The Blockchain & Cryptocurrency Landscape

Jeremy Clark

The Blockchain & Cryptocurrency Landscape

Jeremy Clark

Jeremy Clark

- Associate Professor at the Concordia Institute for Information Systems Engineering (CIISE) in Montreal
- NSERC / Raymond Chabot Grant Thornton / Catallaxy Industry Research Chair in Blockchain Technologies
- PhD from the University of Waterloo (2009)
- Team of ten graduate students
- Numerous academic papers on Bitcoin/Blockchain
- Contributed to courses (Concordia, Princeton, MIT) & textbook on Bitcoin/blockchain
- Testified to Senate and House committees on Bitcoin/blockchain

MADIBA
security
research
group

UNIVERSITÉ
Concordia
UNIVERSITY

GINA CODY
SCHOOL OF ENGINEERING
AND COMPUTER SCIENCE

Funding & Partners:

NSERC
CRSNG

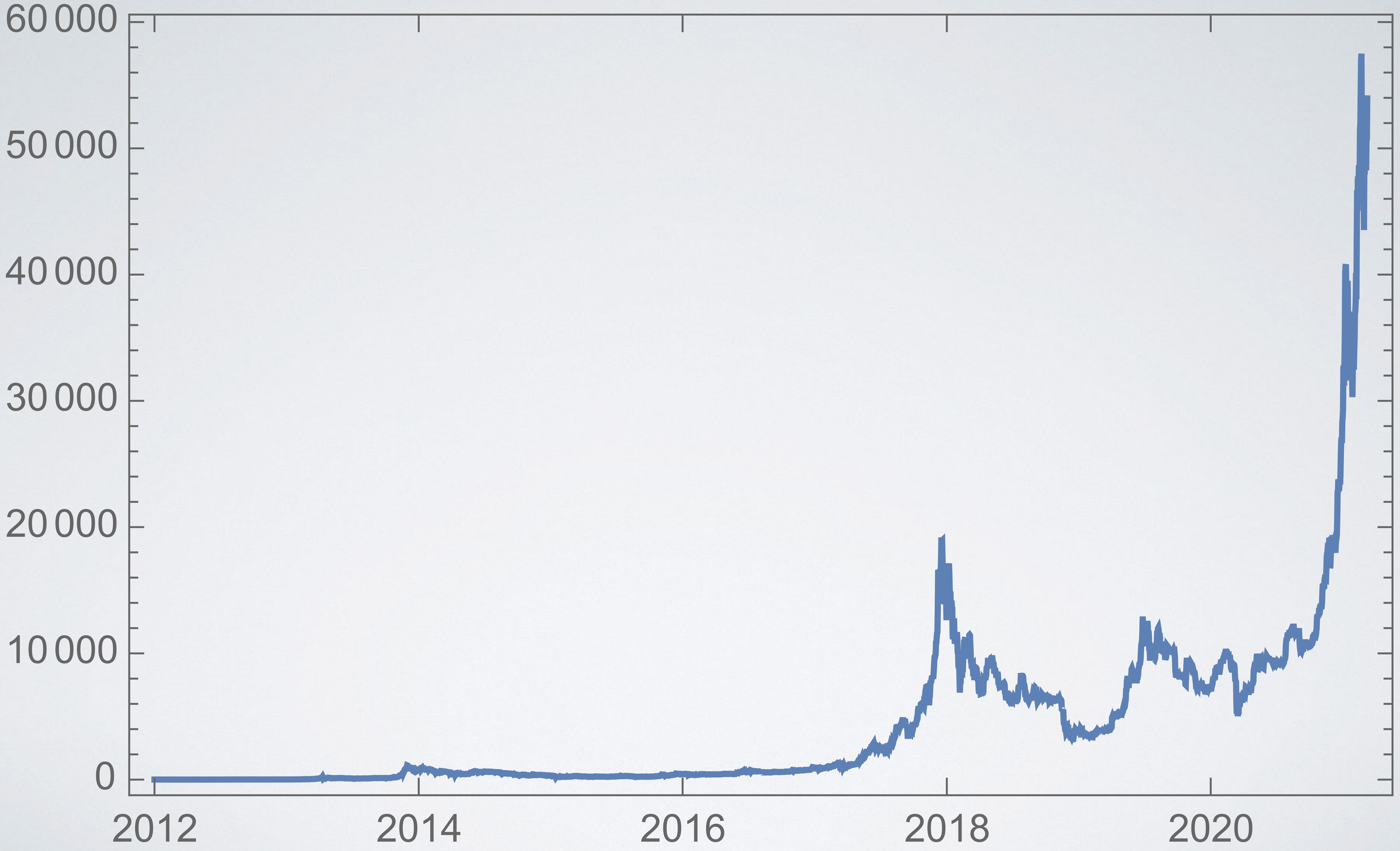
Raymond Chabot
Grant Thornton

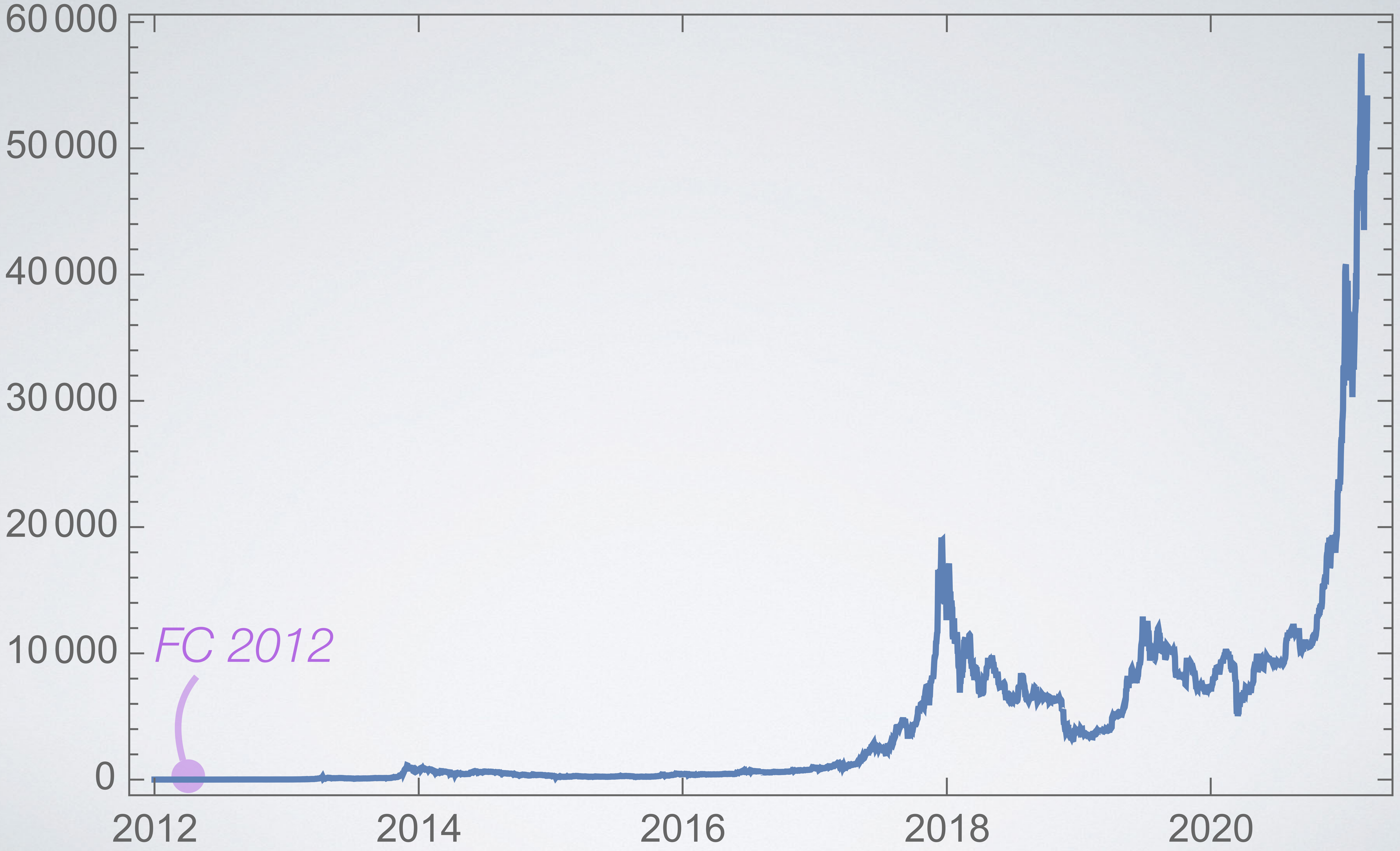
catallaxy

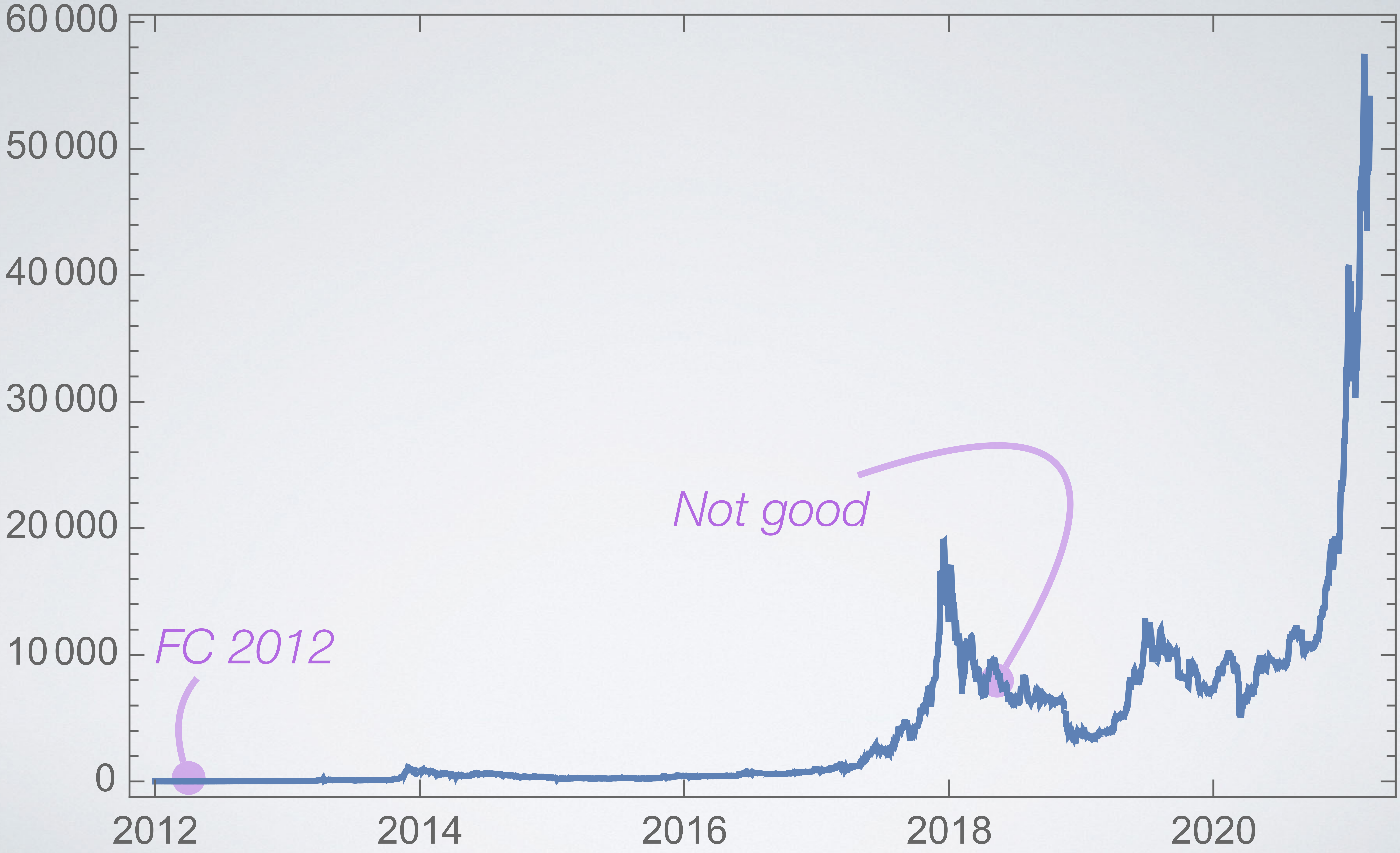
AUTORITÉ
DES MARCHÉS
FINANCIERS

Fonds de recherche
Nature et
technologies
Québec

Office of the
Privacy Commissioner
of Canada

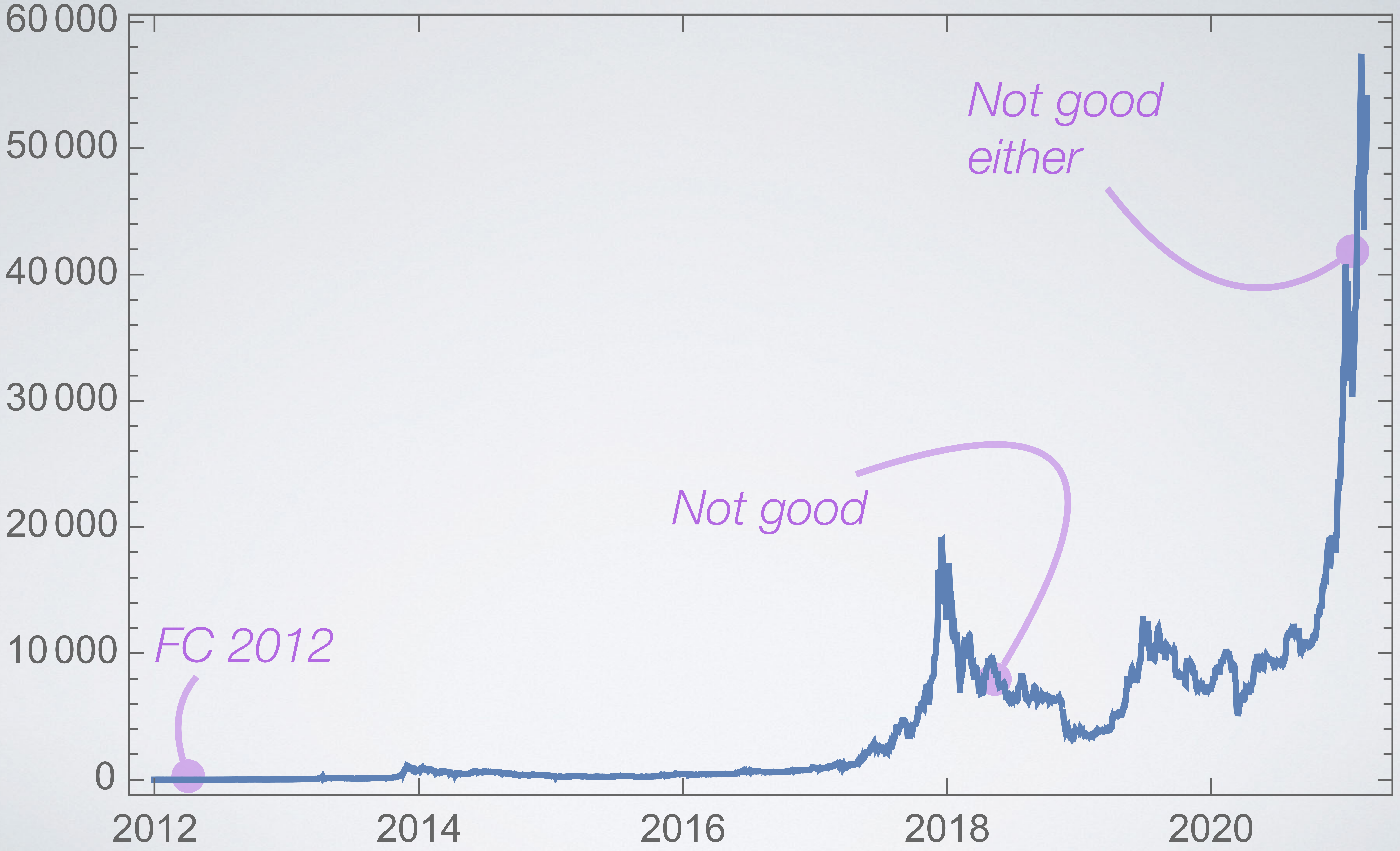

60 000
50 000
40 000
30 000
20 000
10 000
0
2012
2014
2016
2018
2020

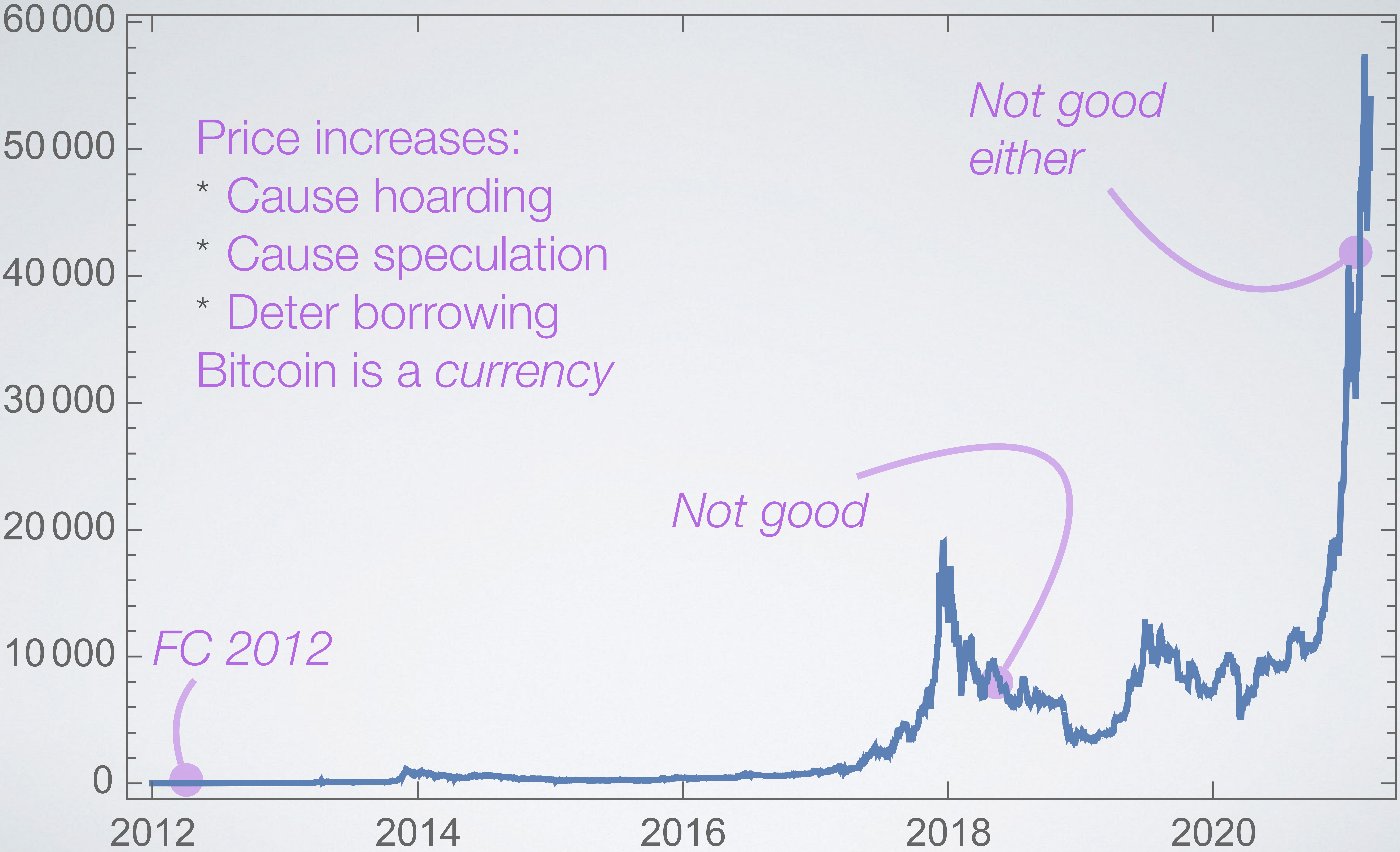

60 000
50 000
40 000
30 000
20 000
10 000
0
2012
2014
2016
2018
2020
FC 2012



FC 2012

Not good


60 000
50 000
40 000
30 000
20 000
10 000
0
2012
2014
2016
2018
2020
Not good
either
Not good
FC 2012



Price increases:

