Bitcoin & Blockchains
Landscape & Future Directions

Jeremy Clark

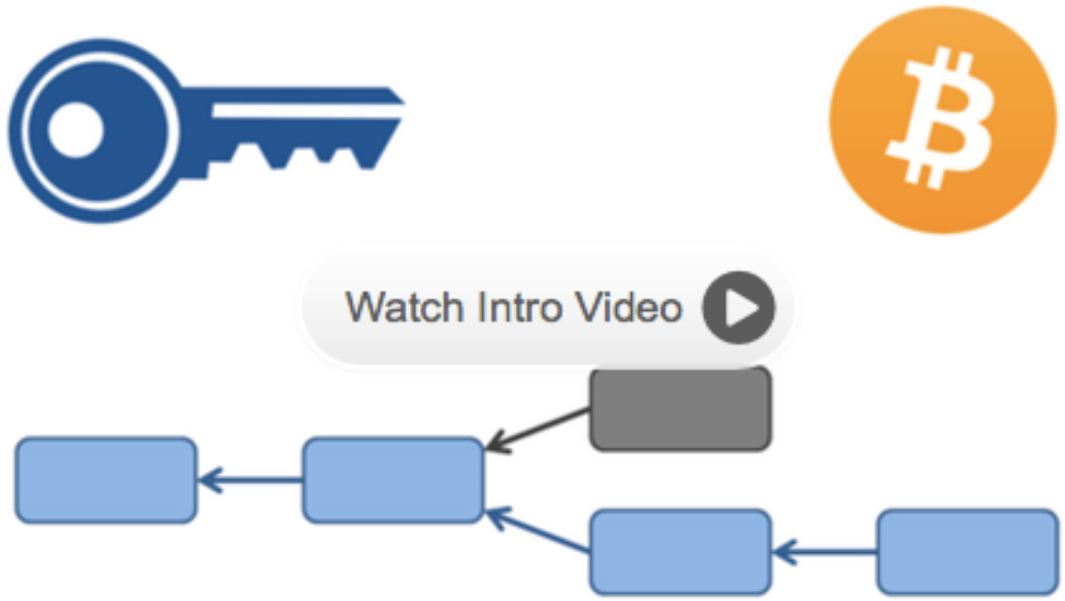
Jeremy Clark

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

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

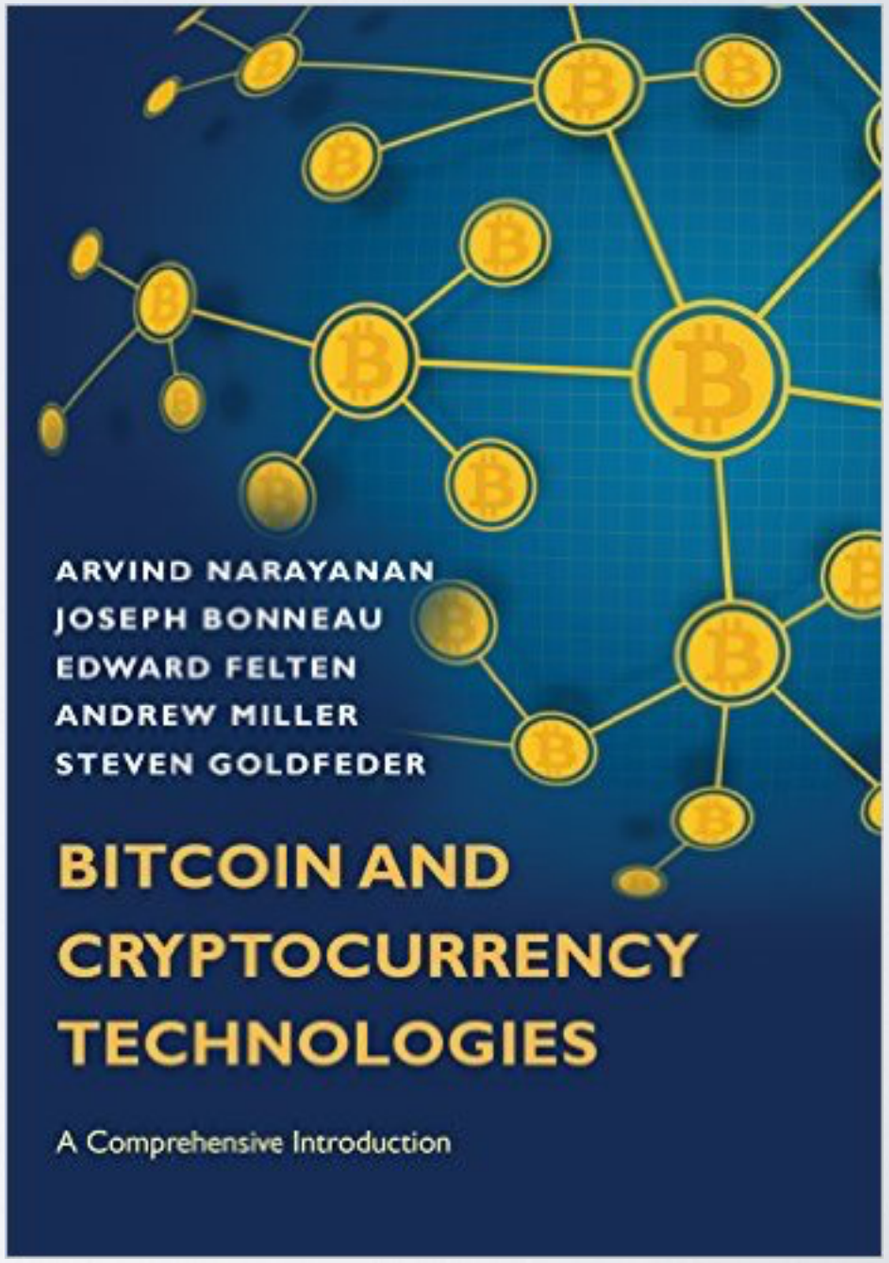
with a preface by Jeremy Clark

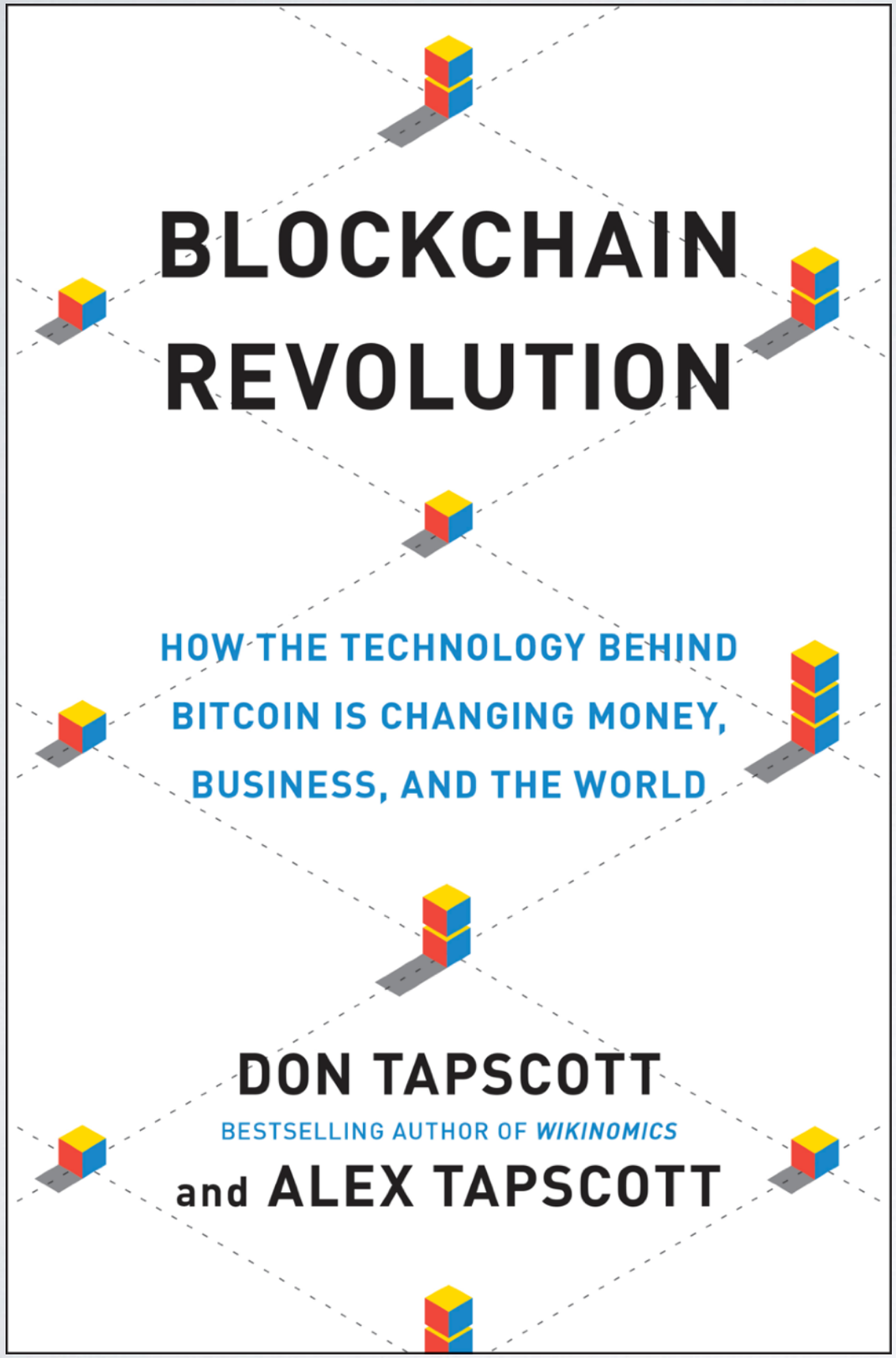
Draft — Feb 9, 2016

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.





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

ACC
Agora
AIMP
Allopass
b-money
BankNet
Bitbit
Bitgold
Bitpass

Many Schemes

PayPal

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

Expedia

Travel Purchase Order **$83.15 USD**
0.31322605 BTC

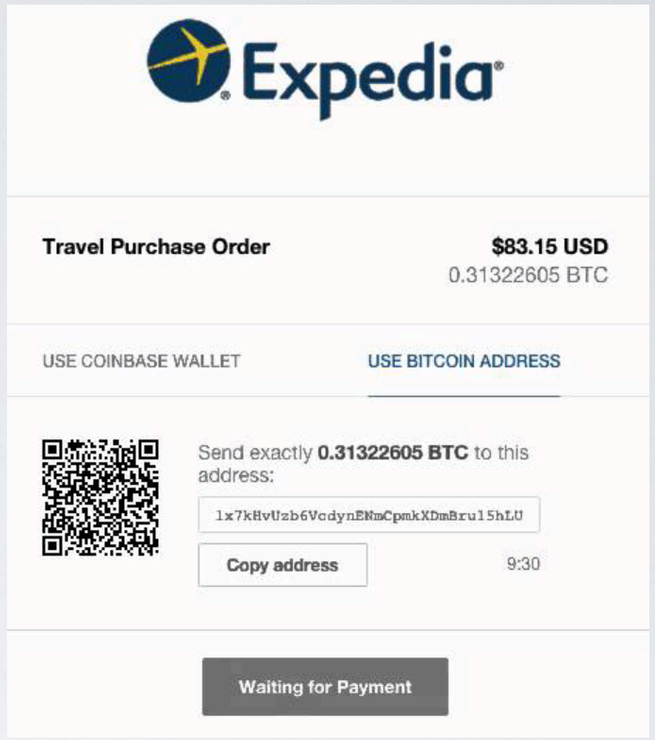
USE COINBASE WALLET | USE BITCOIN ADDRESS

Send exactly **0.31322605 BTC** to this address:

`1x7kHvUzb6VcdynENmCpmkXDmBrul5hLU`

Copy address 9:30

Waiting for Payment



Recent Trades (XBT/CAD)

1 - 15 of 250 trades

Time	Order	Price	Volume
17:16:14 +00:00	sell	C$580.193	0.33660000
17:00:50 +00:00	sell	C$578.291	2.00000000
16:36:44 +00:00	sell	C$578.641	0.18081567
16:36:40 +00:00	sell	C$578.641	0.80000000
16:36:39 +00:00	sell	C$578.641	2.25528436
16:03:06 +00:00	buy	C$582.002	0.03436414
15:55:20 +00:00	buy	C$581.649	0.48183239
15:55:19 +00:00	sell	C$581.649	0.47803974
15:53:01 +00:00	buy	C$584.186	0.07600000
15:23:26 +00:00	sell	C$582.624	0.42260000
15:09:46 +00:00	buy	C$581.855	0.07770000
13:28:01 +00:00	sell	C$578.001	0.73508491
13:28:01 +00:00	sell	C$578.120	3.26491509
13:23:37 +00:00	buy	C$581.077	16.28760000
13:23:36 +00:00	buy	C$579.315	10.71240000

Bitcoin Economics

- New BTC is introduced on a fixed schedule
- Currently 25 BTC (~$400K CAD) every 10 minutes
- This amount decreases over time
- There is hard cap of 21M BTC (8 decimal ticks)

- New BTC is claimed as seignorage to computers (miners) maintaining the ledger
- Unlike most digital cash, BTC is purposely hard to produce (to stall its creation to every 10 min) and computers compete to claim it
- Miners subsidize user fees with seignorage

Blockchain in a slide

Bitcoin was proposed in 2008

Under the covers, an open P2P network agrees on the set of valid transactions and records them

The blockchain is the data structure, and its update rules ensure trustless consensus

Recently, interest in blockchain as a general primitive to implementing decentralized ledgers

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

Properties

1) Non-equivocation
   - Different people at different times see the same thing
   - Not just “see” but “have”
   - Your local copy is the golden copy

2) Mitigated trust-assumptions
   - Bitcoin operates in a trustless environment
   - Distributed ledgers exist on a spectrum of trust

3) Transparency
   - Validated records require disclosure
   - Most useful for lit ledgers
   - Pseudonymity

4) Efficiency
   - Digitized assets can be **settled:**
     - Minutes/hours without trust
     - Seconds with trust or collateral
   - Distributed means no “clock on the wall”
     - Updates are “chunky” and no time priority
   - Computational effort required without trust

