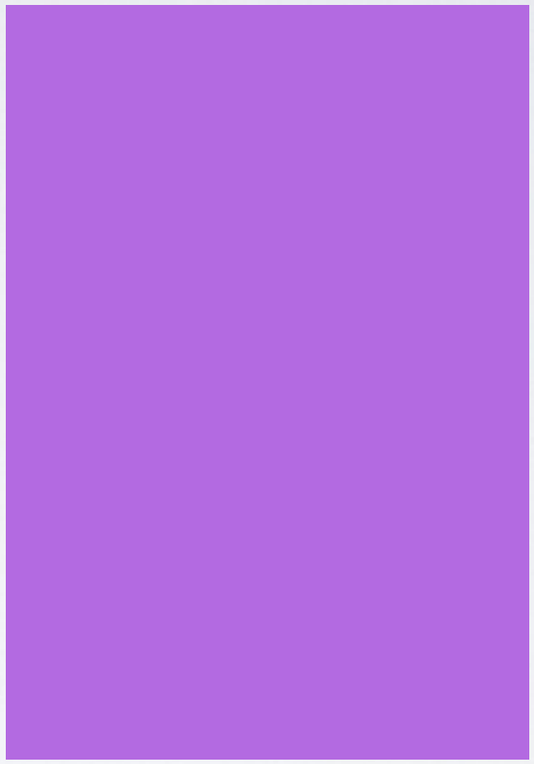
With some crypto, we can even prove solvency without revealing:

- Customer information
- Exchanges' total holdings
- Exchanges' addresses

Liabilities

Equity





Assets

Liabilities: customers can check correct inclusion of their liabilities in a total “encrypted” amount

Liabilities: everyone can check that no listed encrypted liability is a negative number

Assert an encrypted amount of total assets owned on a blockchain

Prove ownership of assets totalling this amount (by knowledge of signing key) without specifying the set

Show: [[Assets]] - [[Liabilities]] >= 0

Discussion

Having assets on a blockchain enable new applications

Possible do feed blockchain information into interesting protocols, whether on-blockchain or off-blockchain

Generalizable to a traditional commercial bank?

- Nobody does loans in digital currency
- If so, loan amounts could be included as assets
- Assumes loans are safe: how to quantify actual loan value in an agreeable way? (yield, credit risk, etc)