* Cause hoarding

* Cause speculation

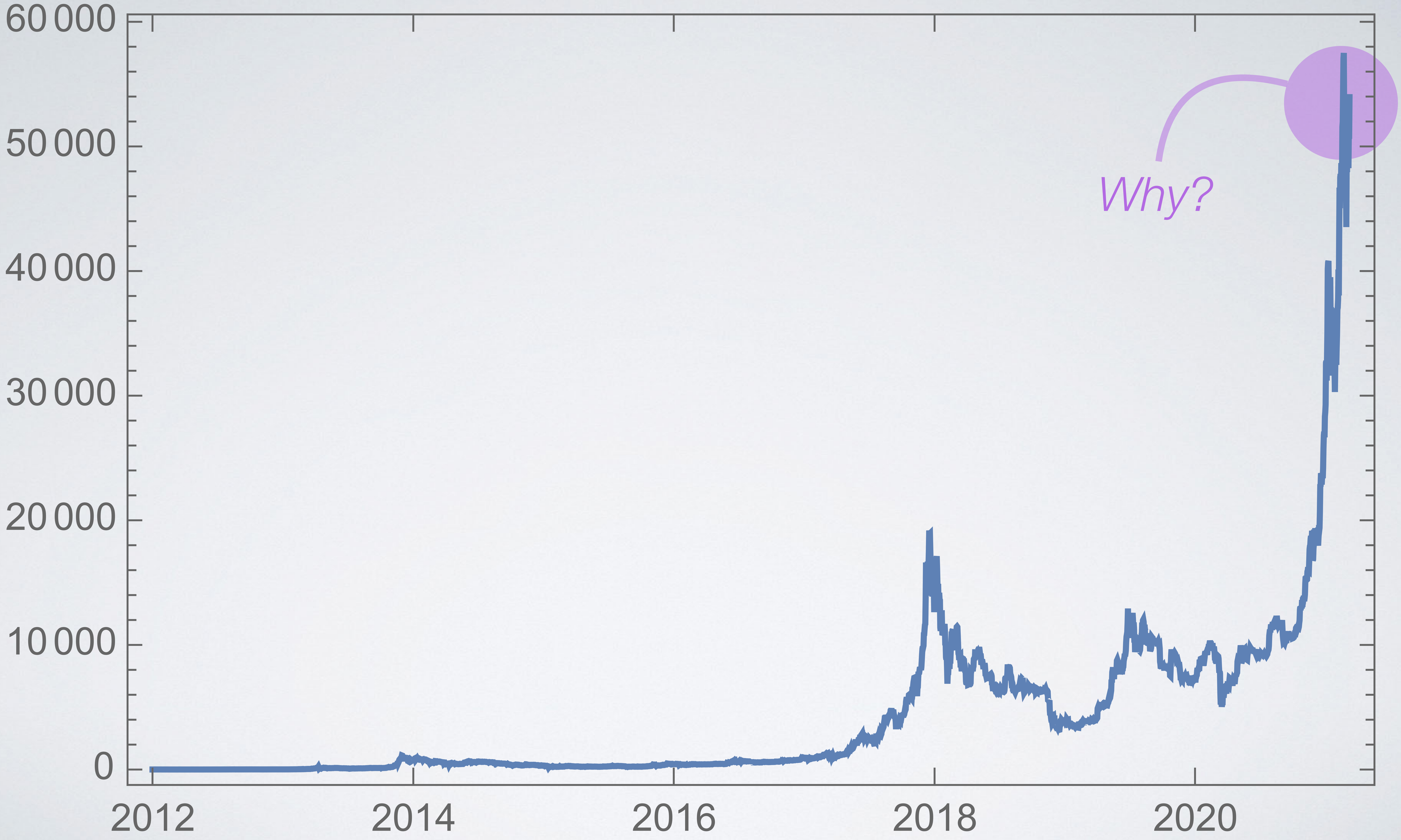
* Deter borrowing

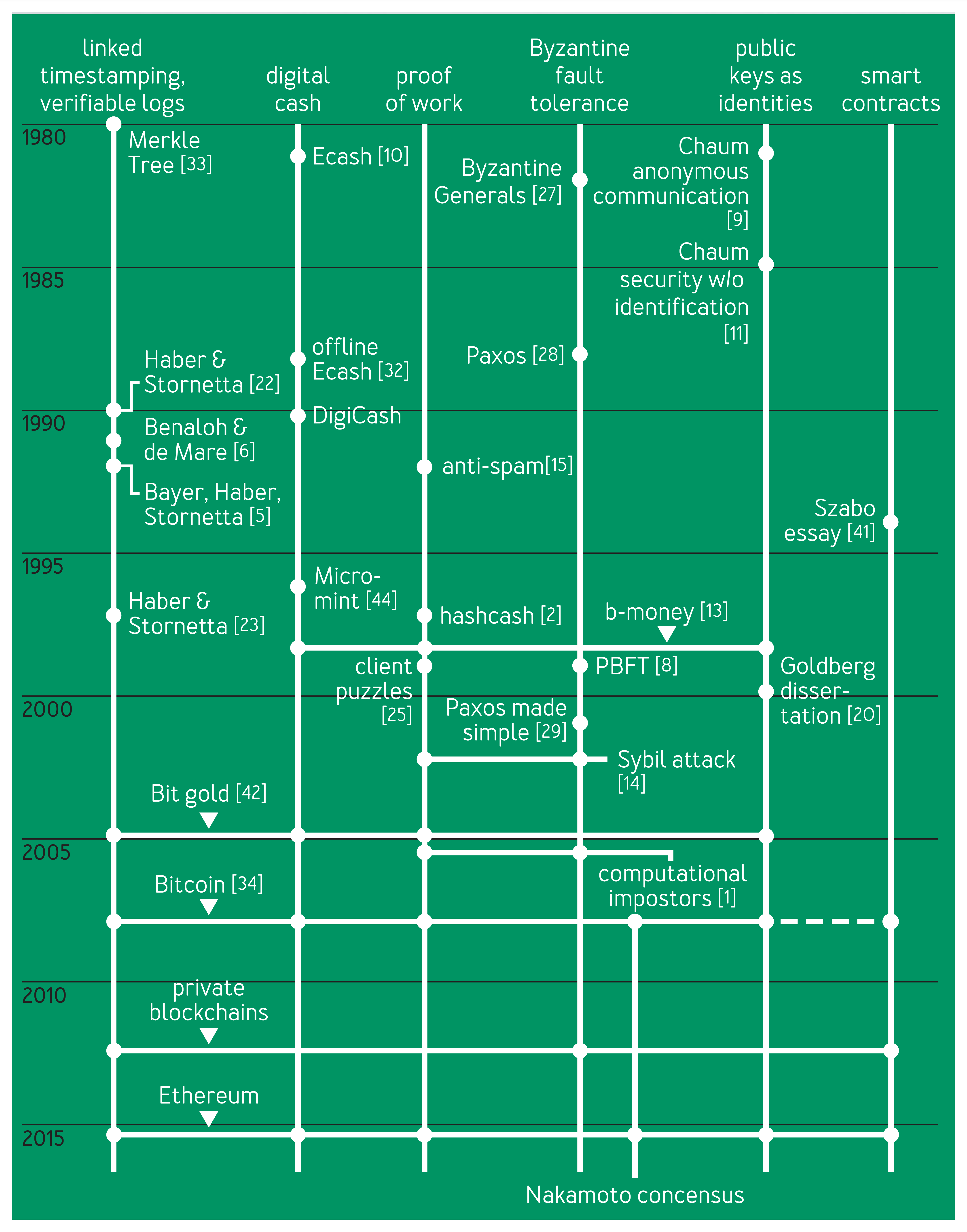
Bitcoin is a *currency*

FC 2012

Not good

Not good either


60 000
50 000
40 000
30 000
20 000
10 000
0
2012
2014
2016
2018
2020
Why?



linked timestamping, verifiable logs

digital cash

proof of work

Byzantine fault tolerance

public keys as identities

smart contracts

1980

Merkle Tree [33]

Ecash [10]

Byzantine Generals [27]

Chaum anonymous communication [9]

Chaum security w/o identification [11]

1985

Haber & Stornetta [22]

offline Ecash [32]

Paxos [28]

1990

DigiCash

Benaloh & de Mare [6]

Bayer, Haber, Stornetta [5]

anti-spam[15]

Szabo essay [41]

1995

Micro-mint [44]

Haber & Stornetta [23]

hashcash [2]

b-money [13]

client puzzles [25]

PBFT [8]

Goldberg disser-tation [20]

2000

Paxos made simple [29]

Sybil attack [14]

Bit gold [42]

2005

computational impostors [1]

Bitcoin [34]

2010

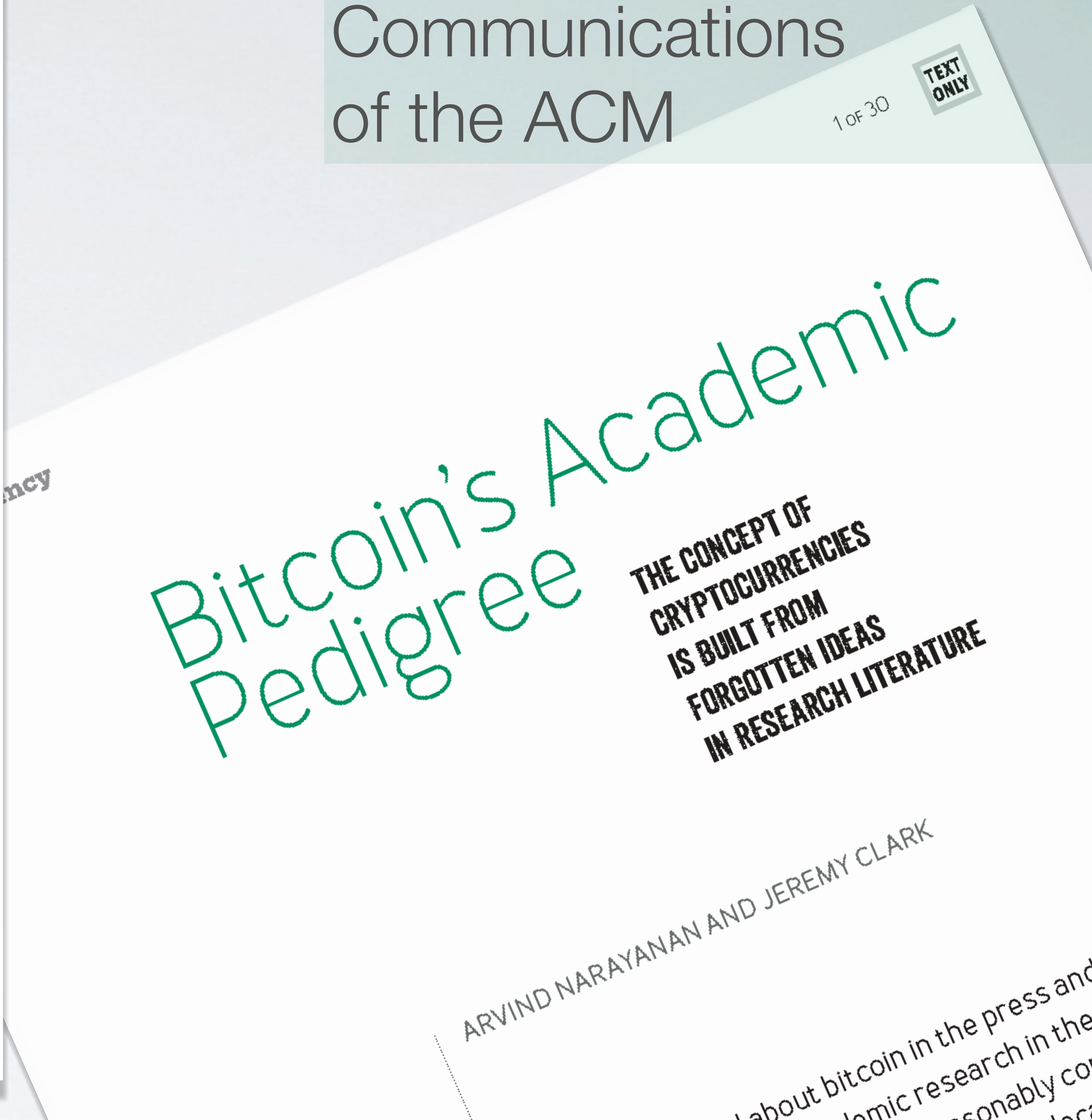
private blockchains

Ethereum

2015

Nakamoto concensus

Communications of the ACM



1 of 30

TEXT ONLY

ncy

Bitcoin's Academic Pedigree

THE CONCEPT OF CRYPTOCURRENCIES IS BUILT FROM FORGOTTEN IDEAS IN RESEARCH LITERATURE

ARVIND NARAYANAN AND JEREMY CLARK

about bitcoin in the press and

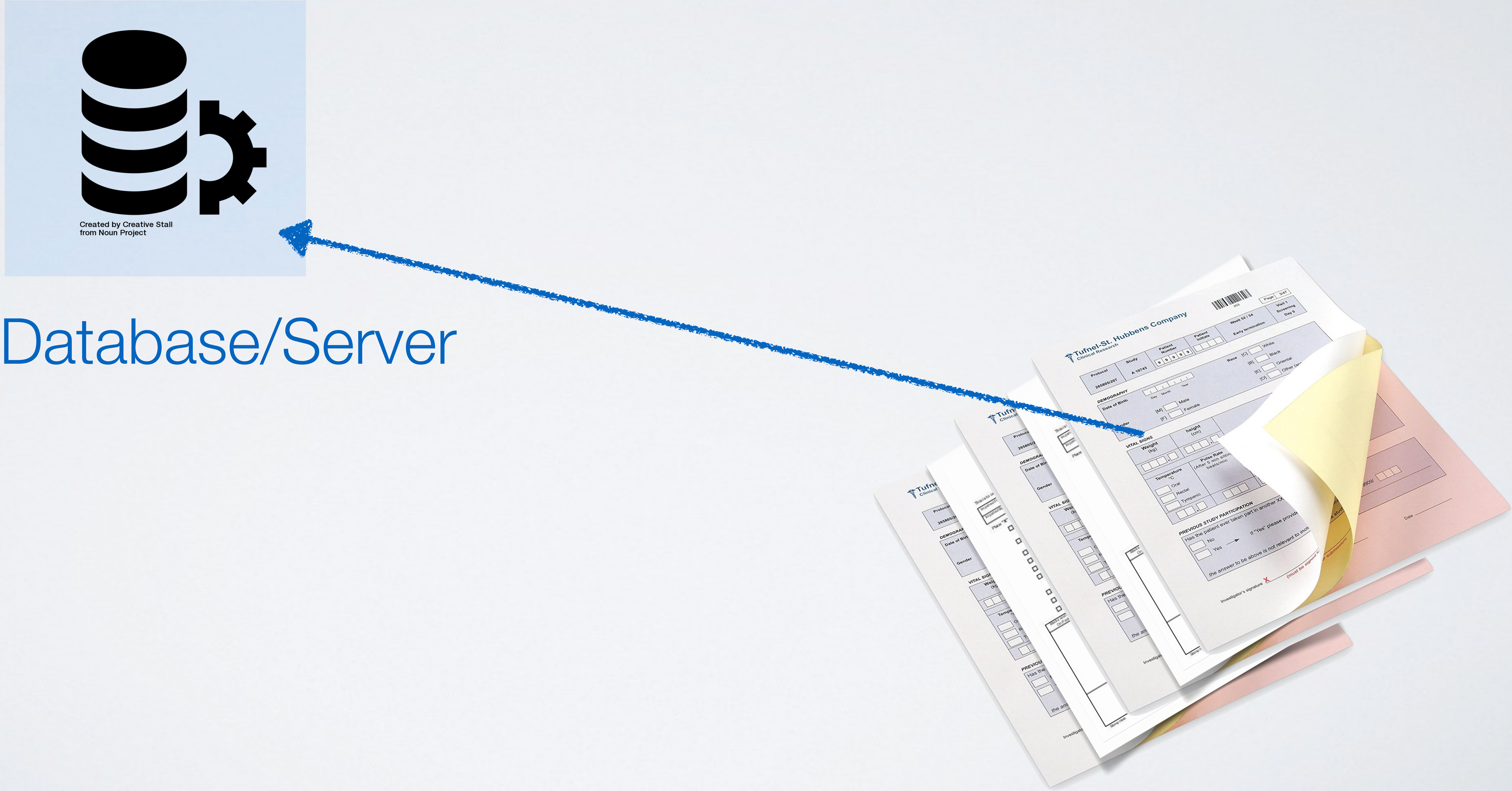
mic research in the

sonably co

Digital Revolution

Blockchain

Digital Revolution



Database/Server

Tufnel-St. Hubbens Company
Clinical Research

253

Page 3/47

Protocol	Study	Patient Number	Patient Initials	Week 52 / 54	Visit 1
265805/207	A 10743	9 9 9 9 9		Early termination	Screening Day 0