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

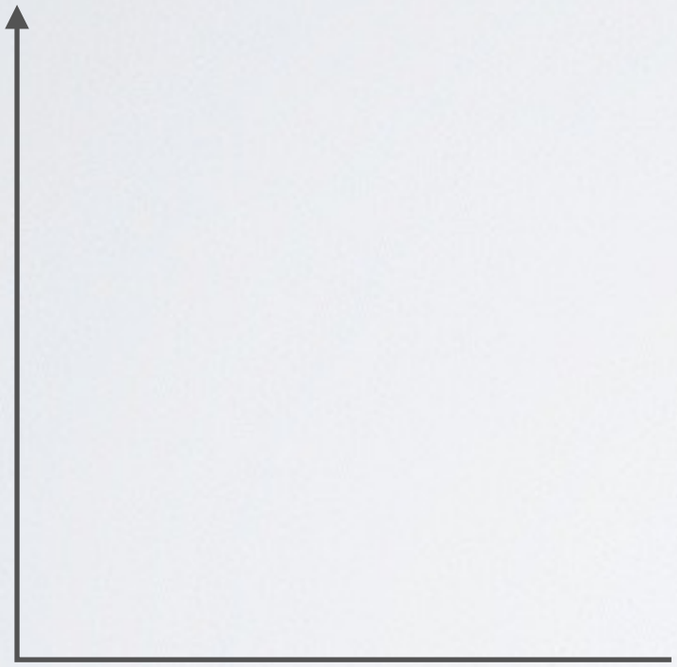
K_B
23 BTC

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

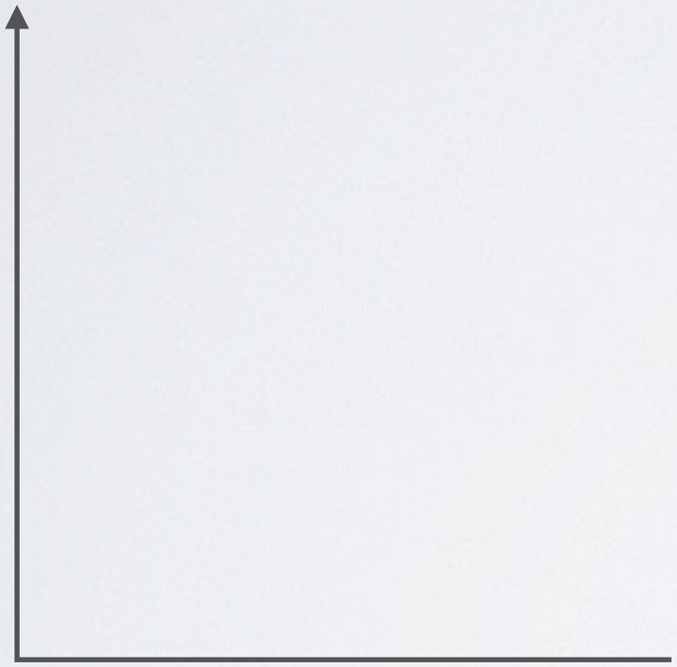
Transaction:	T-9833
Inputs:	{T-5292, K_{A1}, 3.5} {T-3928, K_{A2}, 2.5}
Outputs:	{K_{B1}, 5.0} {K_{A3}, 0.99}
Signature:	{Sig_{A1}} {Sig_{A2}}



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

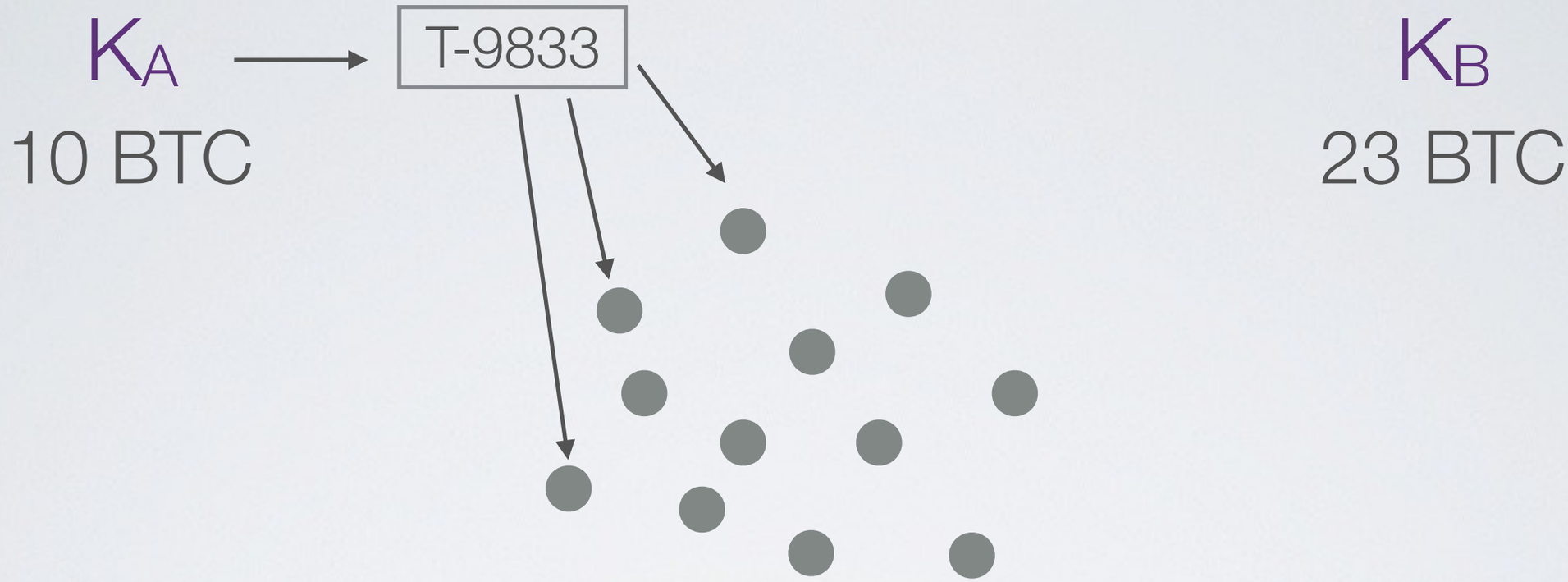
T-2351

T-4528

T-9636

T-9833

Ledger



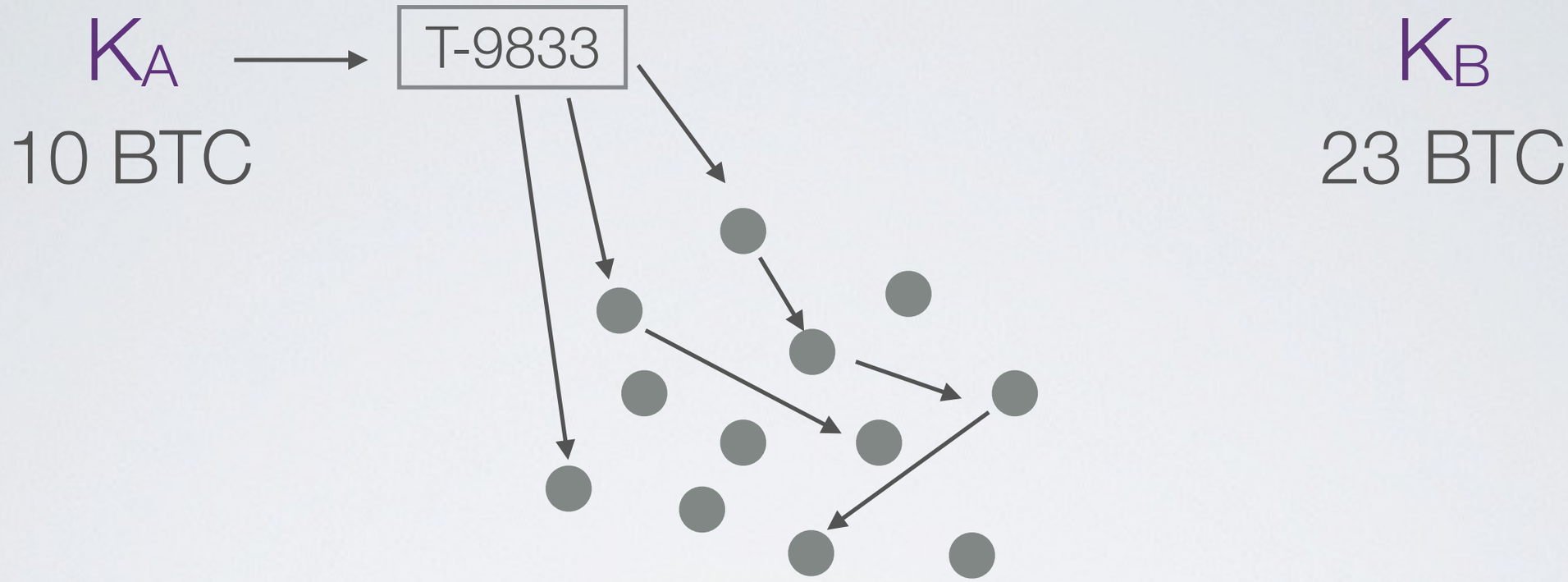
T-2351

T-4528

T-9636

T-9833

Ledger



T-2351

T-4528

T-9636

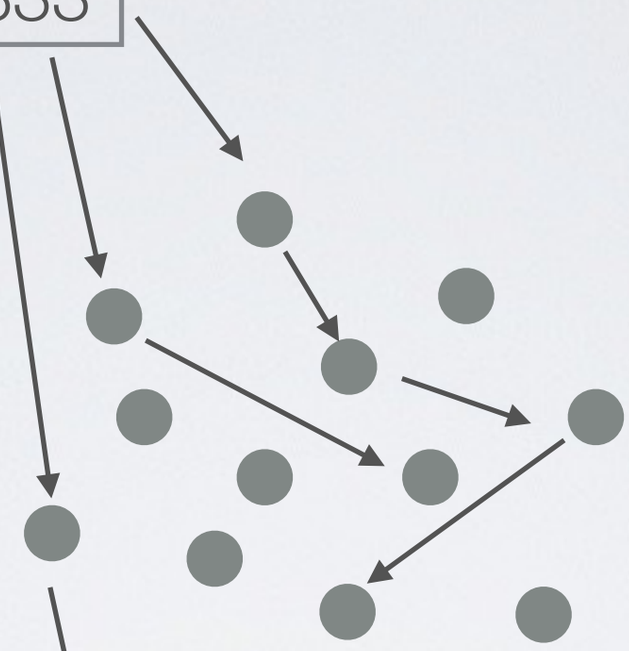
T-9833

Ledger

K_A

10 BTC

T-9833



K_B

23 BTC

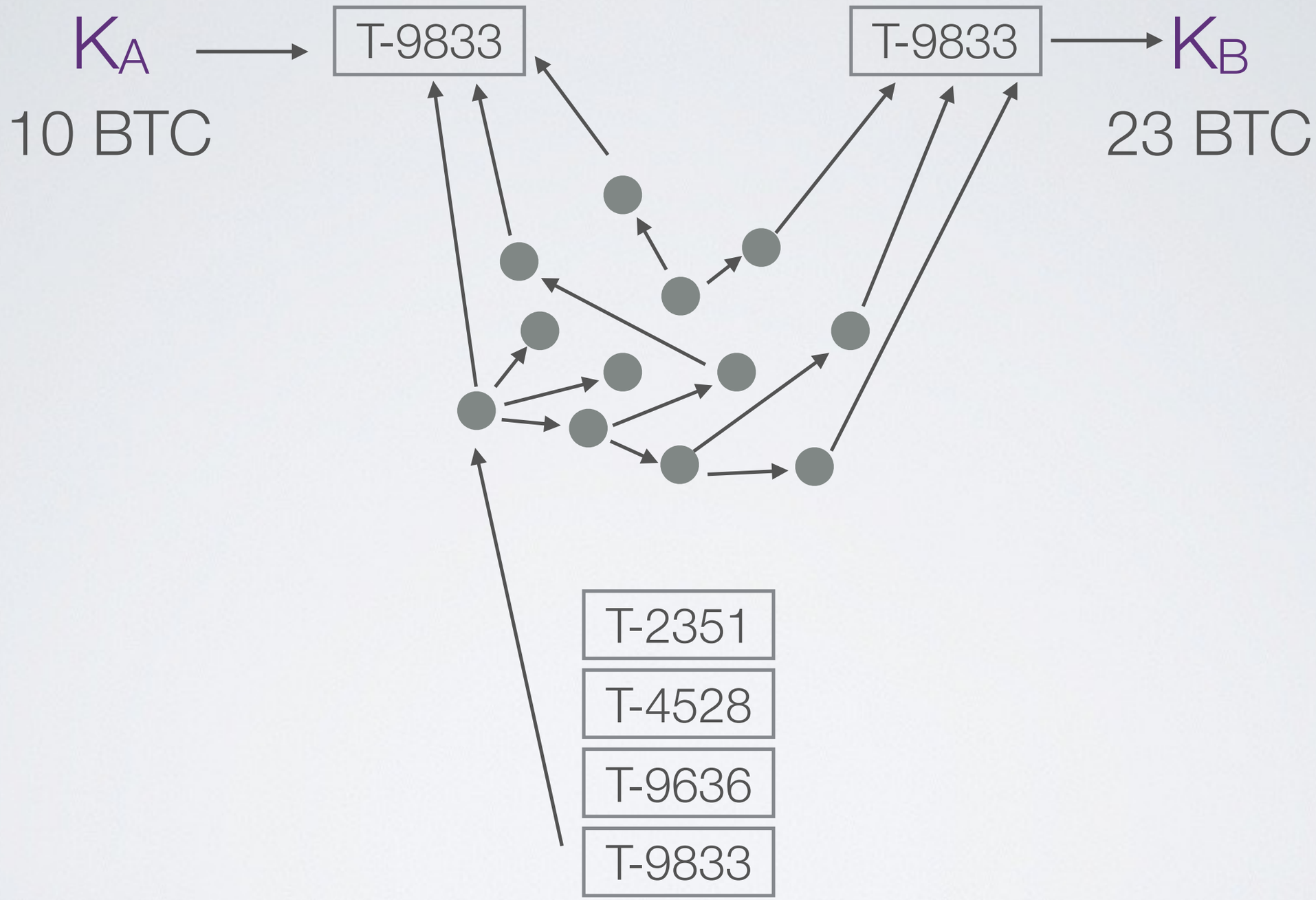
T-2351

T-4528

T-9636

T-9833

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

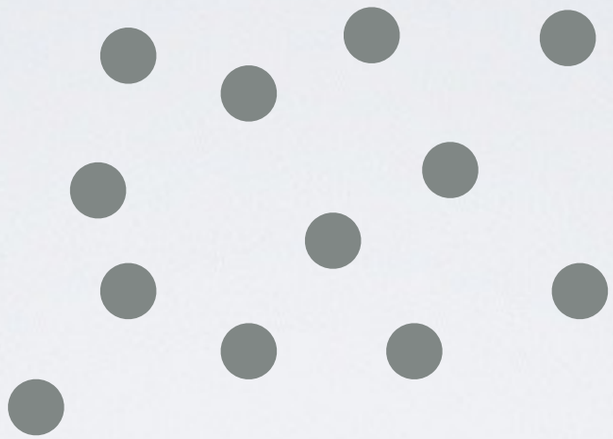
T-2351

T-4528

T-9636

T-9833

Ledger



Block 11

T-2351

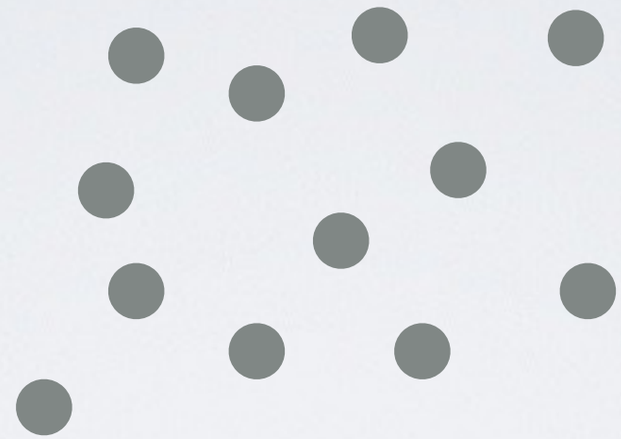
T-4528

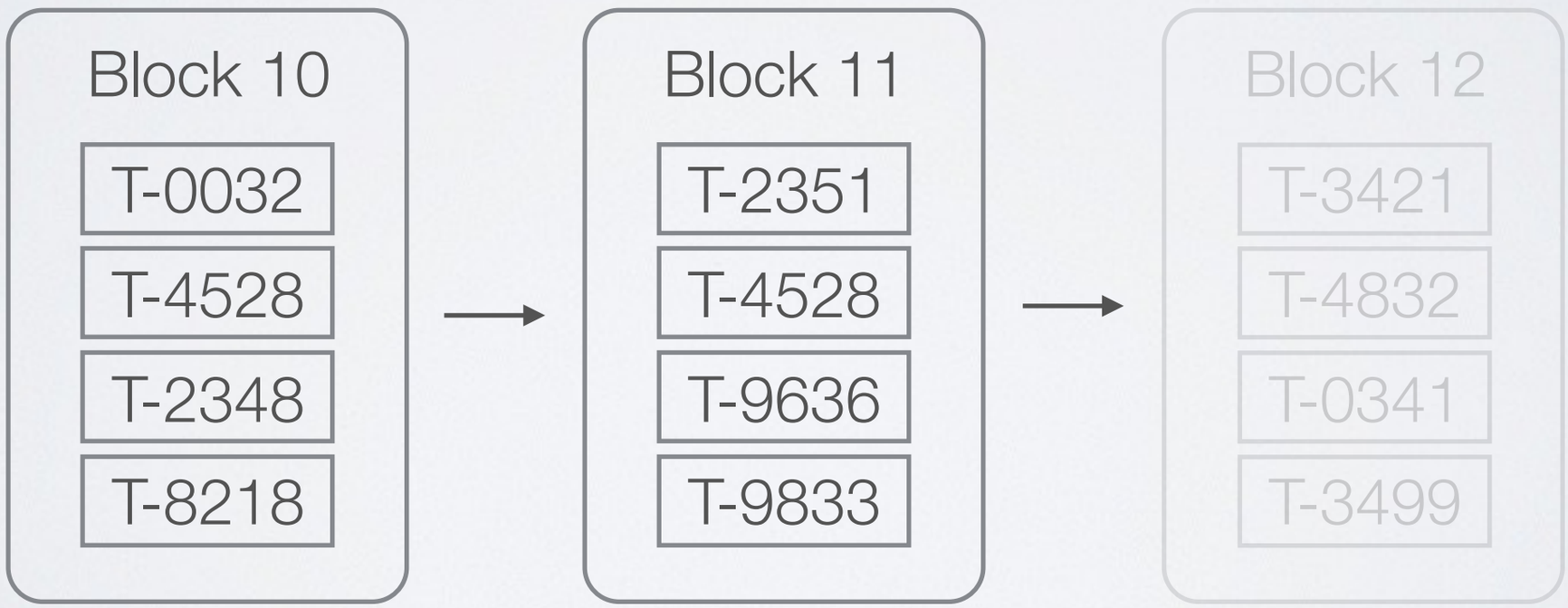
T-9636

T-9833

Ledger

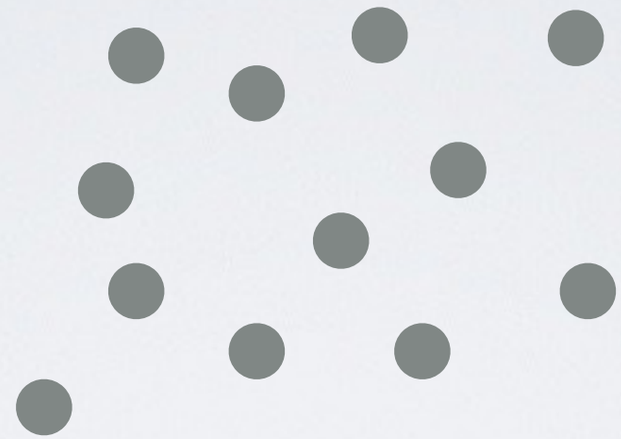
Hash Chain