DEMOGRAPHY

Date of Birth Day Month Year

Gender [M] □ Male [F] □ Female

Race [C] □ White [B] □ Black [E] □ Oriental [O] □ Other (sp

VITAL SIGNS

Weight (kg) □□□.□

height (cm) □□□.□

Temperature °C □ Oral □ Rectal □ Tympanic □□.□

Pulse Rate (After 5 min sitting) beats/min □□□

PREVIOUS STUDY PARTICIPATION

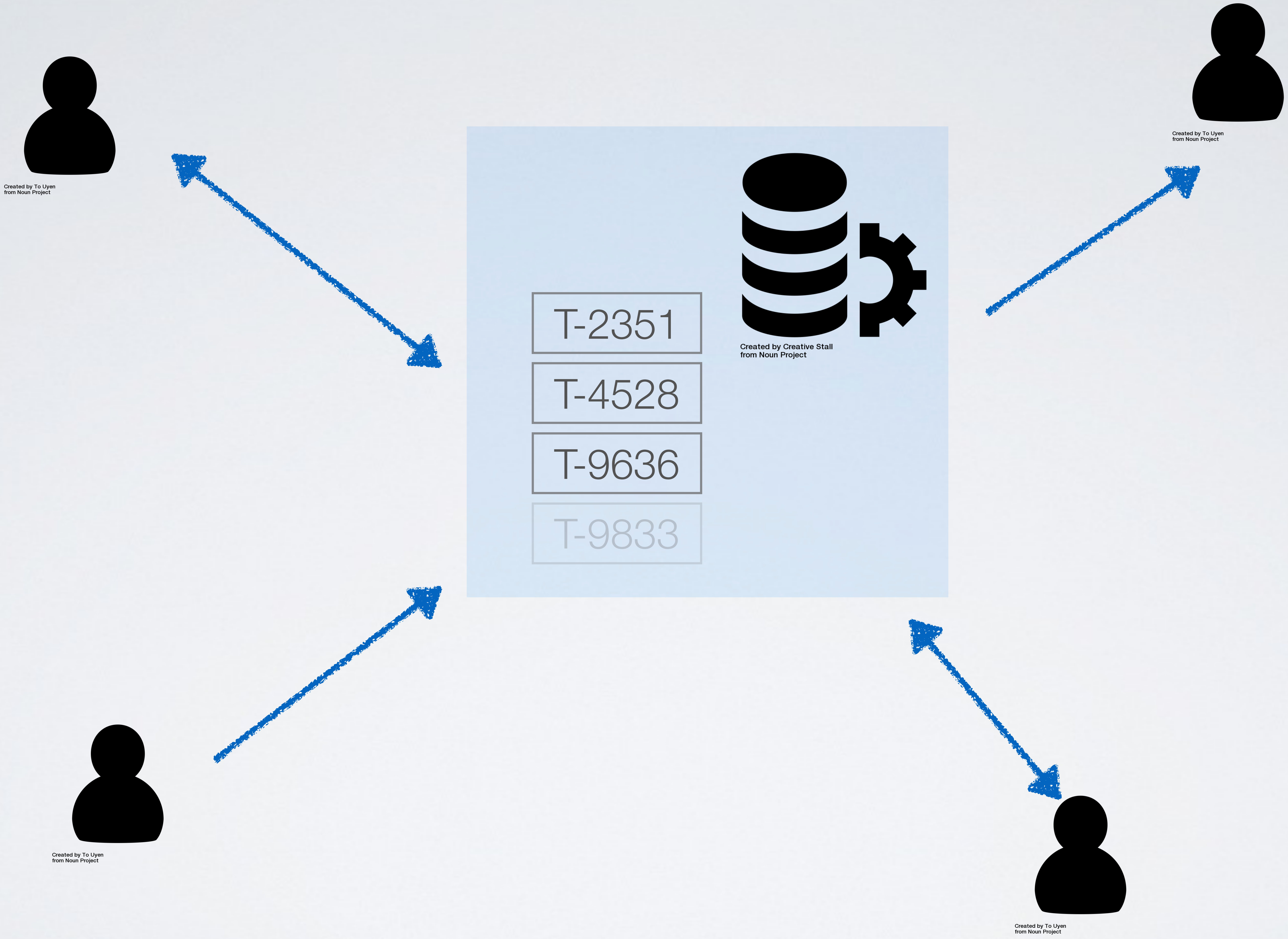
Has the patient ever taken part in another XX

□ No

□ Yes → If "Yes" please provide

the answer to be above is not relevant to incl

Investigator's signature X (must be signed fo



T-2351

T-4528

T-9636

T-9833

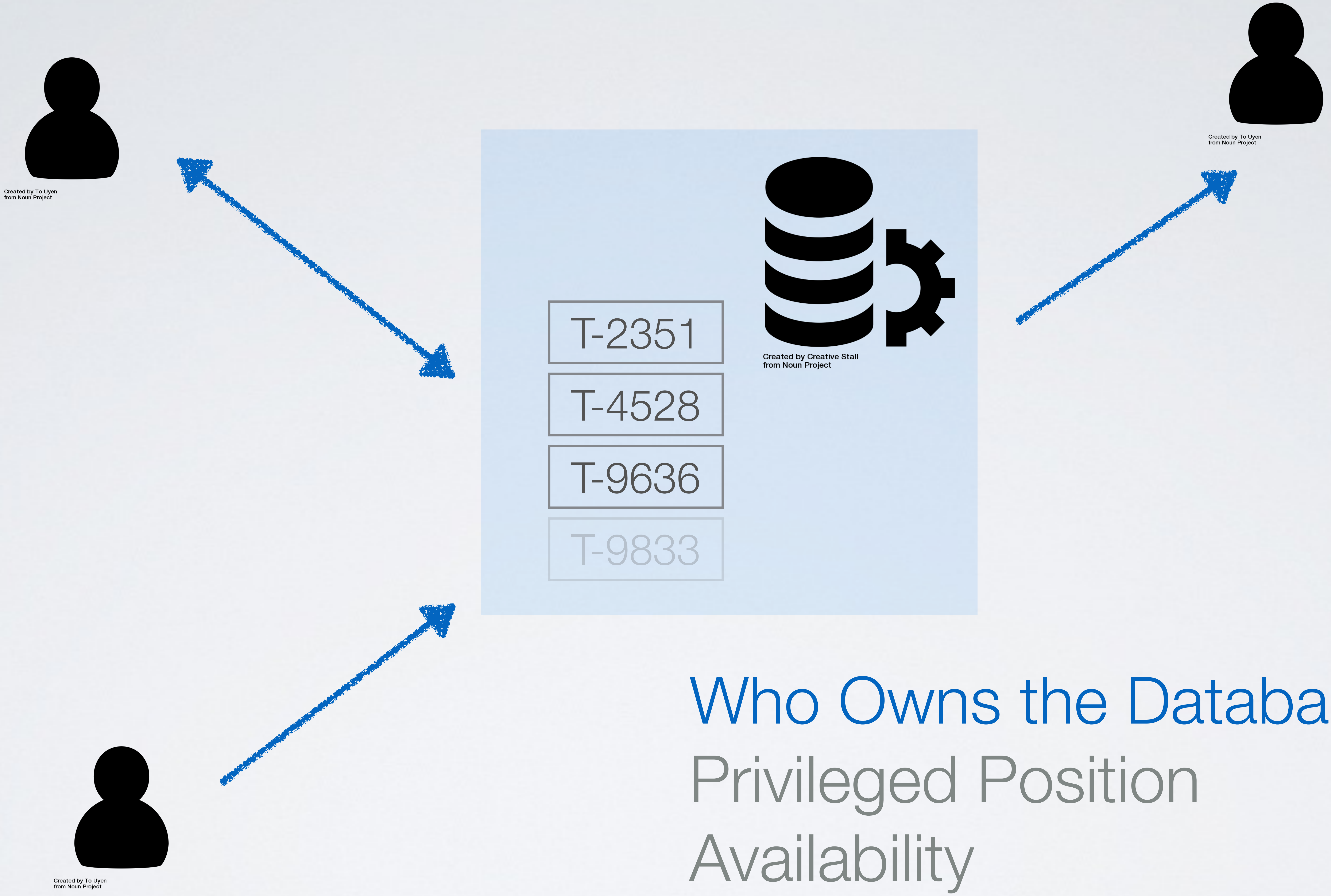
Created by To Uyen
from Noun Project

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

Created by Creative Stall
from Noun Project

Created by To Uyen
from Noun Project

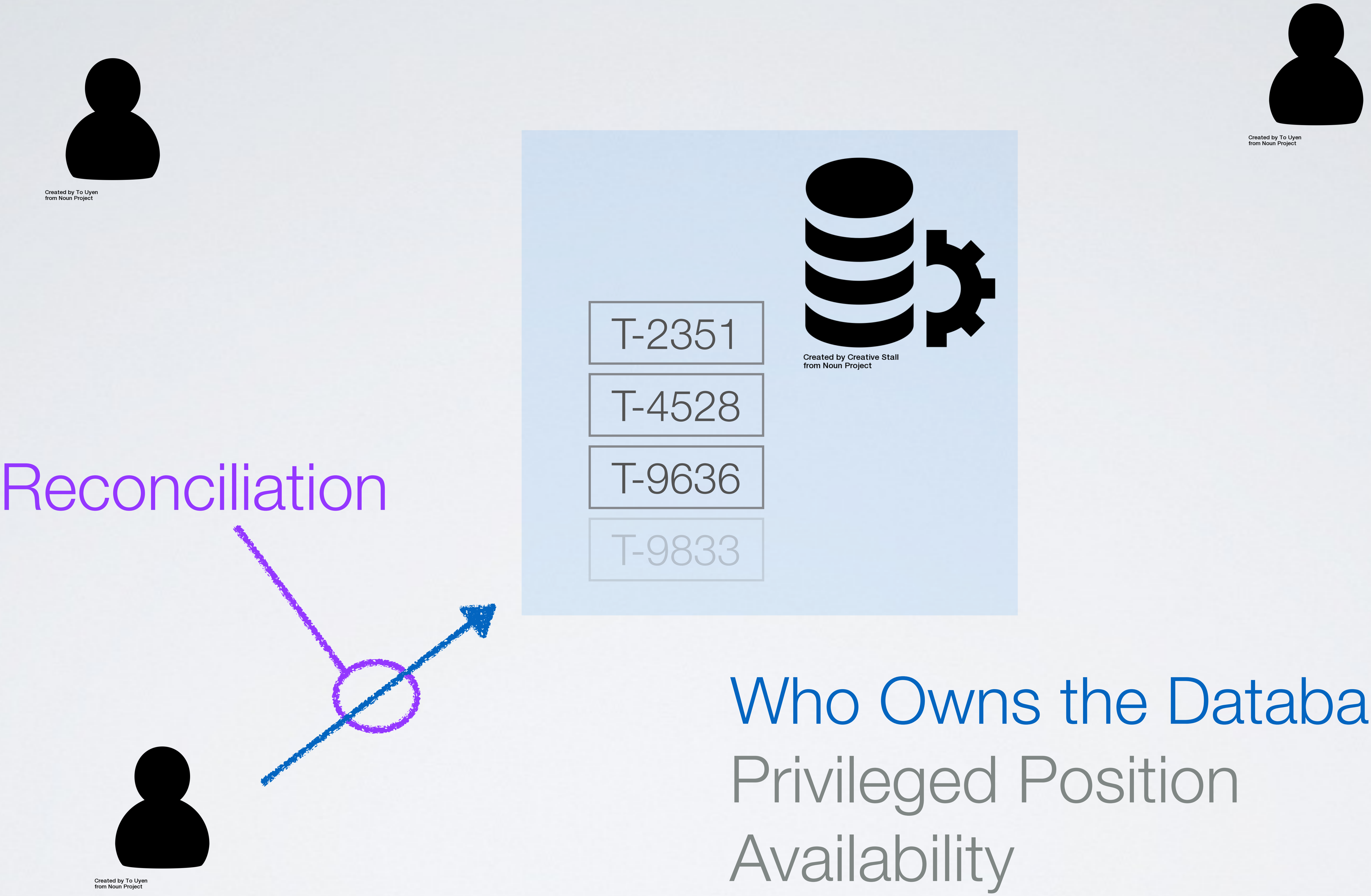
Created by To Uyen
from Noun Project

Who Owns the Database?

Privileged Position

Availability

Manage Access



Reconciliation

T-2351

T-4528

T-9636

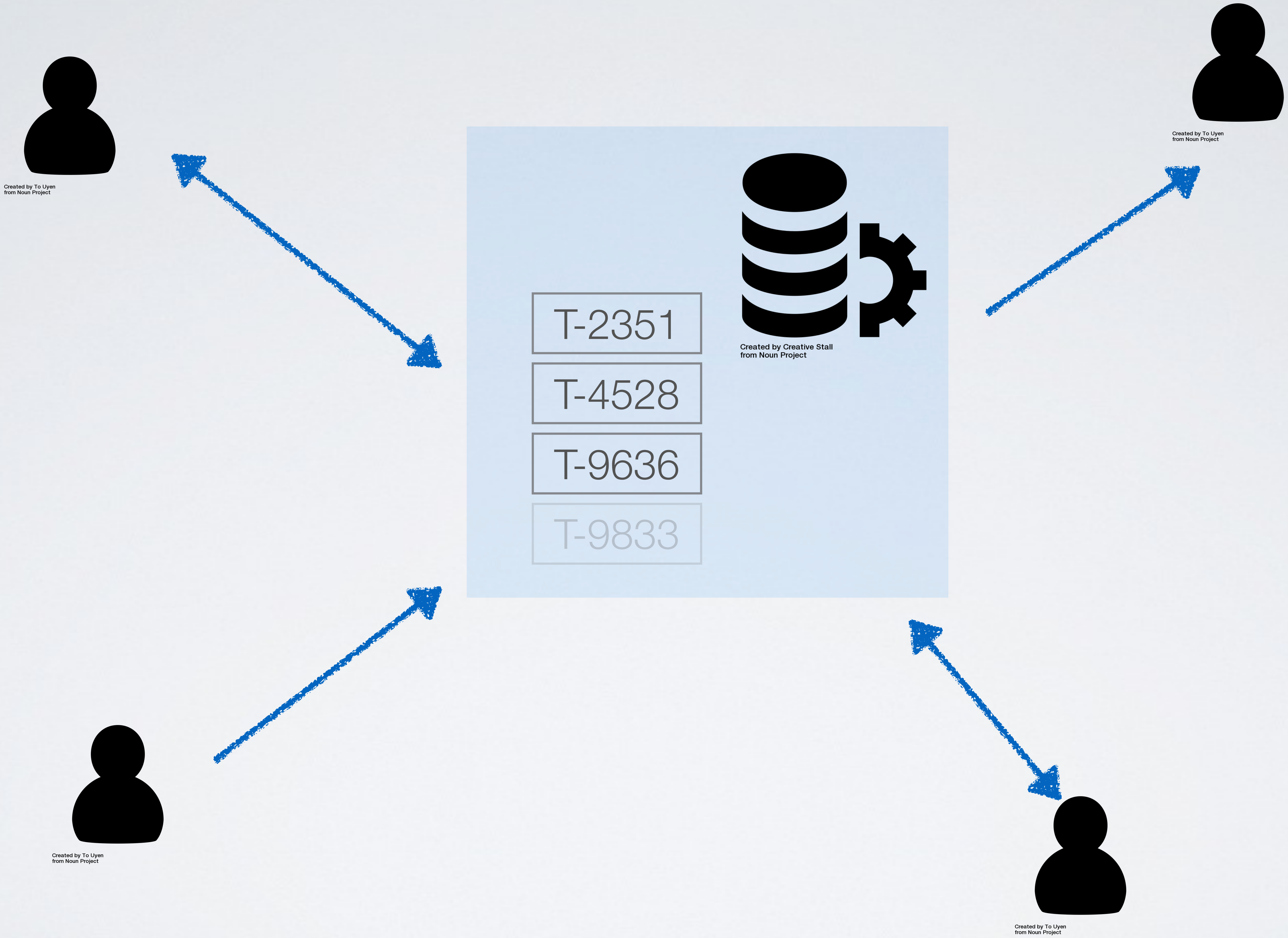
T-9833

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

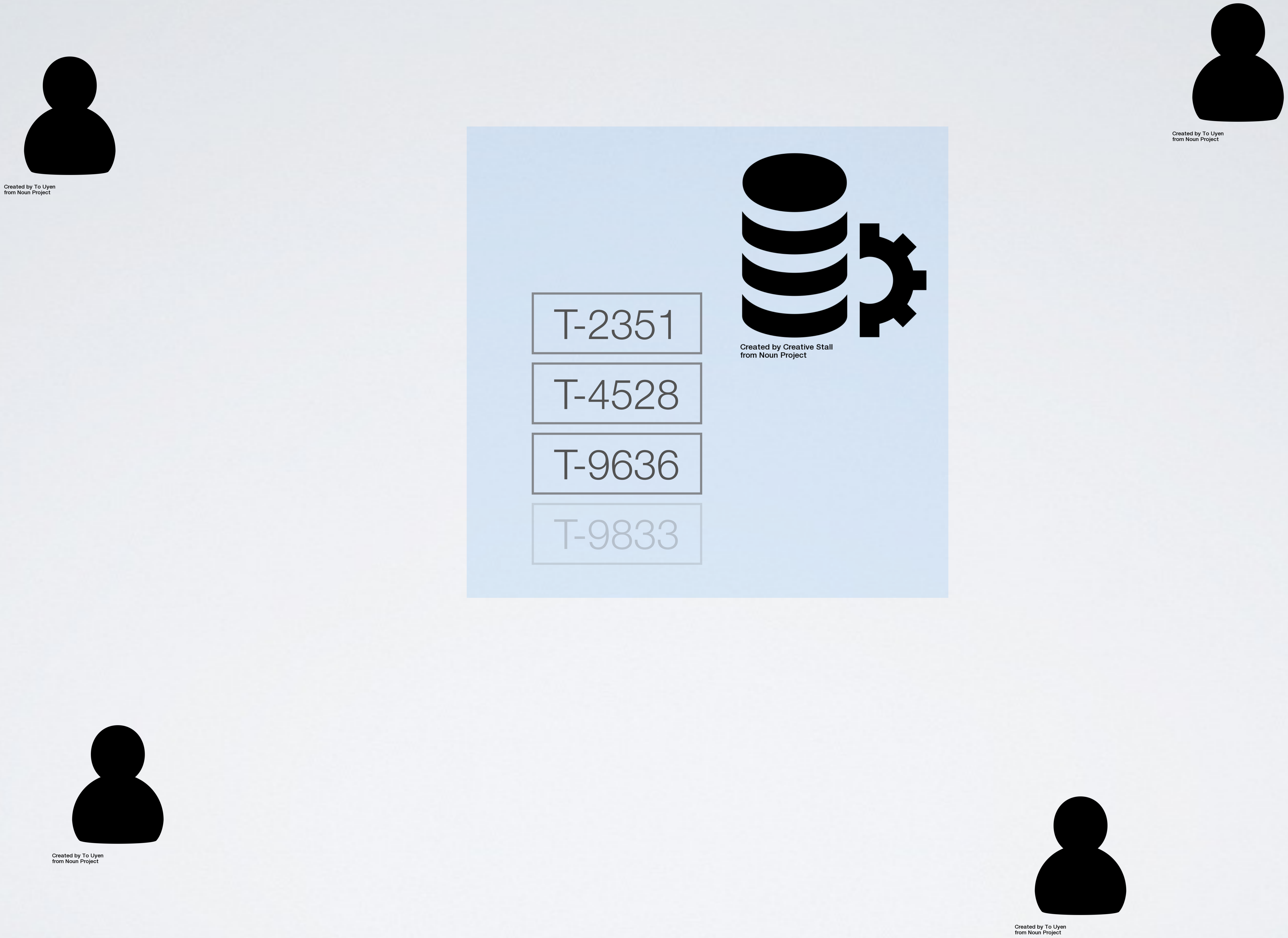
T-9636

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

Created by To Uyen
from Noun Project

T-2351

T-4528

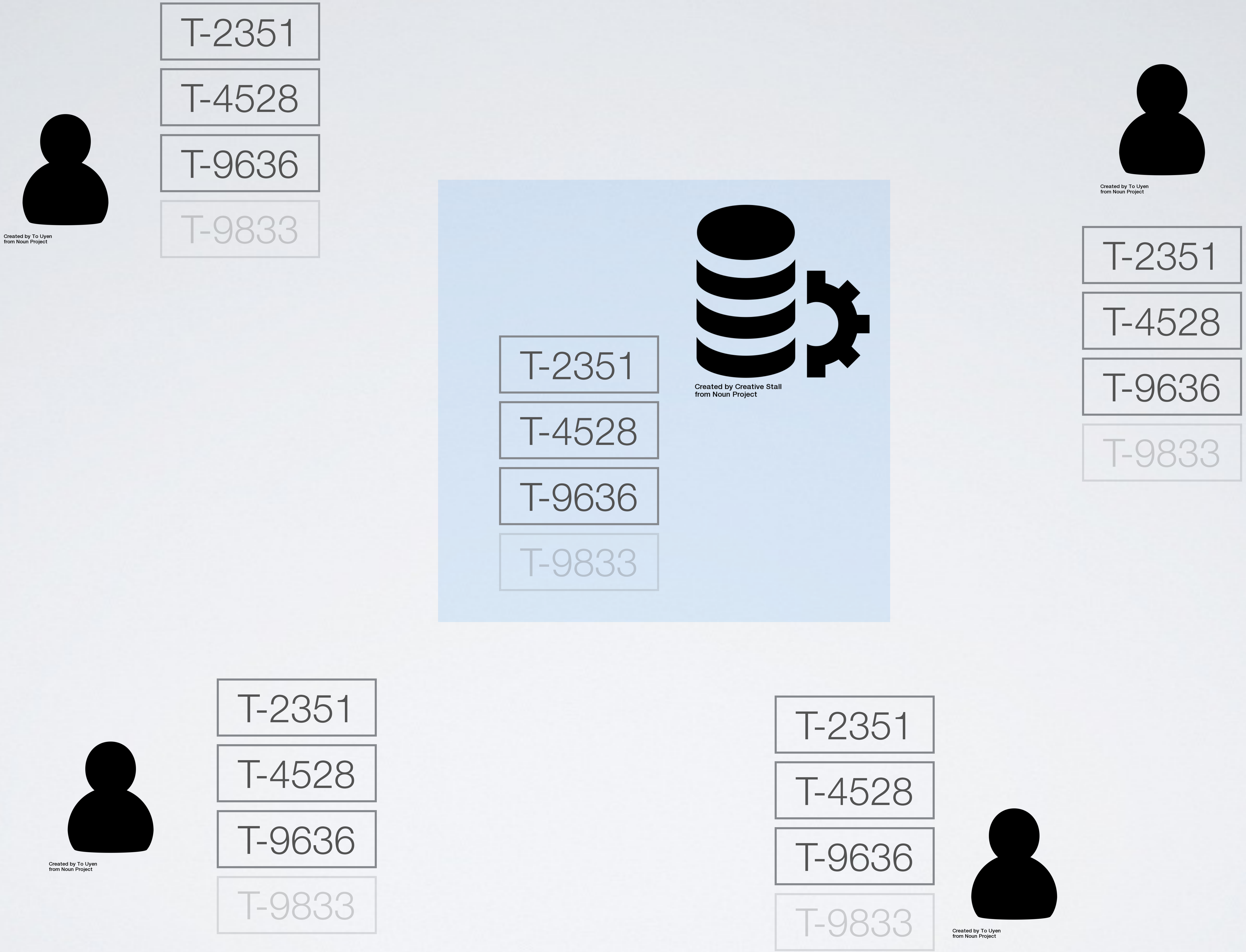
T-9636

T-9833

Created by Creative Stall
from Noun Project

Created by To Uyen
from Noun Project

Created by To Uyen
from Noun Project



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 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