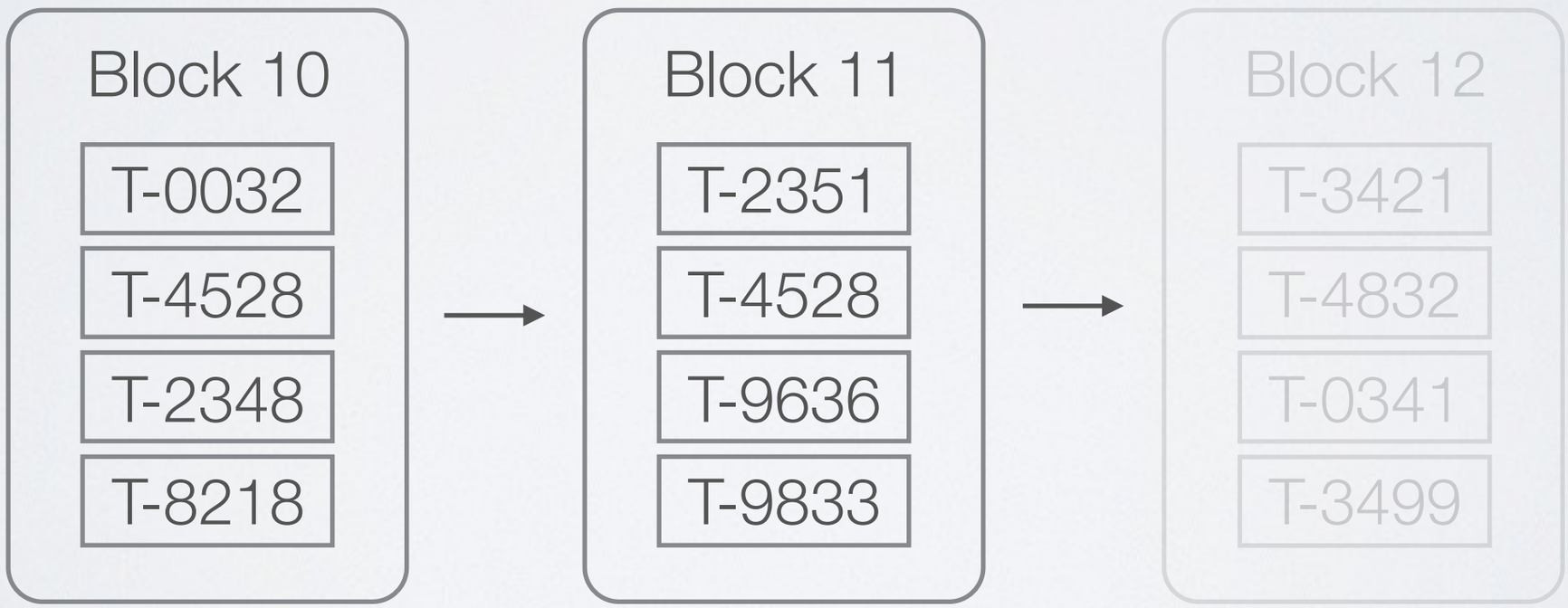


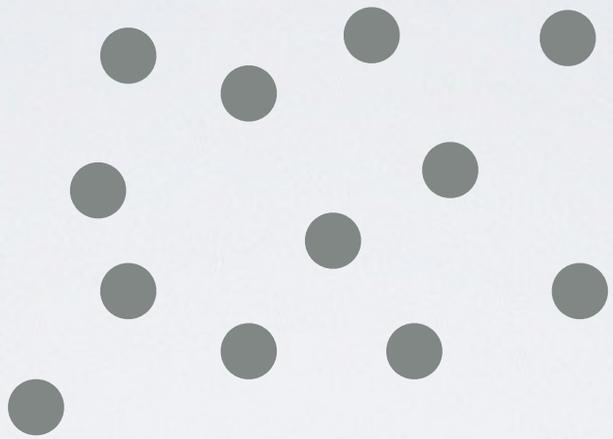


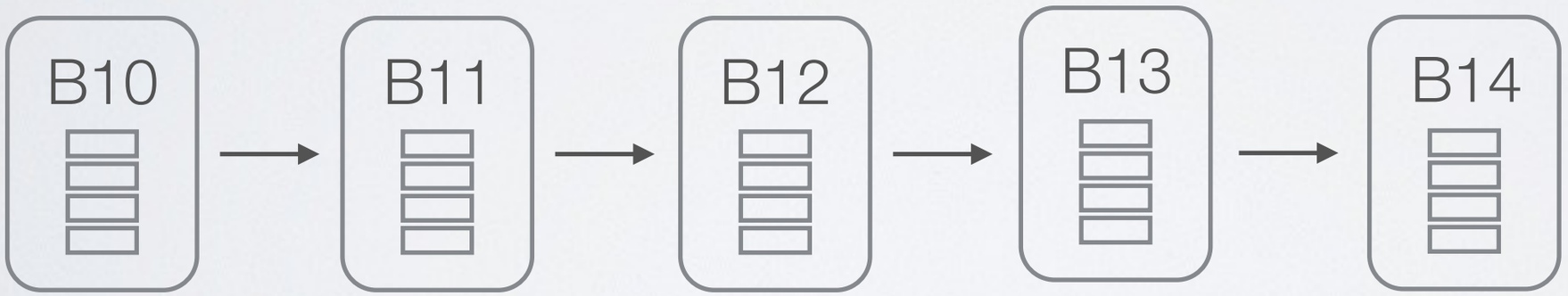
Ledger

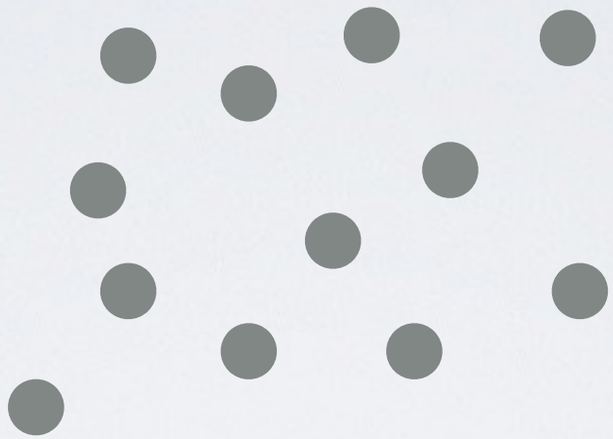
Rate-Limit Block Creation

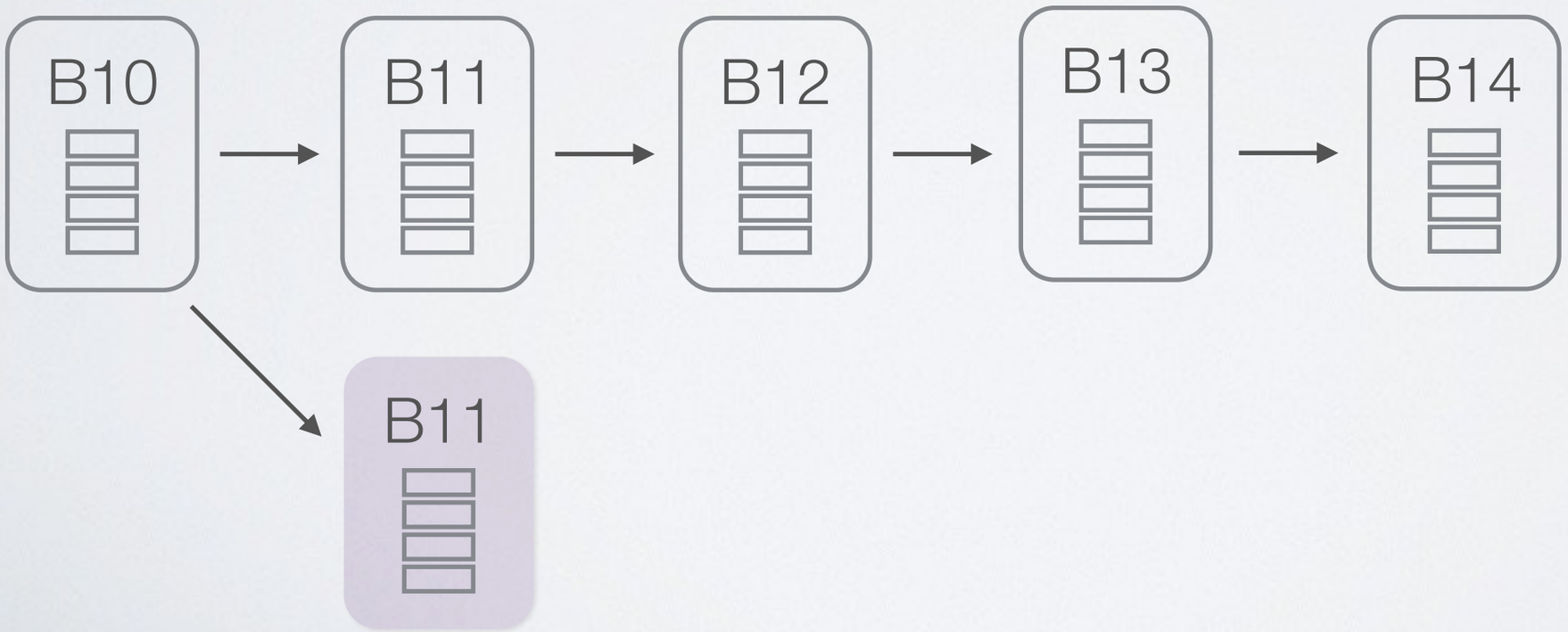


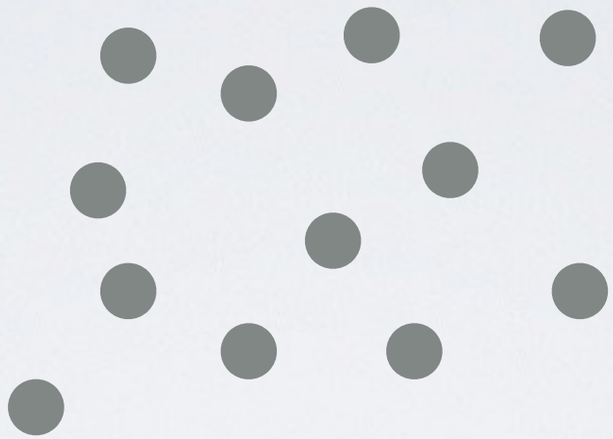


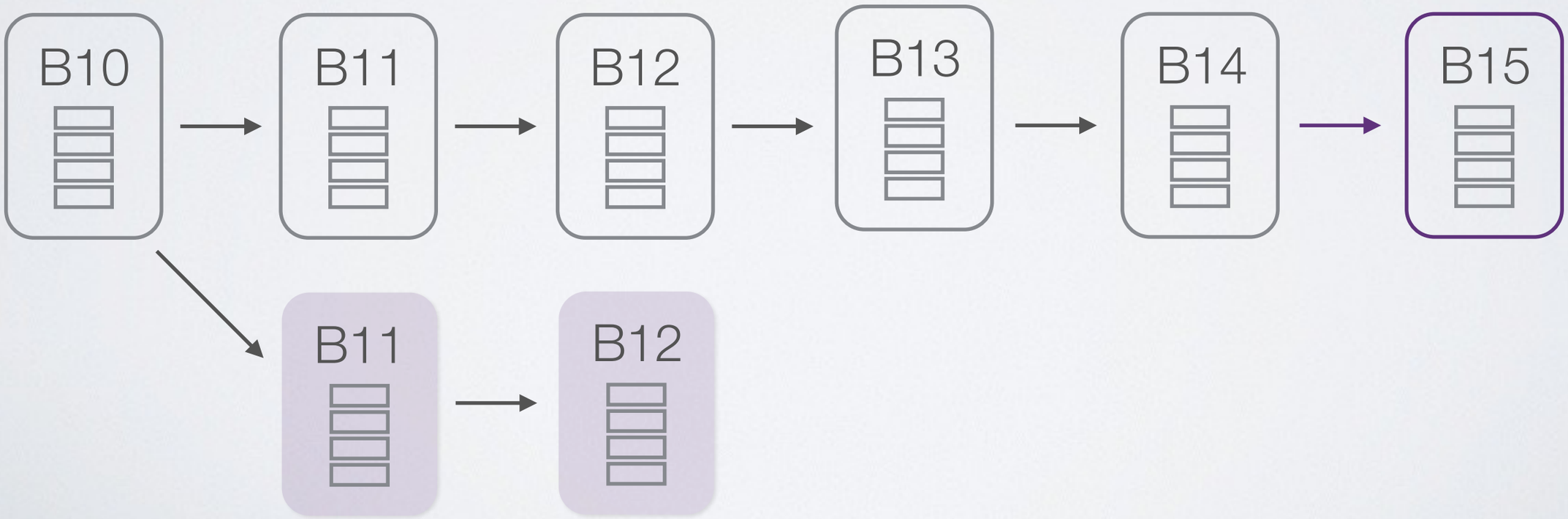


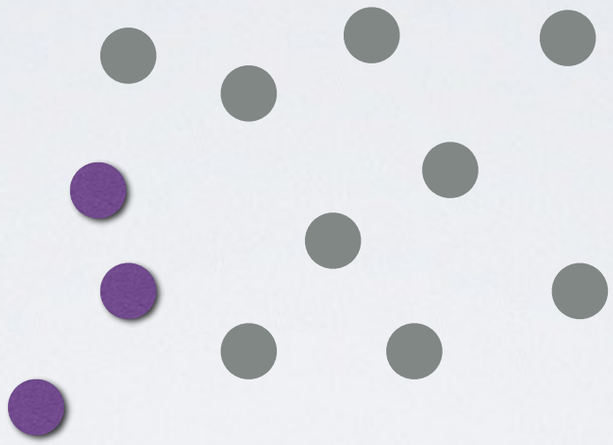

B10
B11
B12
B13
B14

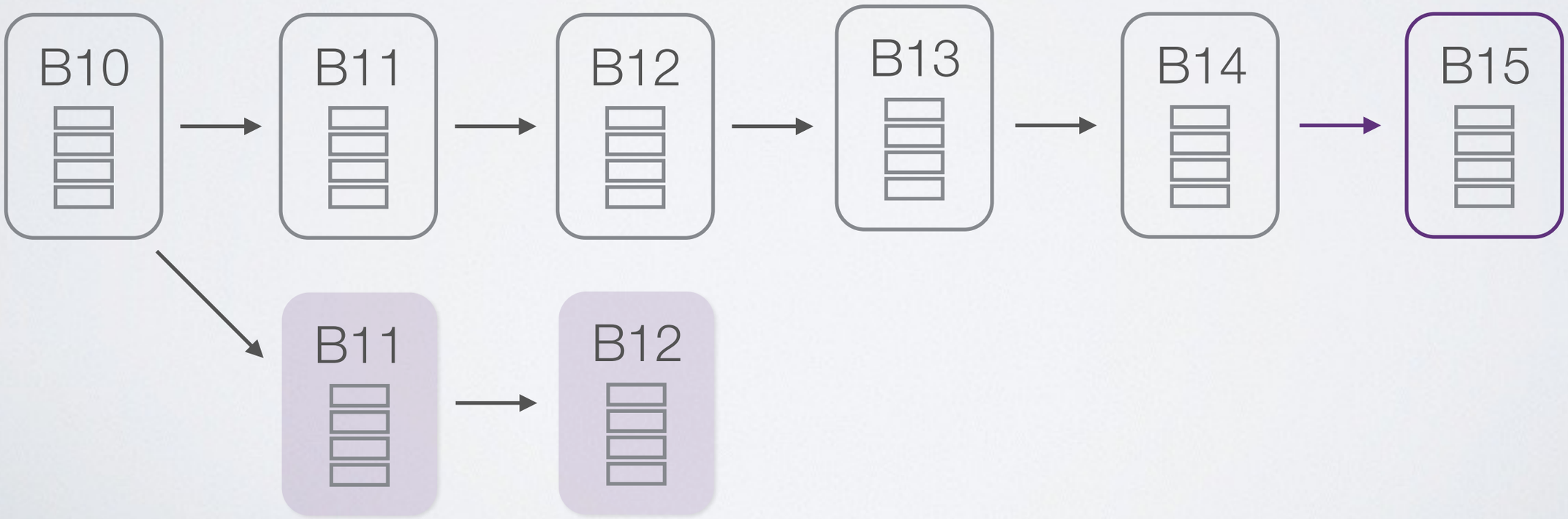


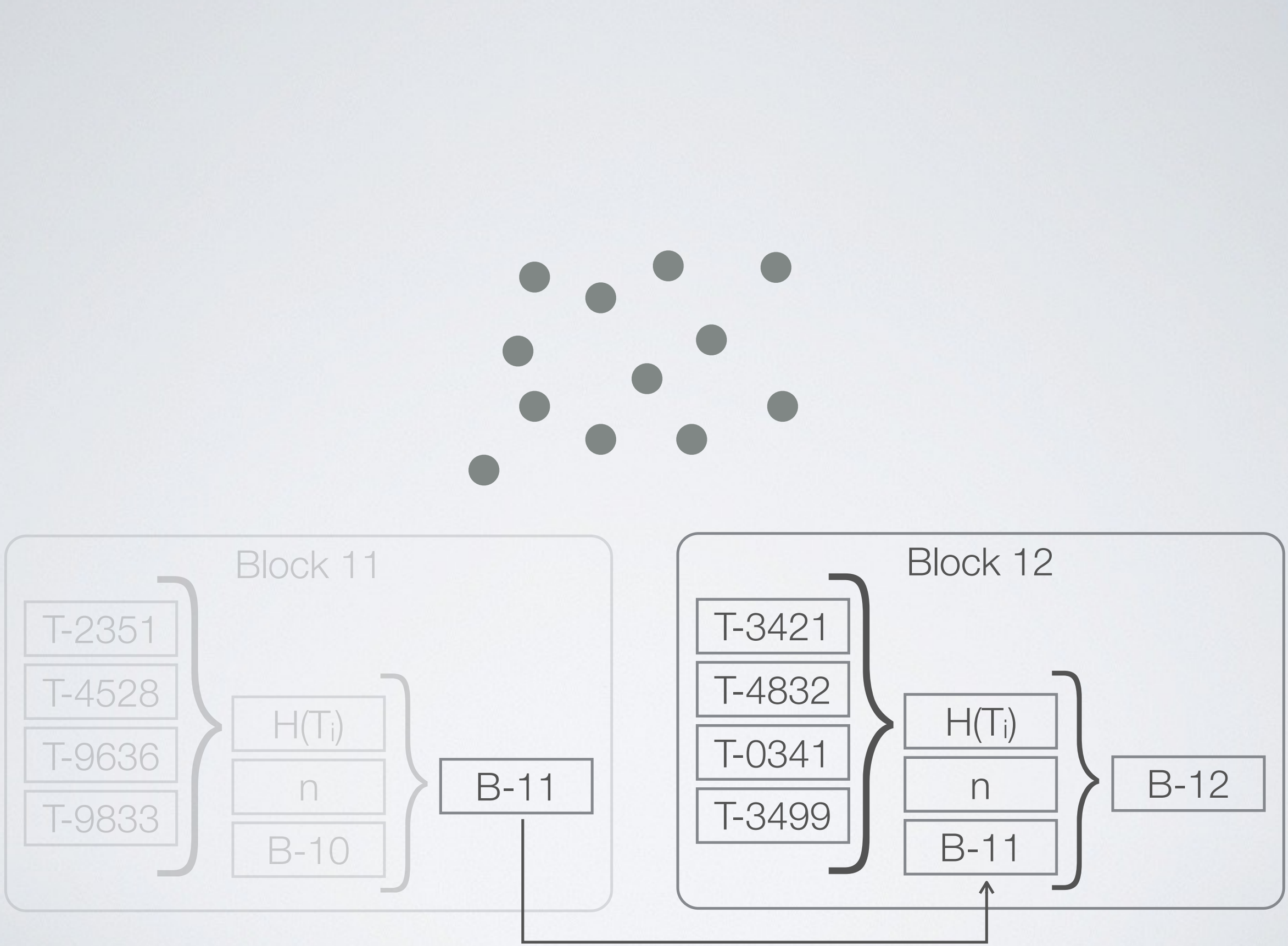

B10
B11
B12
B13
B14
B11




B10
B11
B12
B13
B14
B15
B11
B12



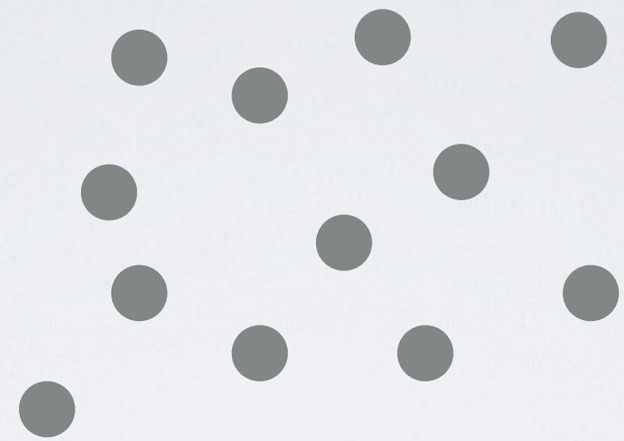

B10
B11
B12
B13
B14
B15
B11
B12

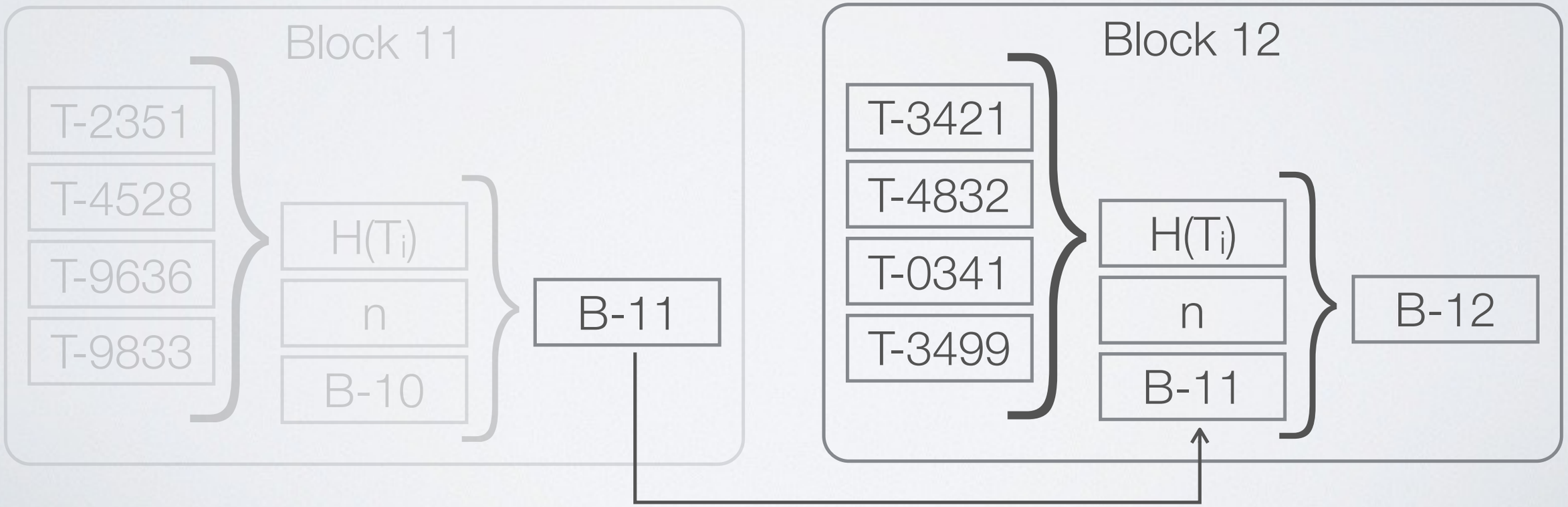

Block 11
T-2351
T-4528
T-9636
T-9833
H(Ti)
n
B-10
B-11
Block 12
T-3421
T-4832
T-0341
T-3499
H(Ti)
n
B-11
B-12