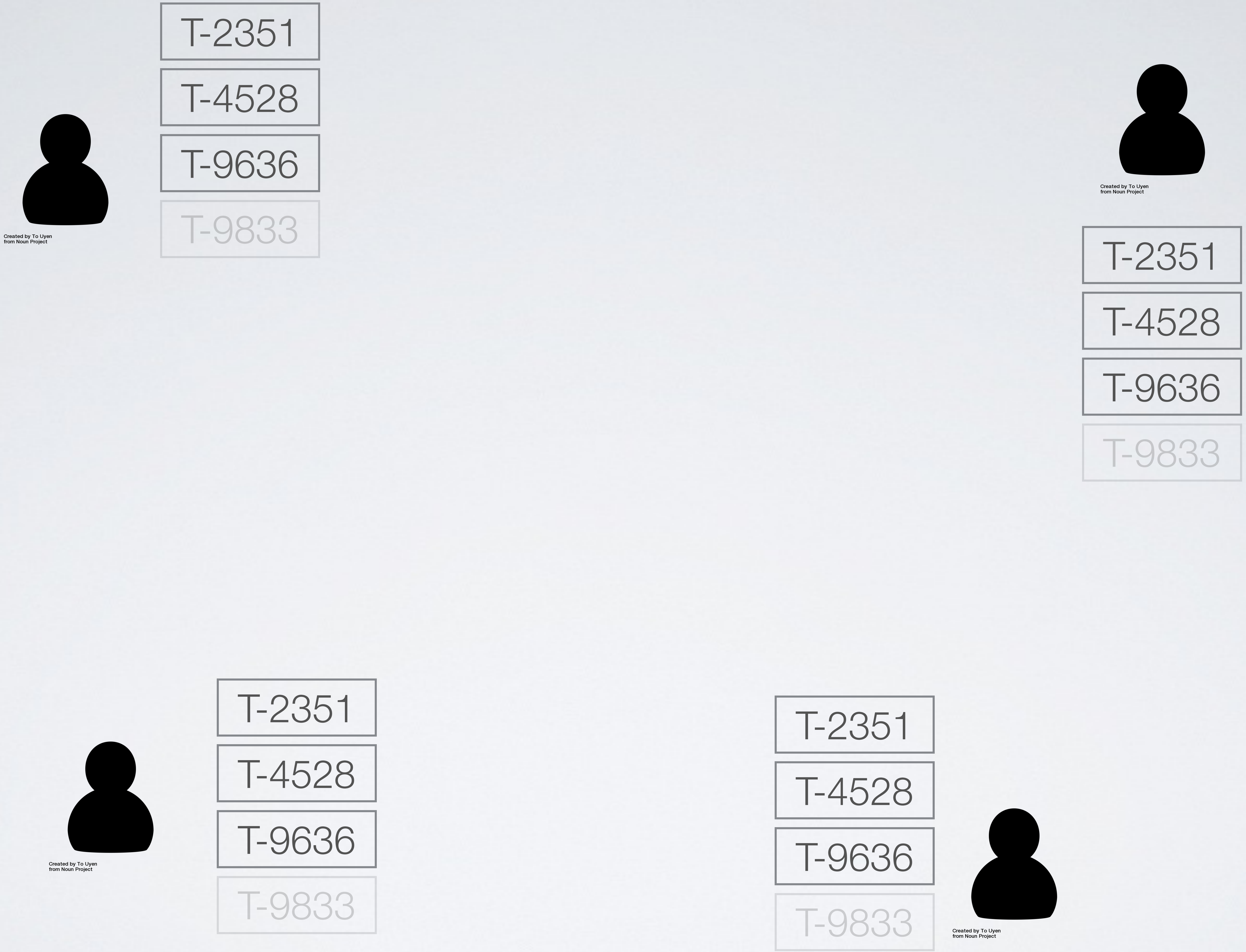
T-2351

T-4528

T-9636

T-9833

Created by To Uyen
from Noun Project



T-2351

T-4528

T-9636

T-9833

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

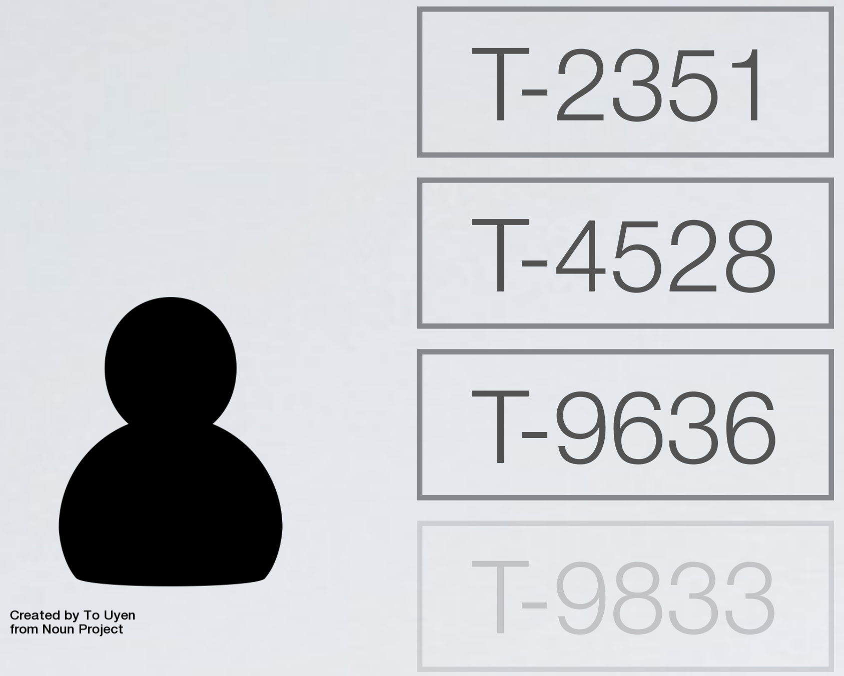
T-4528

T-9636

T-9833

Created by To Uyen
from Noun Project

Disintermediation



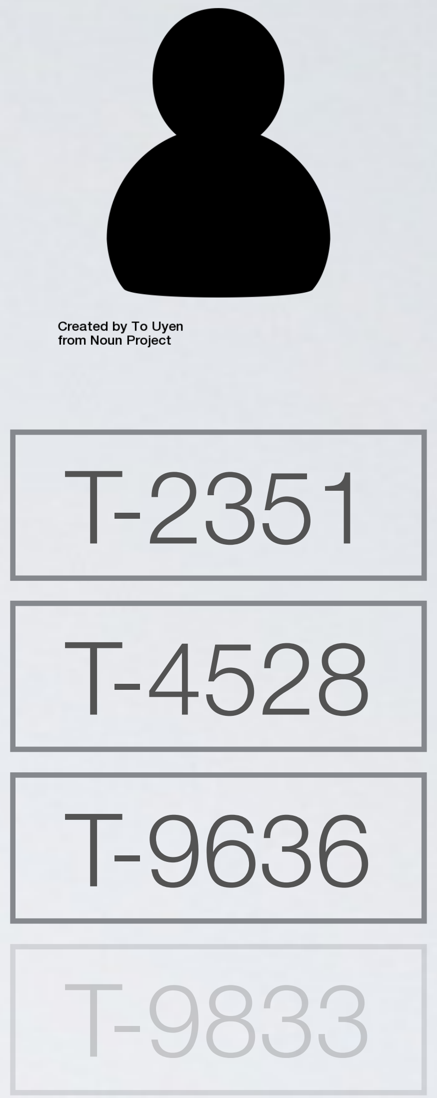
T-2351

T-4528

T-9636

T-9833

Created by To Uyen
from Noun Project



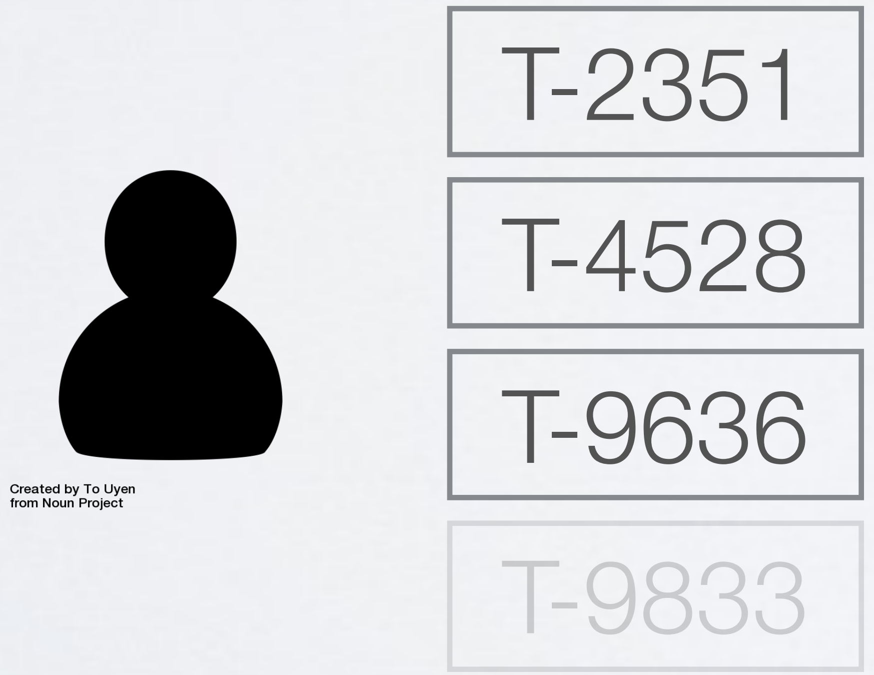
Created by To Uyen
from Noun Project

T-2351

T-4528

T-9636

T-9833



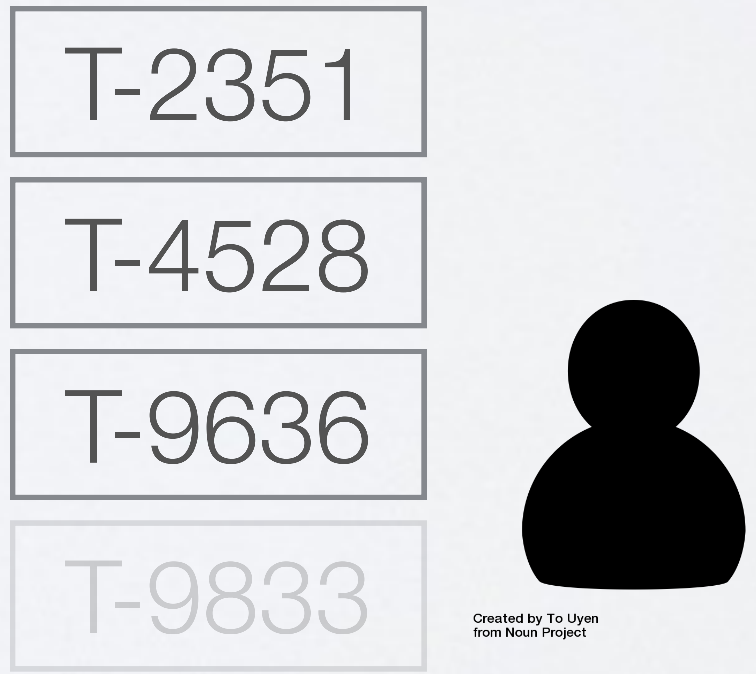
T-2351

T-4528

T-9636

T-9833

Created by To Uyen
from Noun Project



T-2351

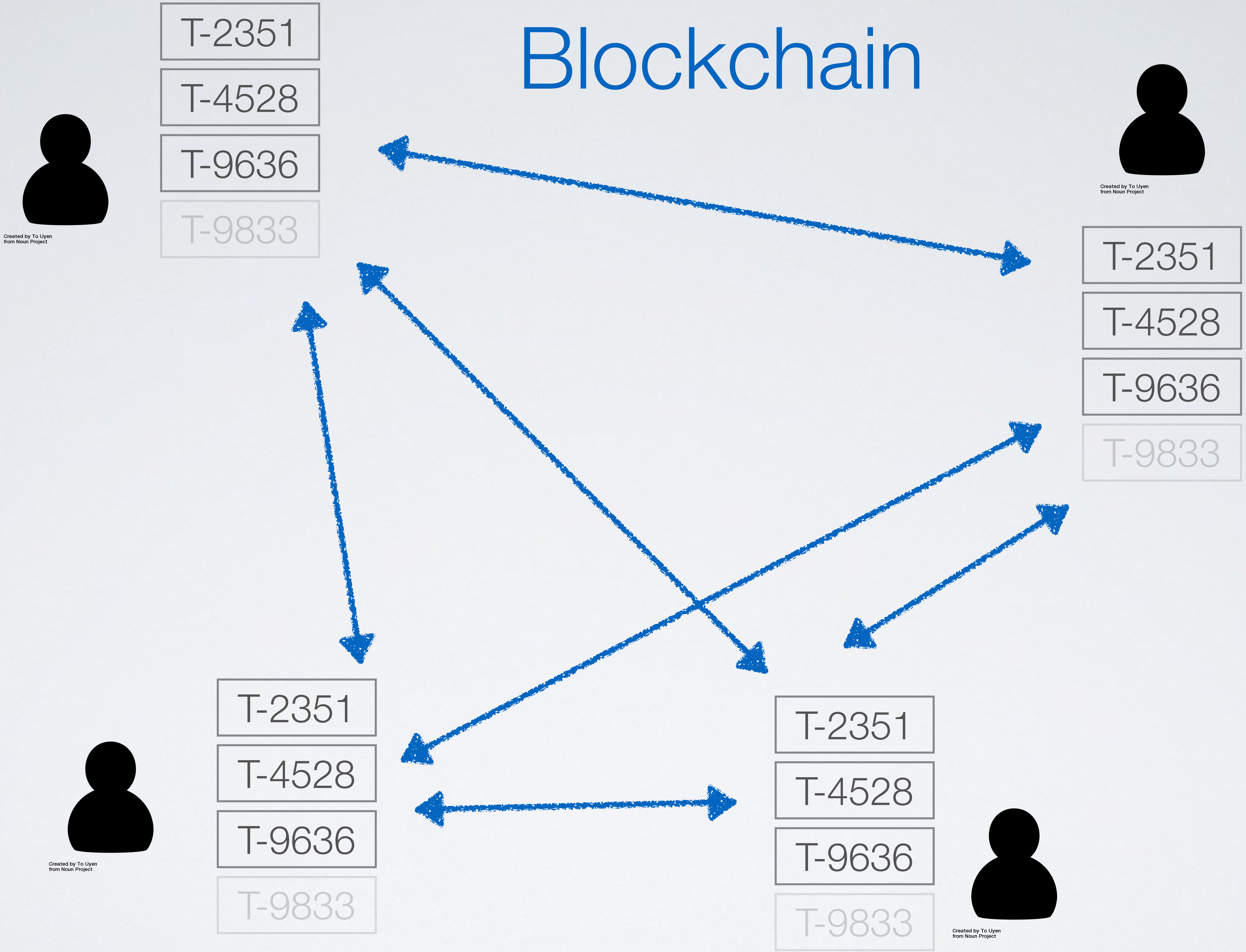
T-4528

T-9636

T-9833

Created by To Uyen
from Noun Project

Blockchain



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