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

= 00000000000XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

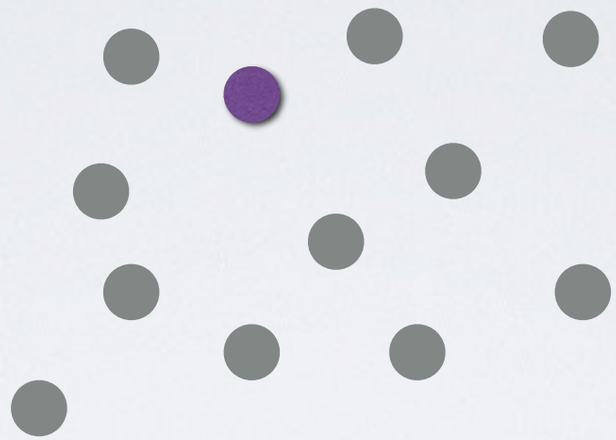
Work = (2^n)

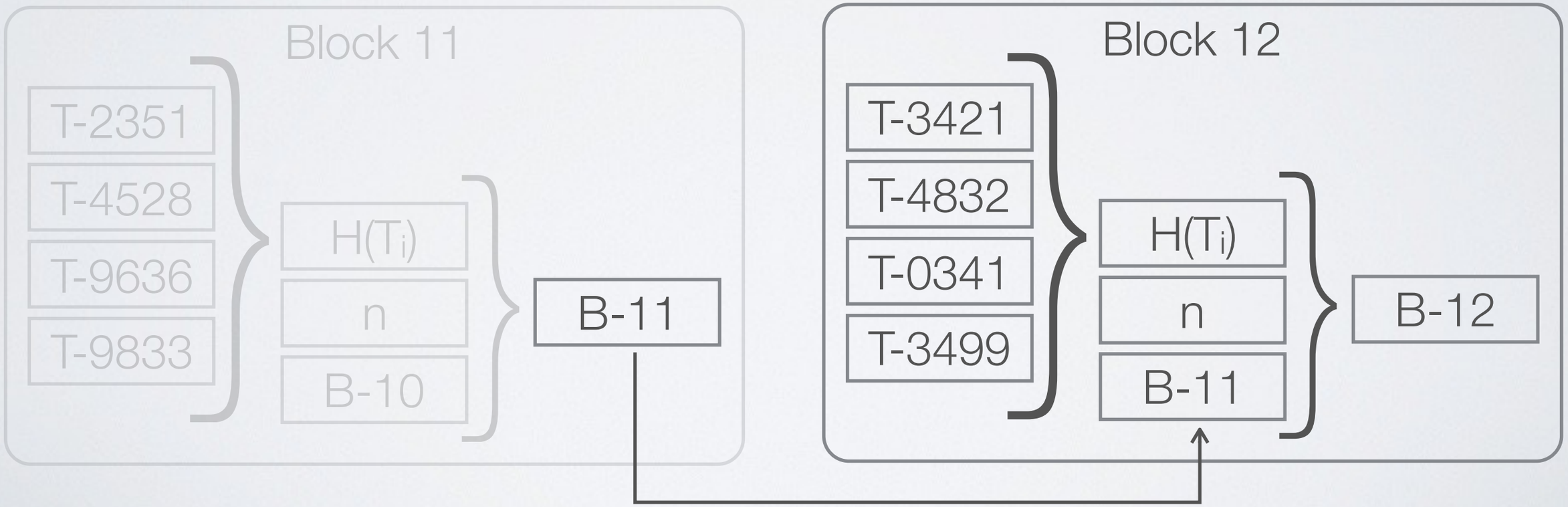




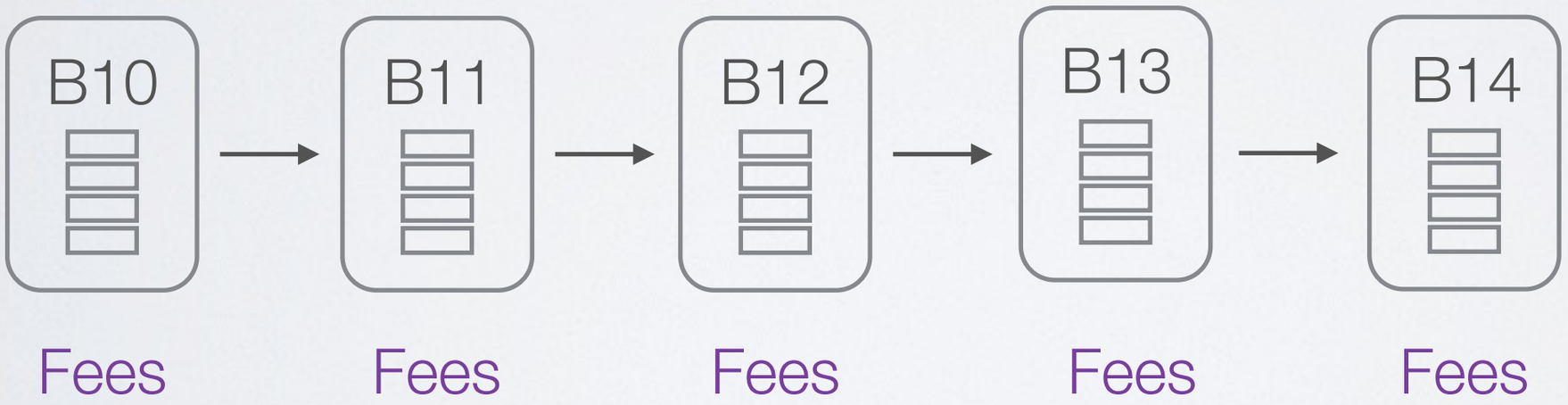
B-12 = H($H(T_i)$ || n || B-11)

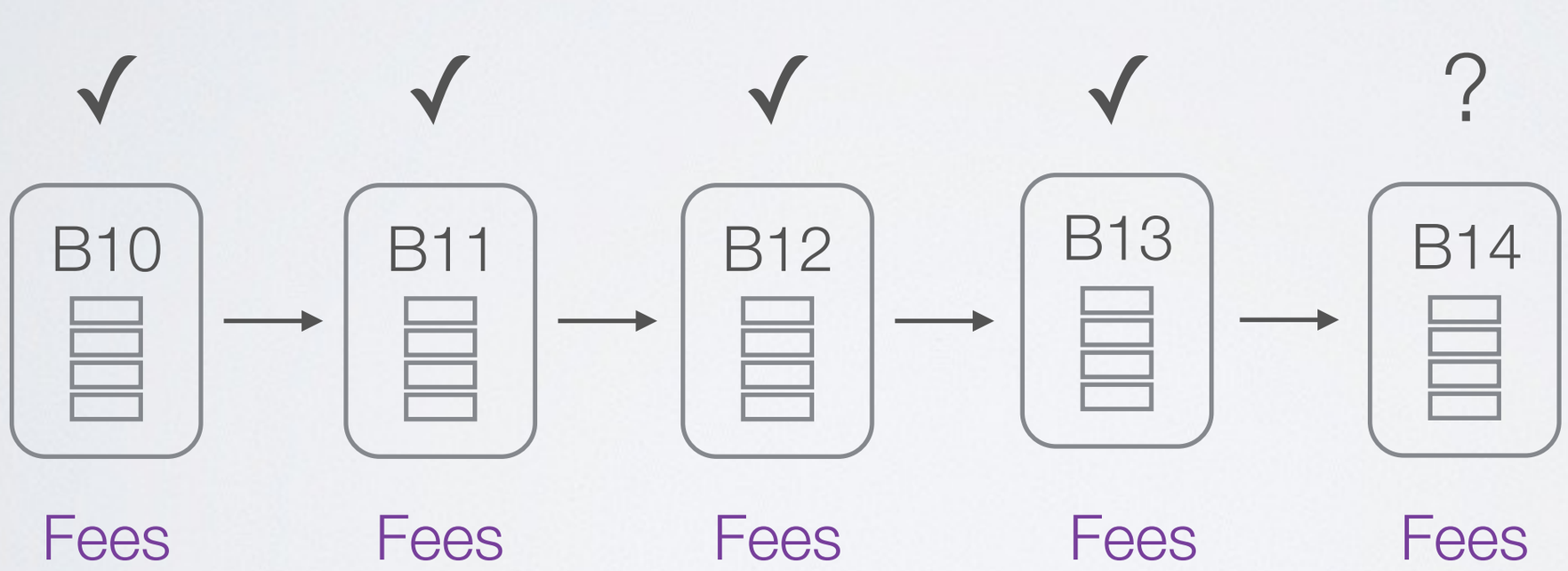
= 00000000000XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