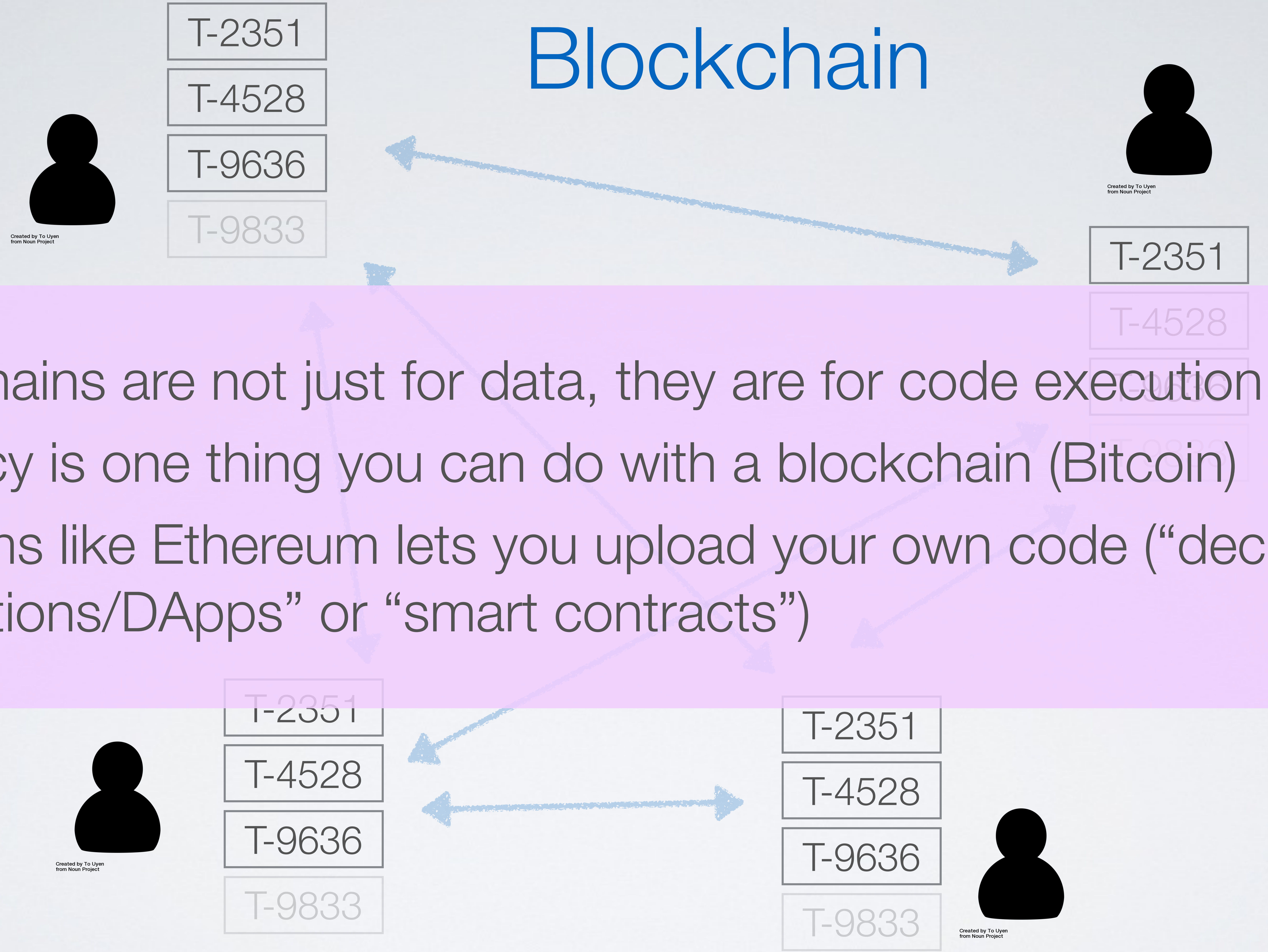
T-2351
T-4528
T-9636
T-9833

Created by To Uyen
from Noun Project

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

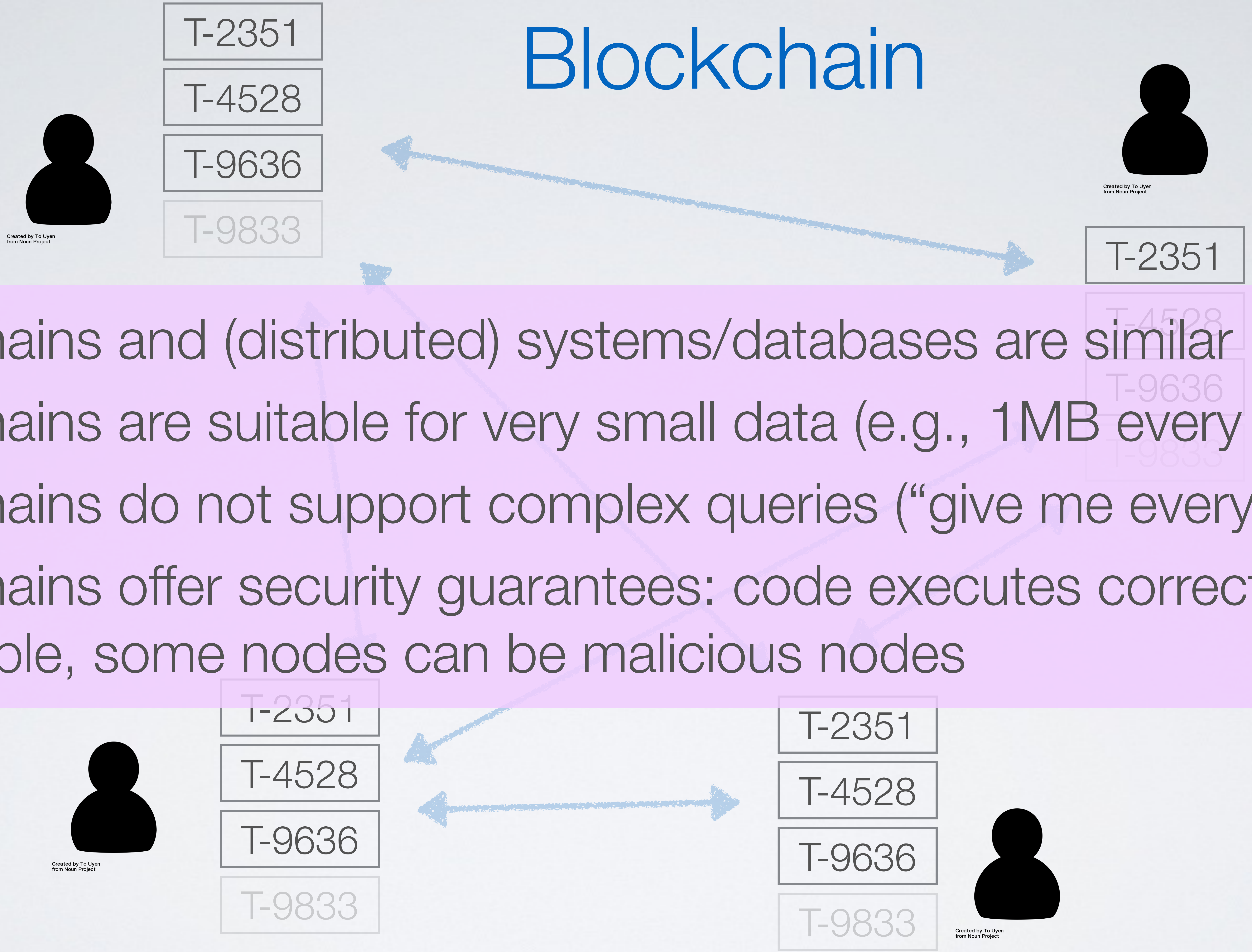
Created by To Uyen
from Noun Project

Blockchain


T-2351
T-4528
T-9636
T-9833
Created by To Uyen from Noun Project
T-2351
T-4528
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
Created by To Uyen from Noun Project

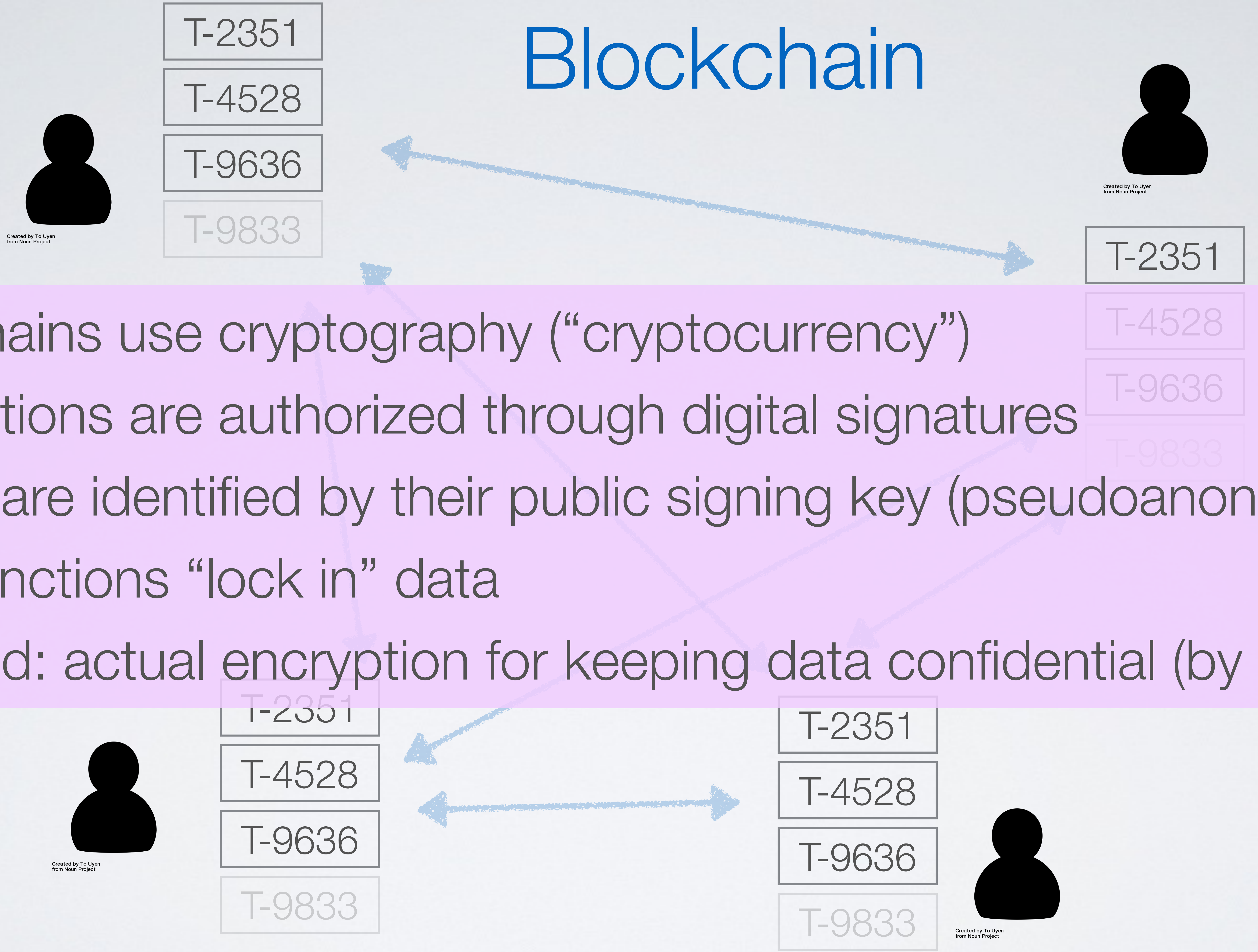
- Blockchains are not just for data, they are for code execution
- Currency is one thing you can do with a blockchain (Bitcoin)
- Platforms like Ethereum lets you upload your own code (“decentralized applications/DApps” or “smart contracts”)

Blockchain


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
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