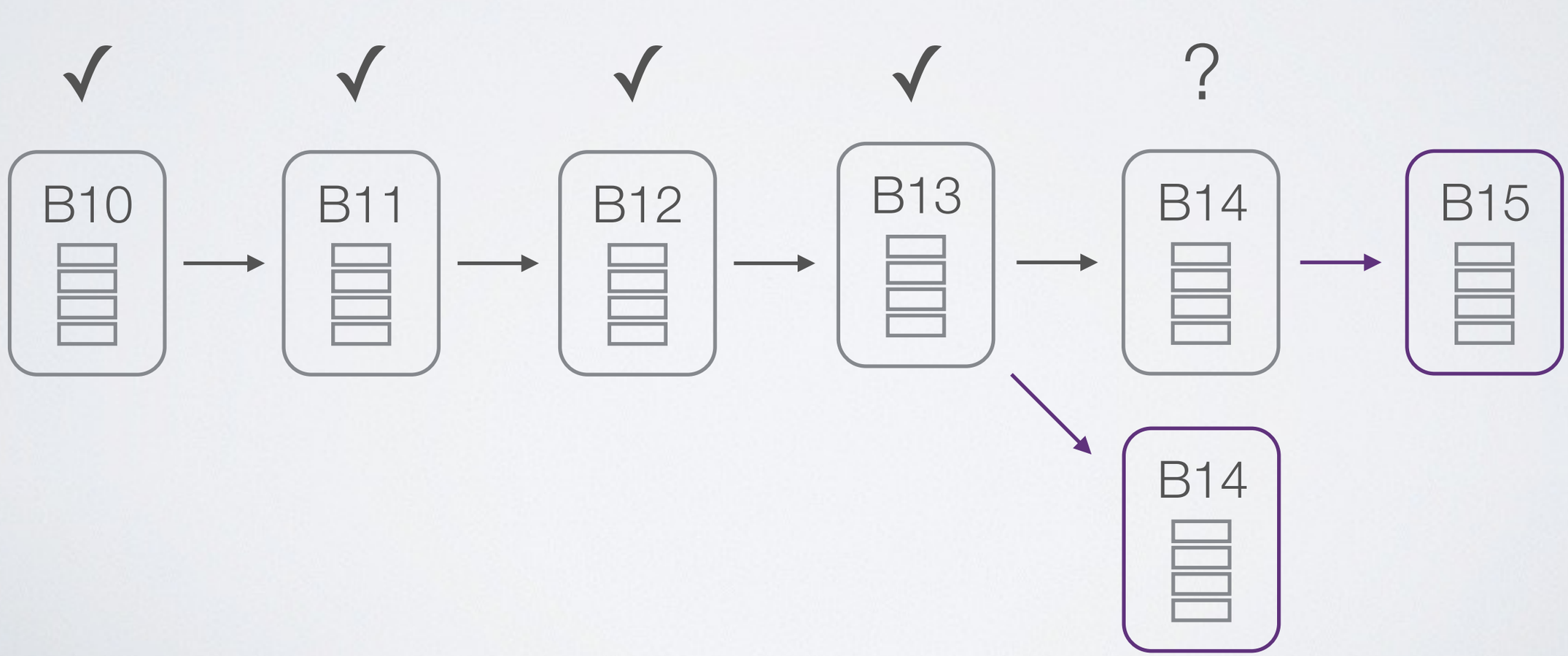


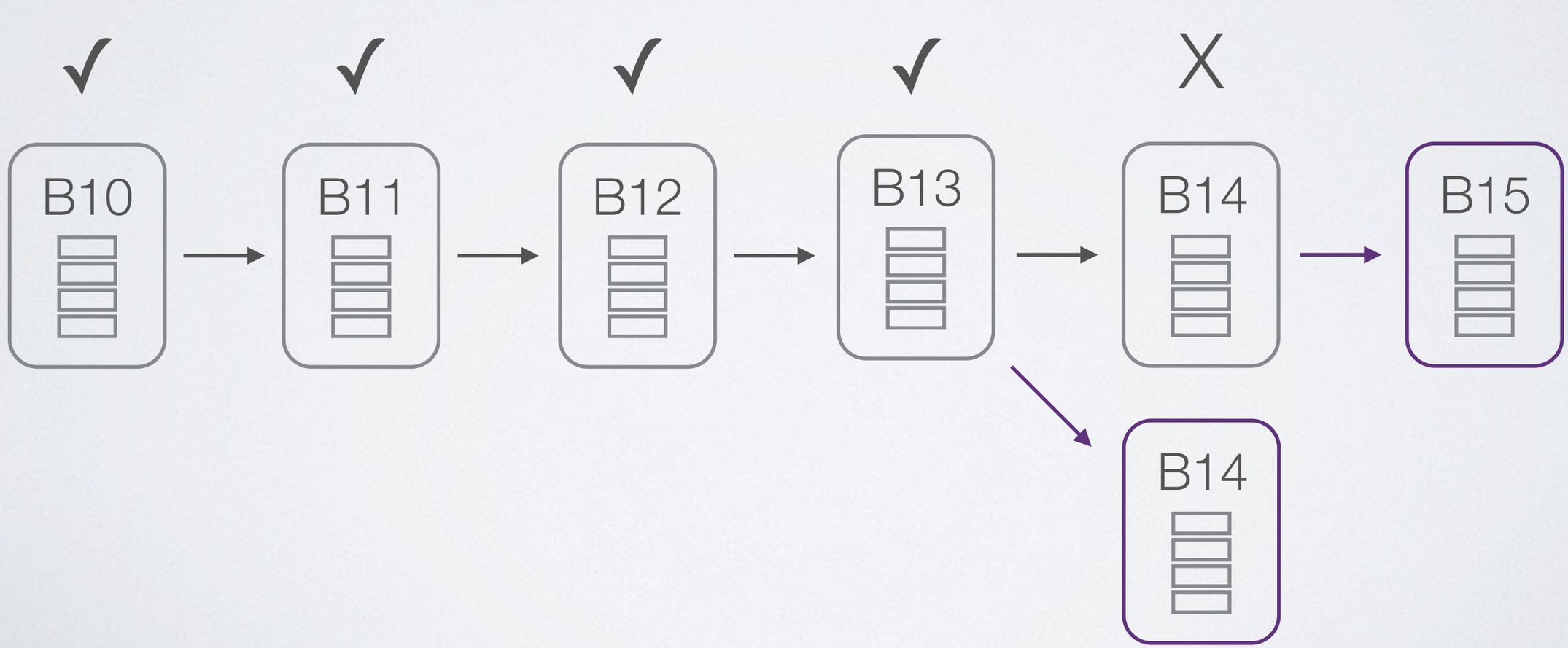


Incentive Compatibility

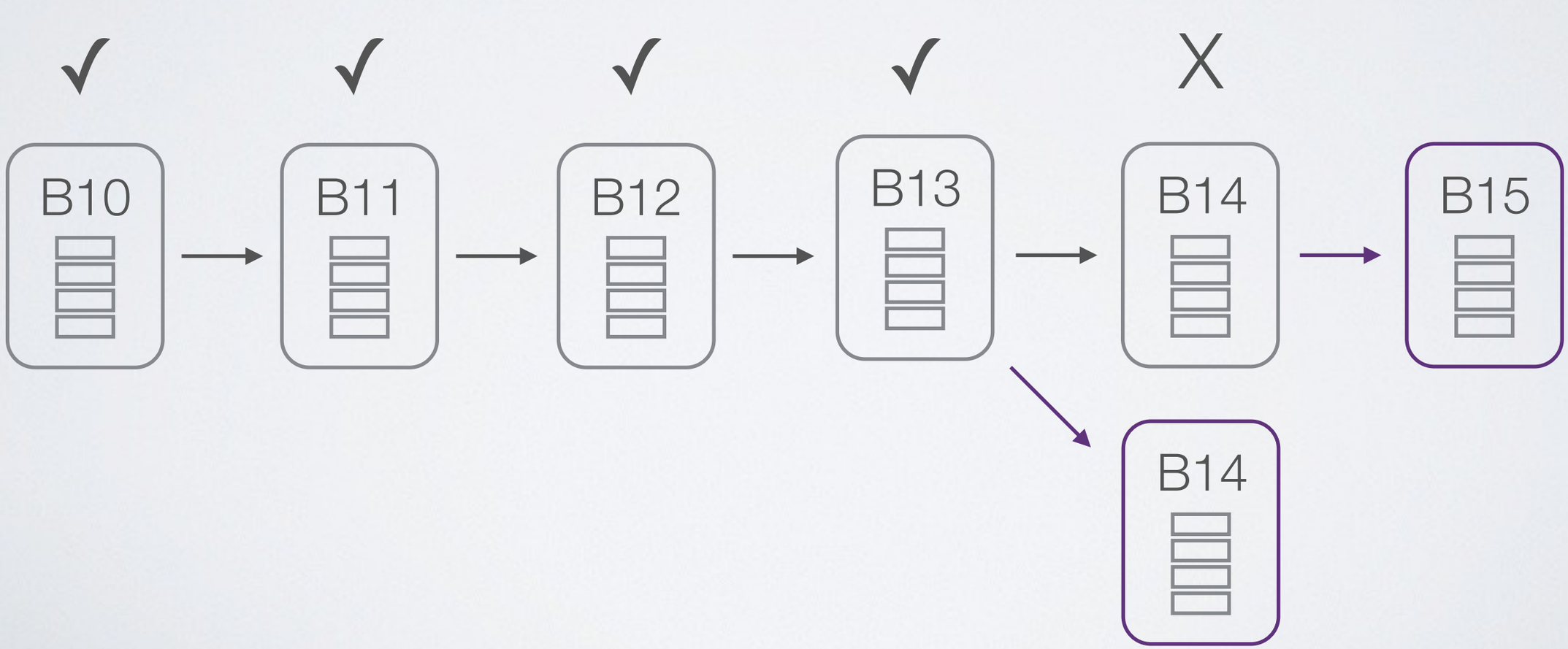



✓
✓
✓
✓
?
B10
B11
B12
B13
B14
Fees
Fees
Fees
Fees
Fees

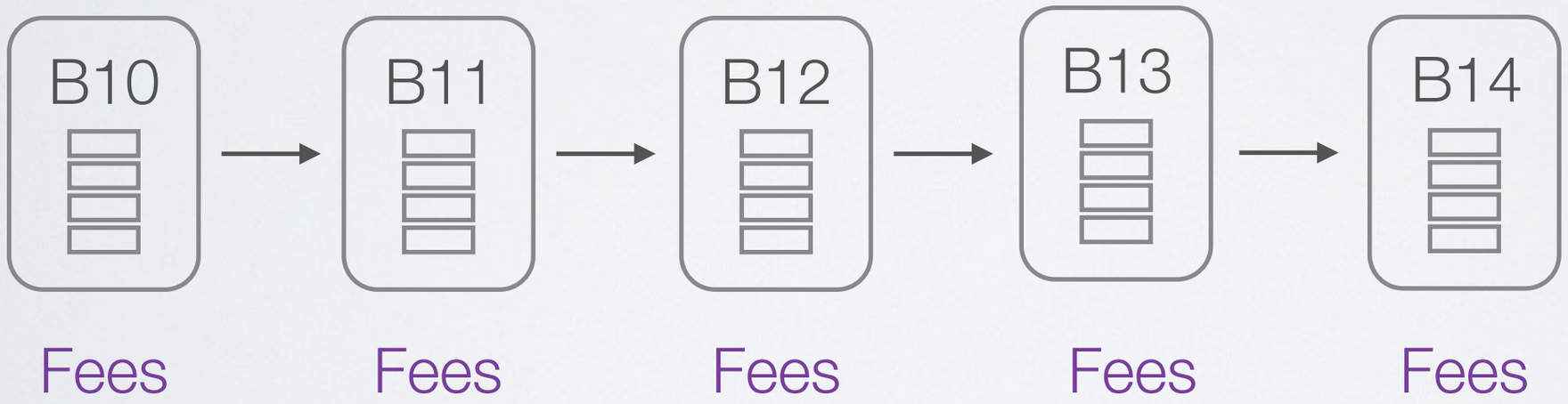

✓
✓
✓
✓
?
B10
B11
B12
B13
B14
B15
B14


✓
✓
✓
✓
X
B10
B11
B12
B13
B14
B15
B14

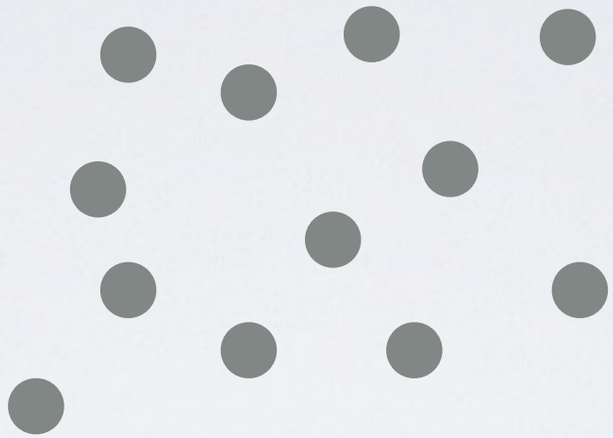
It pays to verify



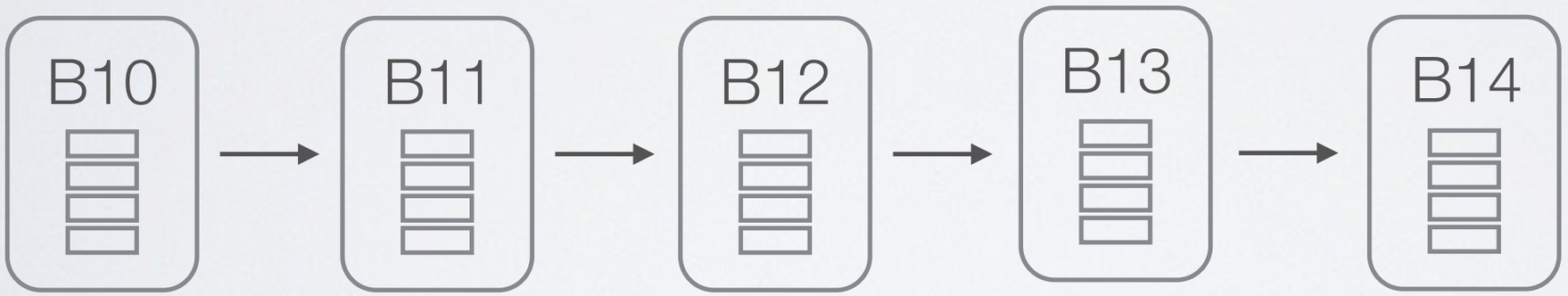
Initial Distribution (Minting)



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?

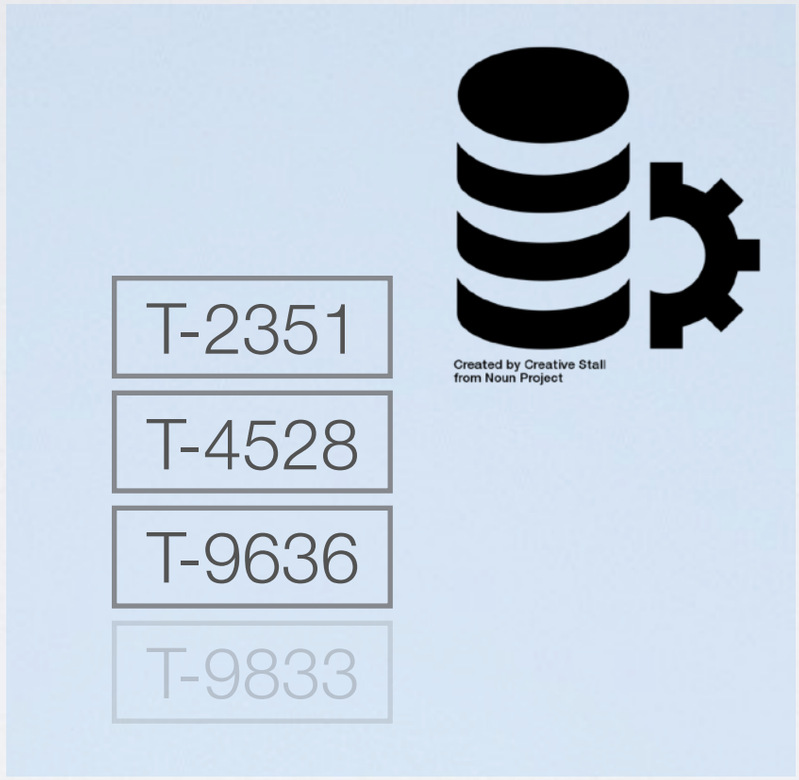
Consensus will form but will take ~6 blocks (~1 hour) for high assurance. Too long to wait in some cases.

T-2351

T-4528

T-9636

T-9833



Ledger:

* append-only record
* past records cannot be directly edited
* indirect edits through appending edits

Created by To Uyen
from Noun Project

Created by To Uyen
from Noun Project

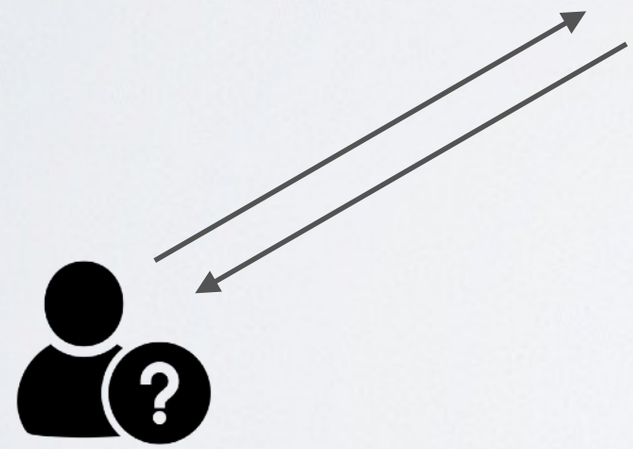
T-2351

T-4528

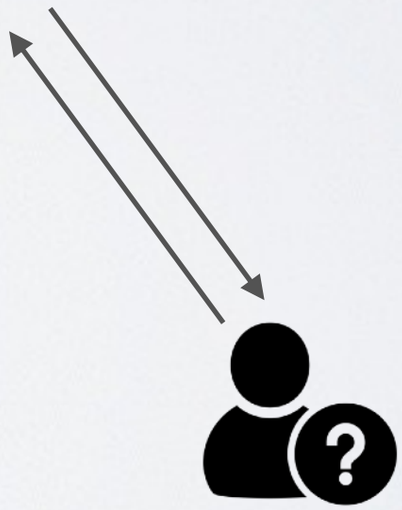
T-9636

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

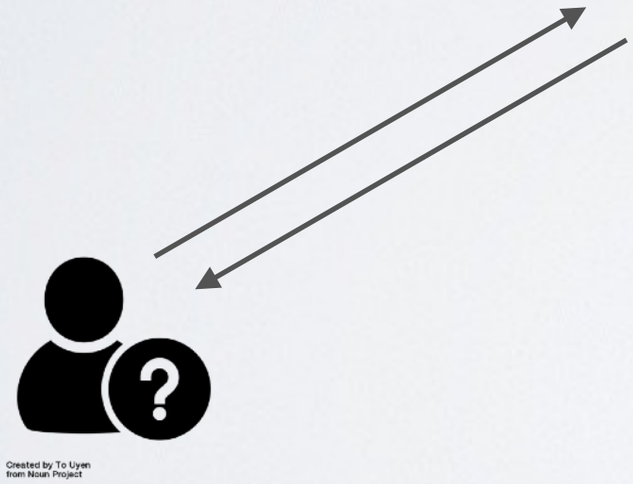
T-4528

T-9636

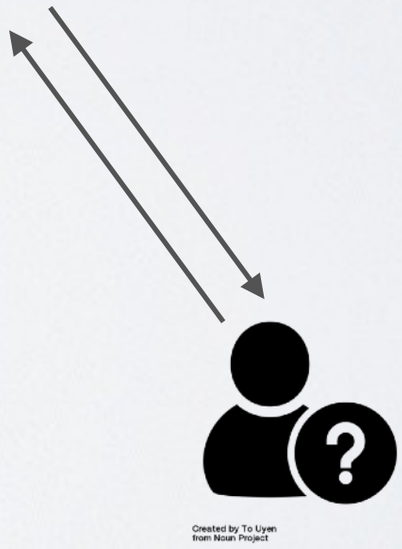
T-9833

Created by Creative Stall
from Noun Project

“Golden record”



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

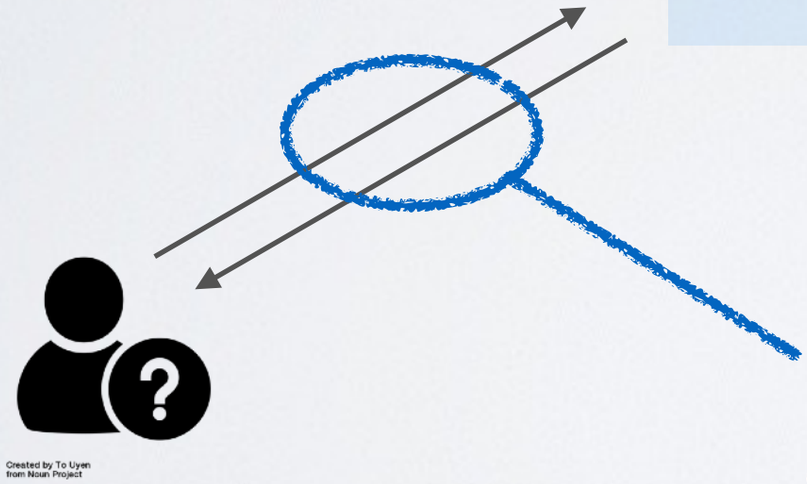
T-4528

T-9636

T-9833

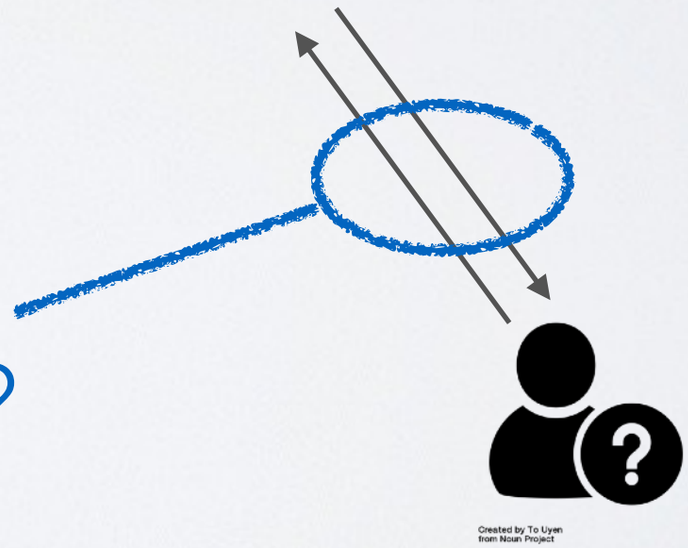
Created by Creative Stall
from Noun Project

“Golden record”



Created by To Uyen
from Noun Project

Same?



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

T-2351

T-4528

T-9636

T-9833

Disintermediation

T-2351

T-4528

T-9636

T-9833

T-2351

T-4528

T-9636

T-9833

T-2351

T-4528

T-9636

T-9833

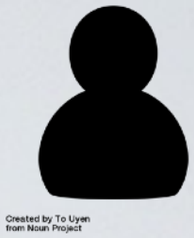
T-2351

T-4528

T-9636

T-9833

Disintermediation



T-2351

T-4528

T-9636

T-9833

T-2351

T-4528

T-9636

T-9833

T-2351

T-4528

T-9636

T-9833

Local Access

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

Consistency?

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

Created by To Uyen
from Noun Project

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

Local Access

Created by To Uyen
from Noun Project

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

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

Disintermediation

Consistency?

Consensus through voting

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

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

Local Access

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

2) Unit of computational effort:

Bitcoin’s blockchain

No trust, open network

Consistency?

- Consensus through voting
- What if you ignore the consensus?

Consistency?

Consensus through voting

What if you ignore the consensus?

1) Closed network:

   Reputation and retaliation

2) Open network:

   Incentives instead of reputation

Are closed network ledgers “blockchains”?

A question of semantics

Same blackbox behaviour, different assumptions

Sometimes called “permissioned”

* Read, write, manage nodes, mint coins, etc

Inserting trust to remove computational work & expand permission model

Can you have blockchain without Bitcoin?

Semantics aside, yes

Works smoothly if you incentivize verification

Properties of blockchains & distributed ledgers

The good and the bad

Consistency / Non-equivocation

Everyone has a consistent set of records
Simplifies reconciliation
Different auditors see the same thing

Verification

Records can be subjected to rules
Rules are enforced by the technology
‘Seeing is believing’

Verification…

…trades off with Confidentiality

Verifiable ledgers need to be lit
Confidentiality can be overlaid
If you can see it, only you can check it

…trades off with Efficiency

Every node verifies everything (even if N/A)
Propagation, verification, consensus take time
Can be offset with trust or collateral

Disintermediation

Remove central maintainers of the ledger
Automated settling and clearing
Reduce reconciliation and dispute resolution
Pass costs onto nodes (economics unclear)
Improve security and reliability

Cannot remove counter-party risk

- Reputation is hard without identity
- Post collateral

Time-stamping

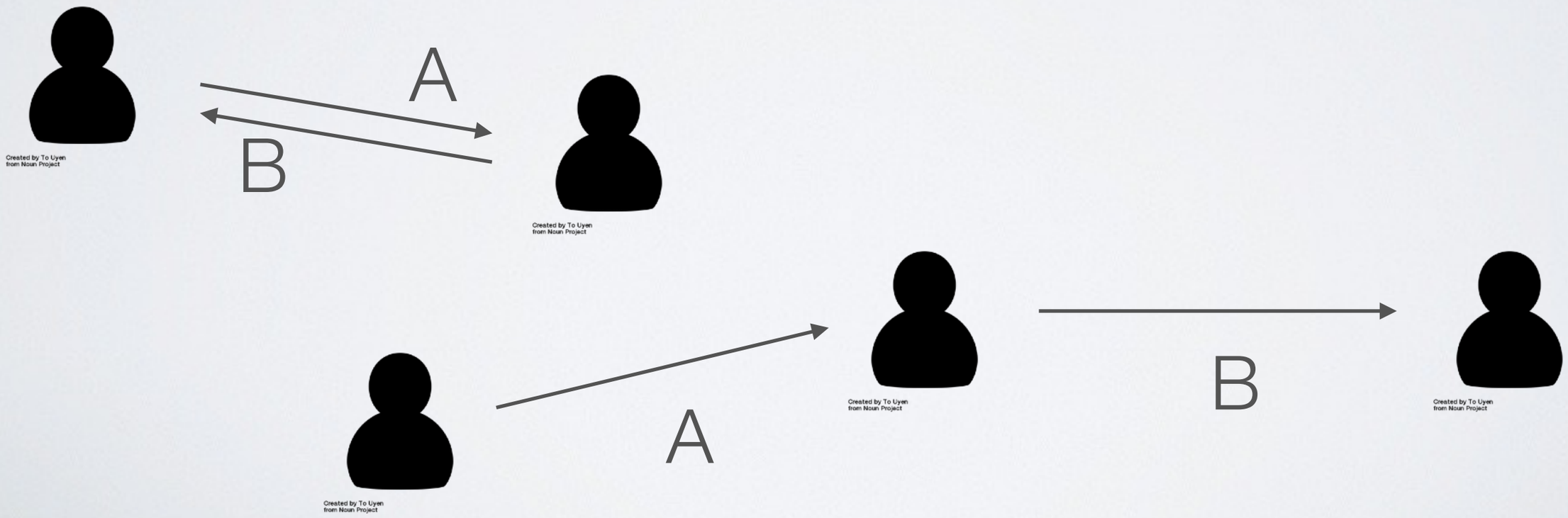
Chunky by design
Chunks are strongly ordered
Propagation delays means no single clock
Cannot do time-priority records

Redundancy

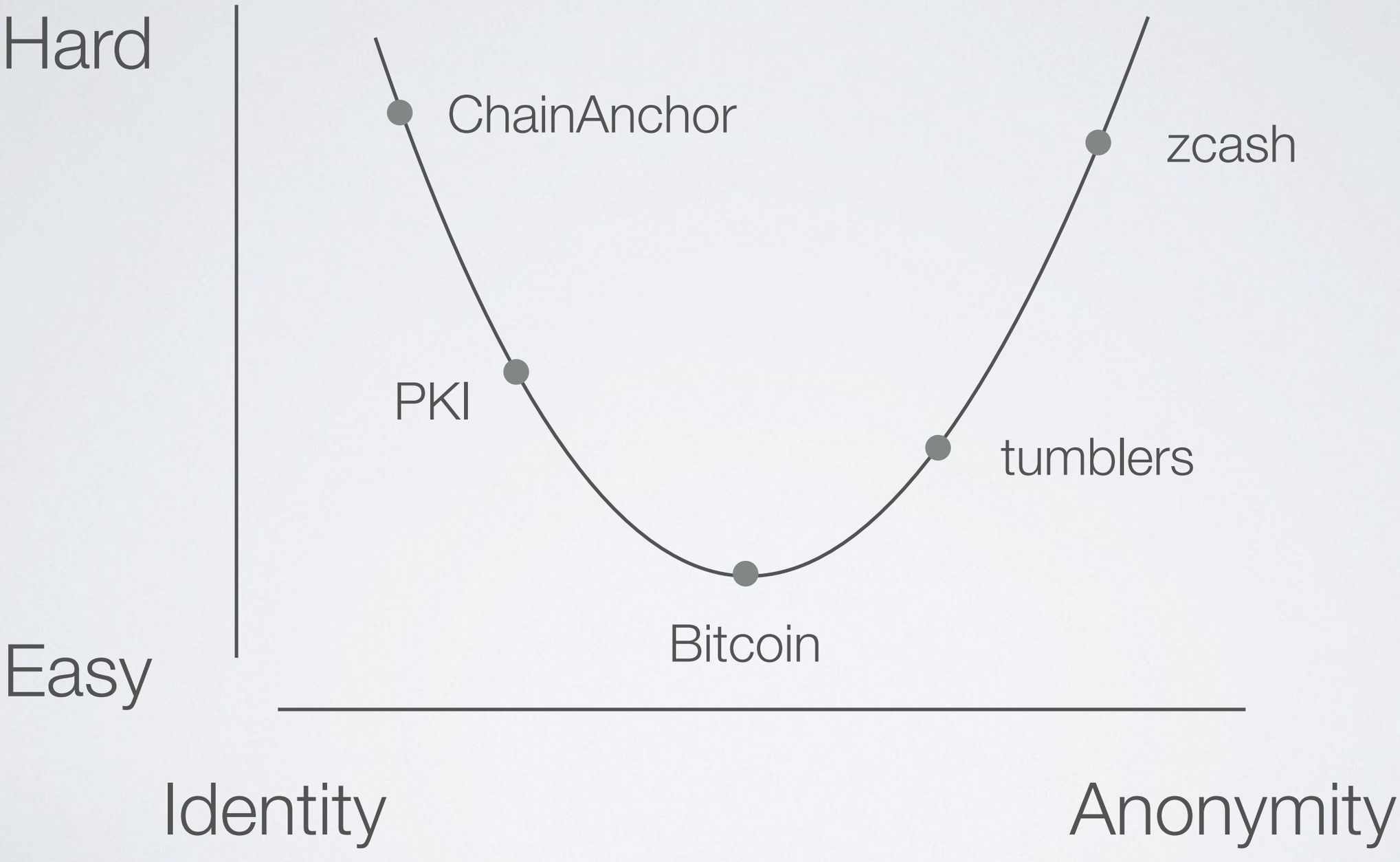
Lots of copies of the data

Complex Transactions

Atomicity: all/nothing transactions
Chain of payments (with transparency)
Netting (credit networks)
Transactions triggered by events



Anonymity


Hard
Easy
Identity
Anonymity
ChainAnchor
zcash
PKI
tumblers
Bitcoin

How to build your blockchain

& interact with other blockchains

Why?

1) Do what Bitcoin does only better
   - Faster validation
   - Reduce “wasteful” computations
   - Change monetary policy

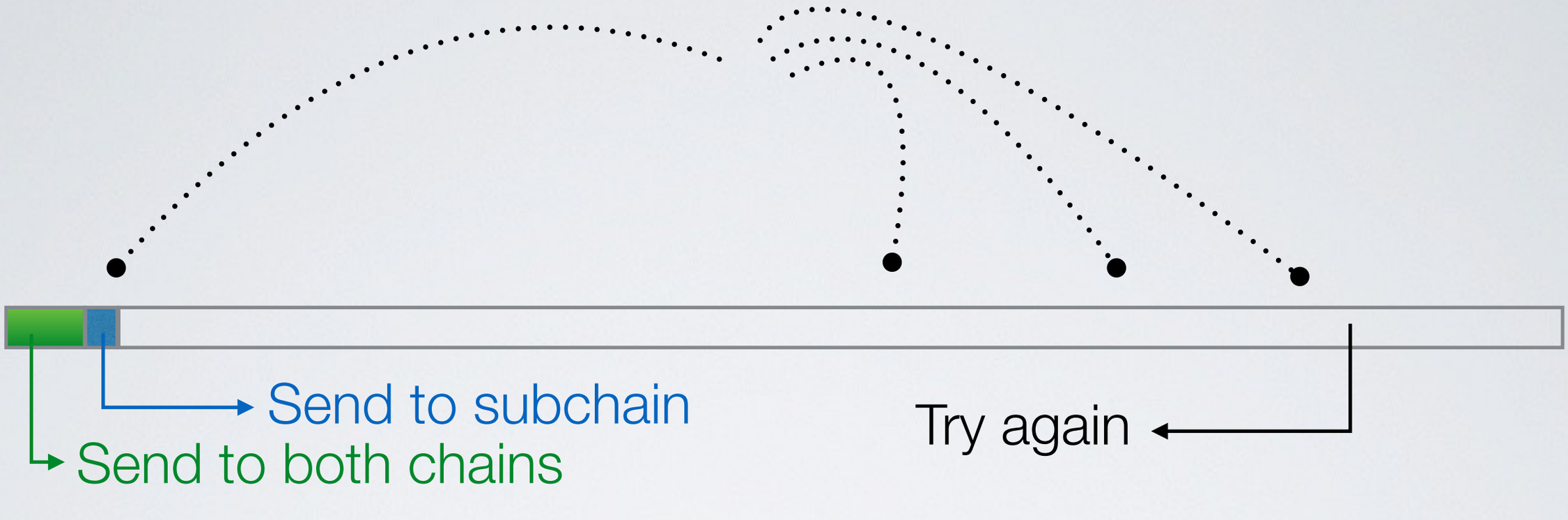
2) Do something Bitcoin doesn’t do
   - With or without a currency

Fork Bitcoin

1) New Genesis Block
   - "Altcoins," private ledgers, credit nets, etc
   - No commonality with Bitcoin necessary
   - Compete with Bitcoin's computational power

2) Build from initial distribution
   - Pre-mine, fork Bitcoin mid-chain, registry

Merge Mining



- Create a subchain to a chain (e.g., Bitcoin)
- Miners embed the sub's latest block into a new main-chain block and solve it
- Requires same PoW (but diff difficulty is fine)
- Bitcoin mining pools support this today

Overlay

- Small amounts of bitcoin -> unforgeable token
- A trusted entity issues tokens
- Tokens subject to same rules as bitcoin
- Tokens could be redeemable for a material asset (currency, bond, equity, etc)
- Tokens could mirror real-world transfers (land deed, artwork, luxury good, etc)
- Example: Bitt provides Barbadian dollars
- Threat: issuer could over-issue

Moving Between Chains (Two Parties)

Alice and Bob swap assets of different chains

- Alice gets a time-locked refund transaction
- Alice deposits to joint account
- Alice sends to Bob using a hash-locked transaction
    - Bob does the same and sends to Alice using the same lock
- If Alice redeems, Bob can as well

Moving Between Chains (Single Party)

1) Unilateral Transfer

- Burn the asset on the main-chain
- Mint pegged amount on sub-chain
- Subchain must watch the main-chain
- Alternatives to burning:
  Donate to charity
  Time-lock some amount for some time

2) Bilateral Transfer

- Main-chain most monitor all sub-chains
- Send to trusted depository instead of burning

Use cases

real & imagined

Layer 3: Market

Layer 2: Transaction Rules

Layer 1: Assets

Example: Bitcoin

Layer 3: Market	Lightning Network, Coloured Coins
Layer 2: Transaction Rules	Transfer
Layer 1: Assets	Currency

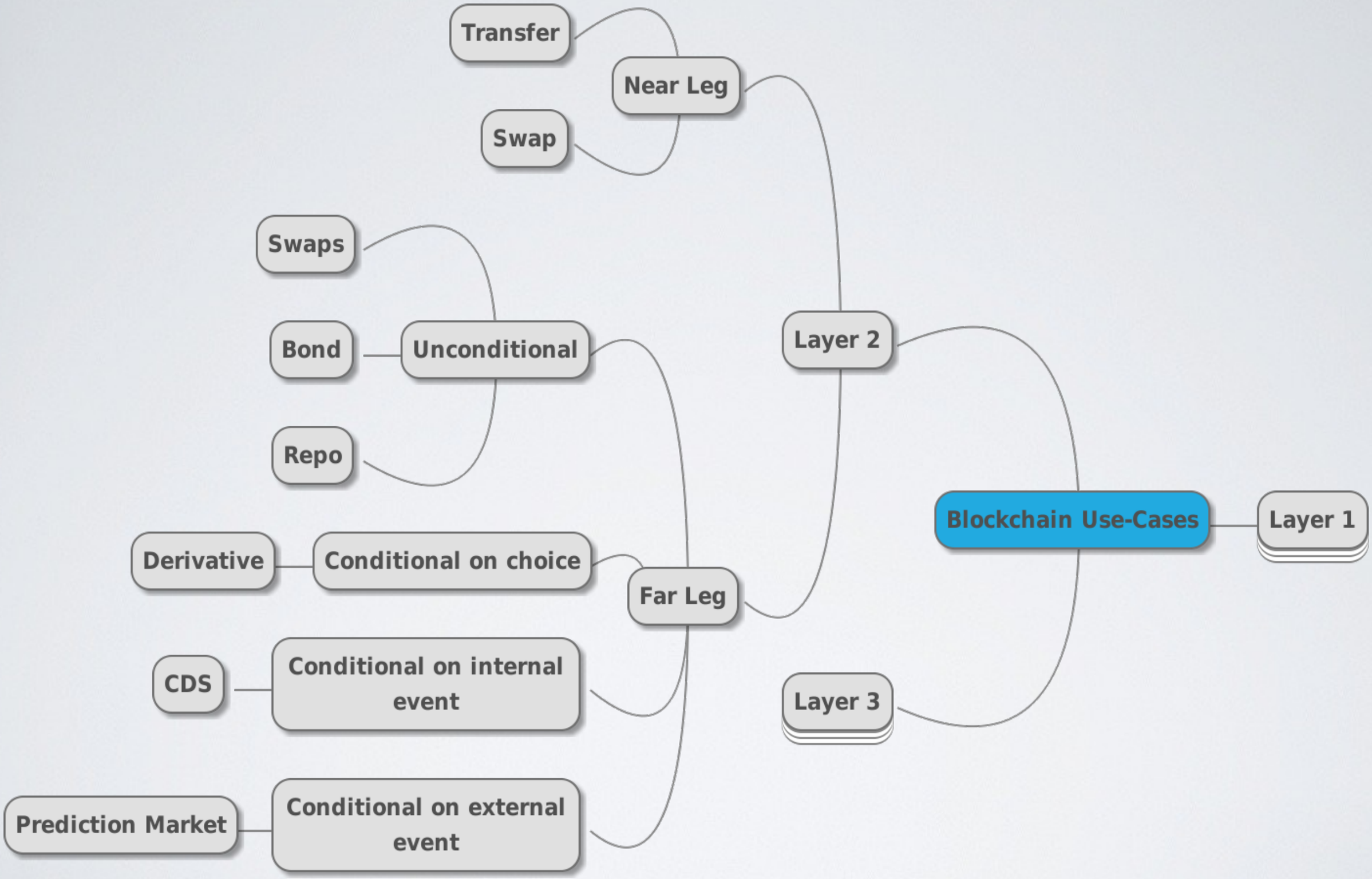
Example: Prediction Market

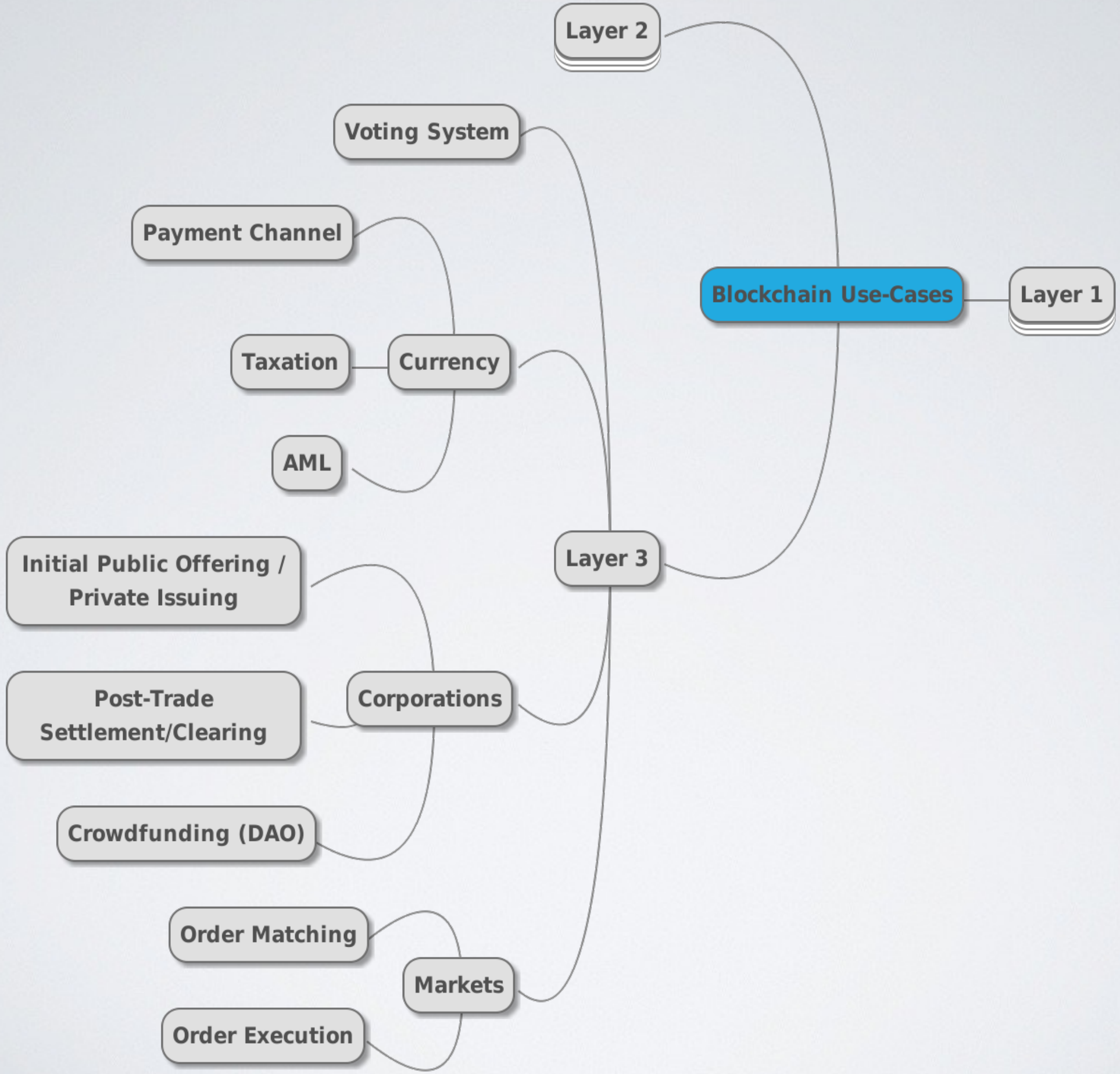
Layer 3: Market	Order Book
Layer 2: Transaction Rules	Transfer, Convert, Open/Close Event
Layer 1: Assets	Currency, Shares

Example: Repurchase Agreements

Layer 3: Market	Margin, Pooling, DBV
Layer 2: Transaction Rules	Transfer, Swap
Layer 1: Assets	Currency, Collateral

- Blockchain Use-Cases
  - Layer 3
  - Layer 2
  - Layer 1
    - Ownership
      - Digital / Dematerialized asset
        - Financial Instrument
        - Loyalty Program
        - Carbon Credits
      - Claim to material asset
        - Tokenized Financial Instruments
      - Certificate of material asset
        - Deeds
        - Artwork
        - Luxury Goods
    - Record Keeping
      - PKI
      - DNS
      - KYC Information
      - Time-stamping
      - Energy Consumption


Transfer
Near Leg
Swap
Swaps
Bond
Unconditional
Repo
Layer 2
Blockchain Use-Cases
Layer 1
Derivative
Conditional on choice
Far Leg
CDS
Conditional on internal event
Layer 3
Prediction Market
Conditional on external event


Blockchain Use-Cases
Layer 1
Layer 2
Layer 3
Voting System
Payment Channel
Currency
Taxation
AML
Corporations
Initial Public Offering / Private Issuing
Post-Trade Settlement/Clearing
Crowdfunding (DAO)
Markets
Order Matching
Order Execution

Questions?

@PulpSpy