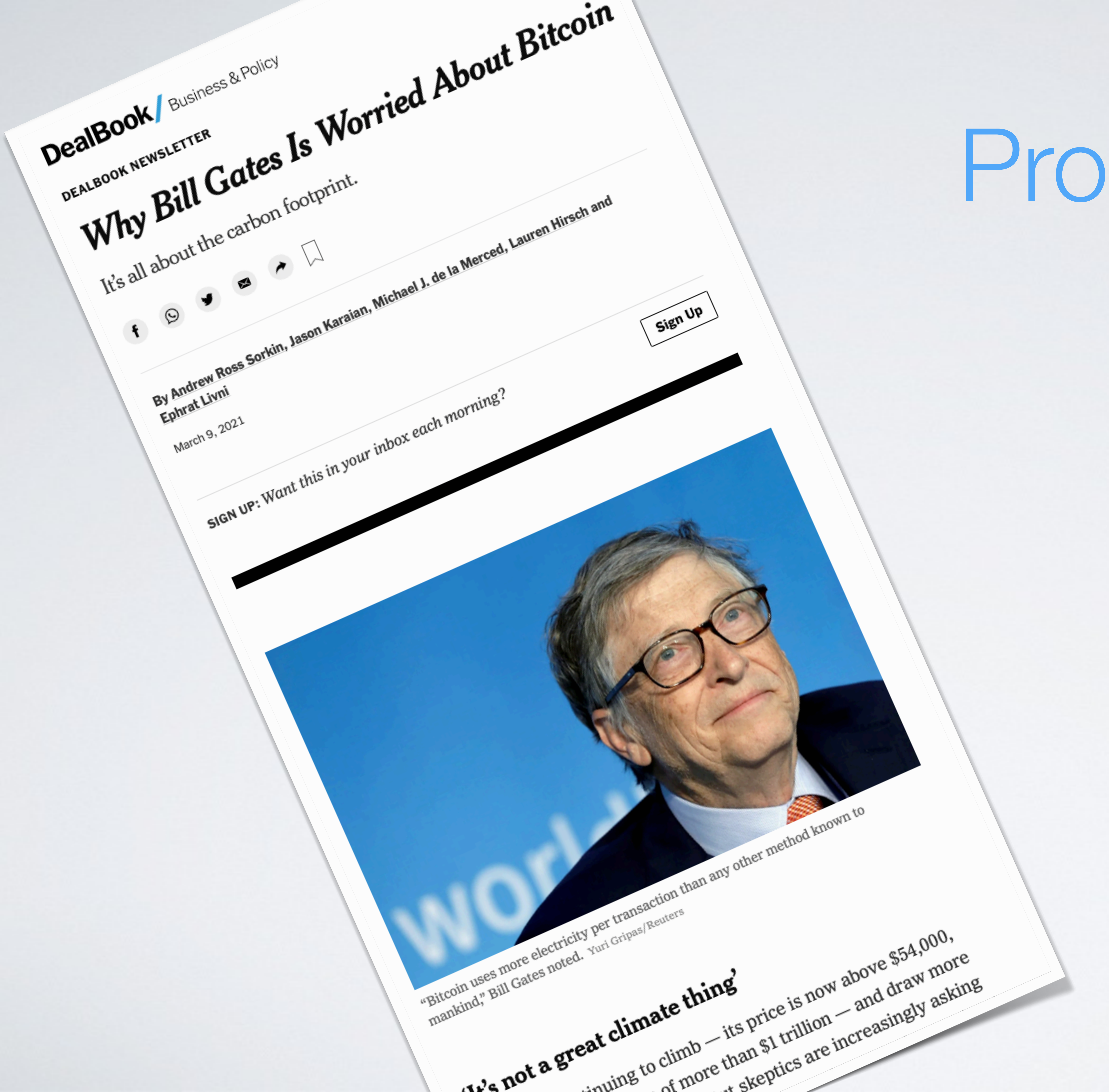
- Blockchains and (distributed) systems/databases are similar
- Blockchains are suitable for very small data (e.g., 1MB every 10 min)
- Blockchains do not support complex queries ("give me everything")
- Blockchains offer security guarantees: code executes correctly, data is immutable, some nodes can be malicious nodes

Blockchain


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
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

- Blockchains use cryptography (“cryptocurrency”)
- Transactions are authorized through digital signatures
- Entities are identified by their public signing key (pseudoanonymity)
- Hash functions “lock in” data
- Not used: actual encryption for keeping data confidential (by default)

Proof of Work



DealBook/ Business & Policy

DEALBOOK NEWSLETTER

Why Bill Gates Is Worried About Bitcoin

It's all about the carbon footprint.

By Andrew Ross Sorkin, Jason Karaian, Michael J. de la Merced, Lauren Hirsch and Ephrat Livni

March 9, 2021

SIGN UP: *Want this in your inbox each morning?*

Sign Up

"Bitcoin uses more electricity per transaction than any other method known to mankind," Bill Gates noted. Yuri Gripas/Reuters

'It's not a great climate thing'

inuing to climb — its price is now above $54,000,
of more than $1 trillion — and draw more
ut skeptics are increasingly asking

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

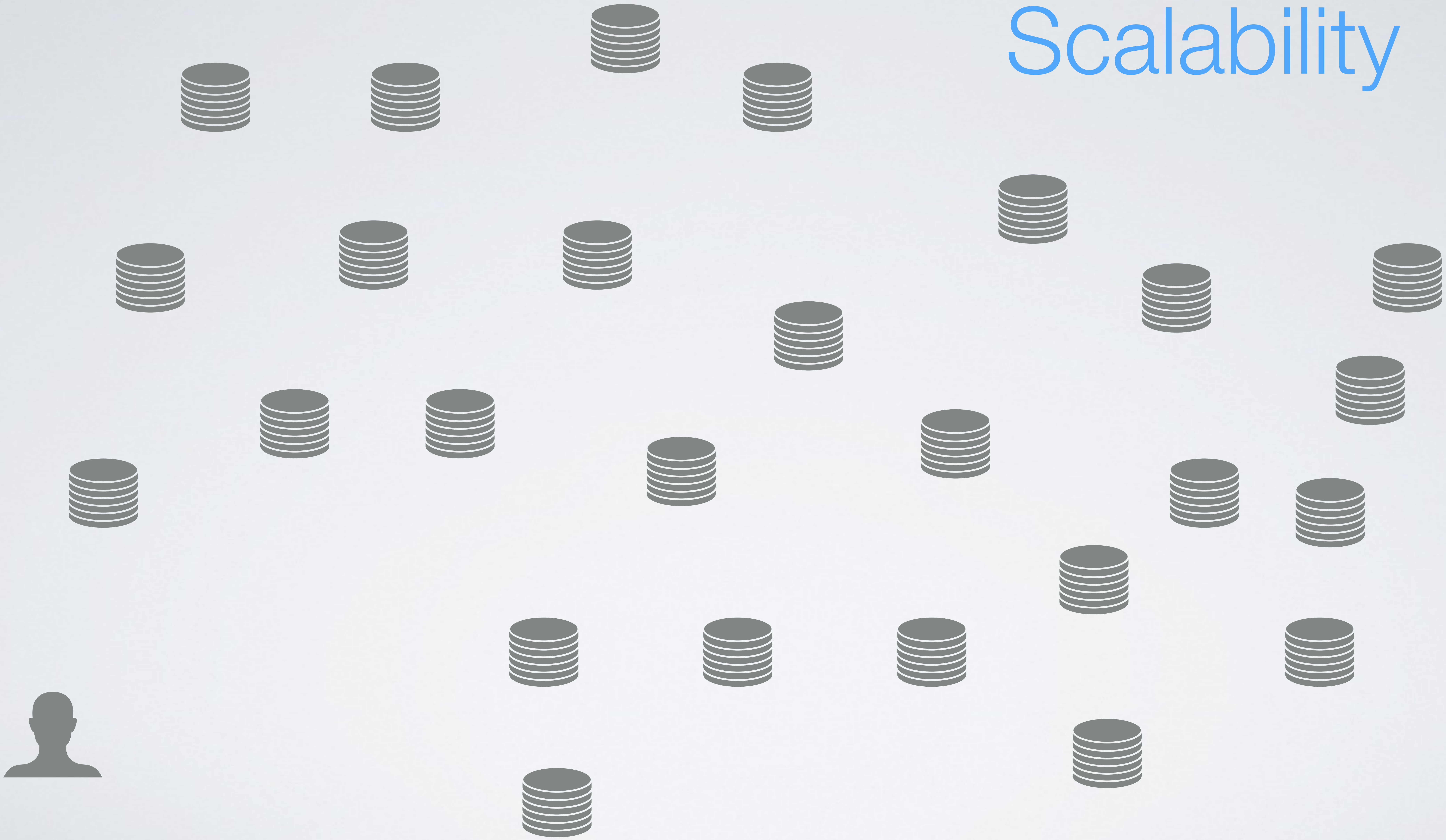
2) Unit of computational effort:

Bitcoin’s blockchain

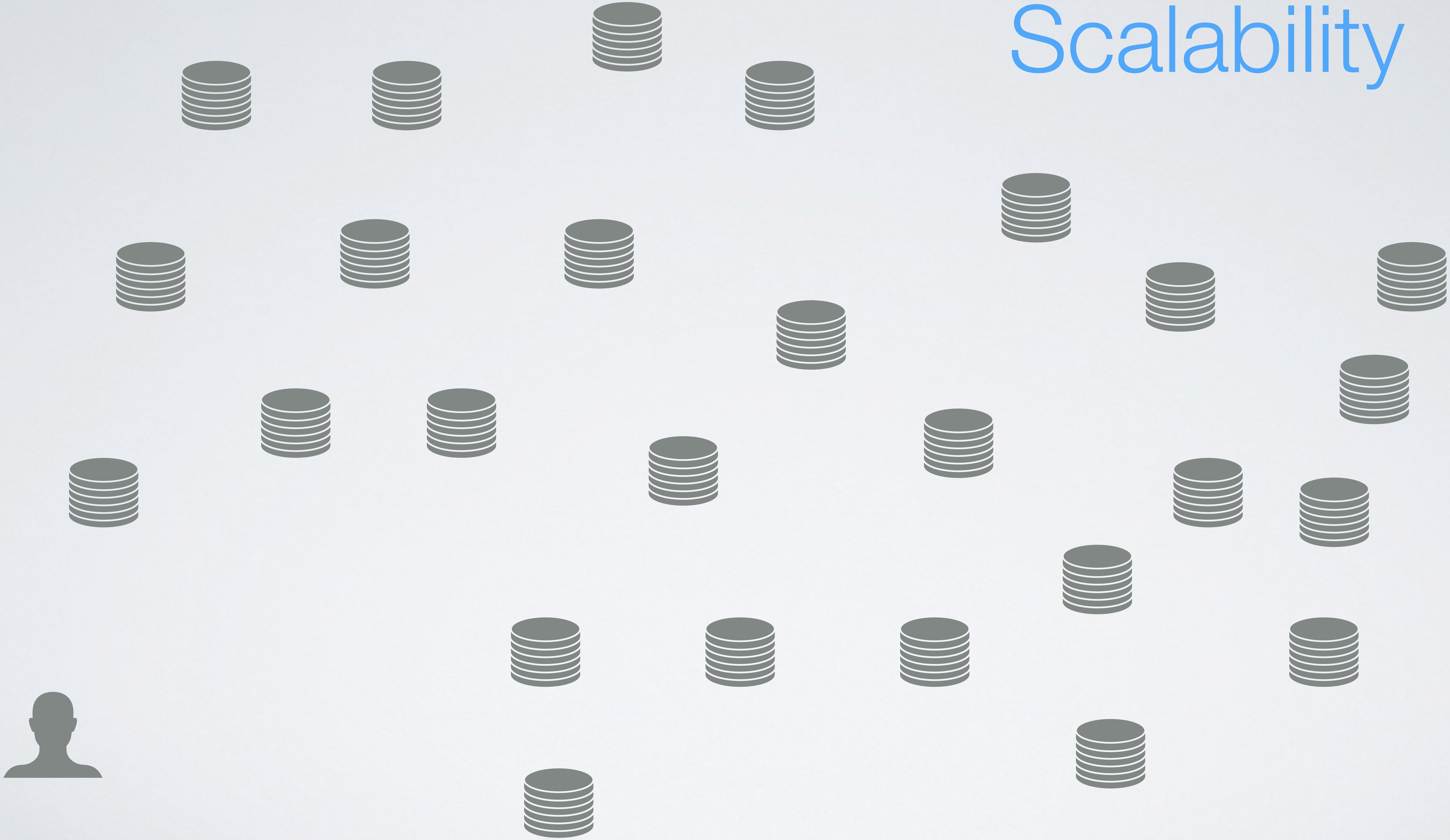
No trust, open network

Research Directions

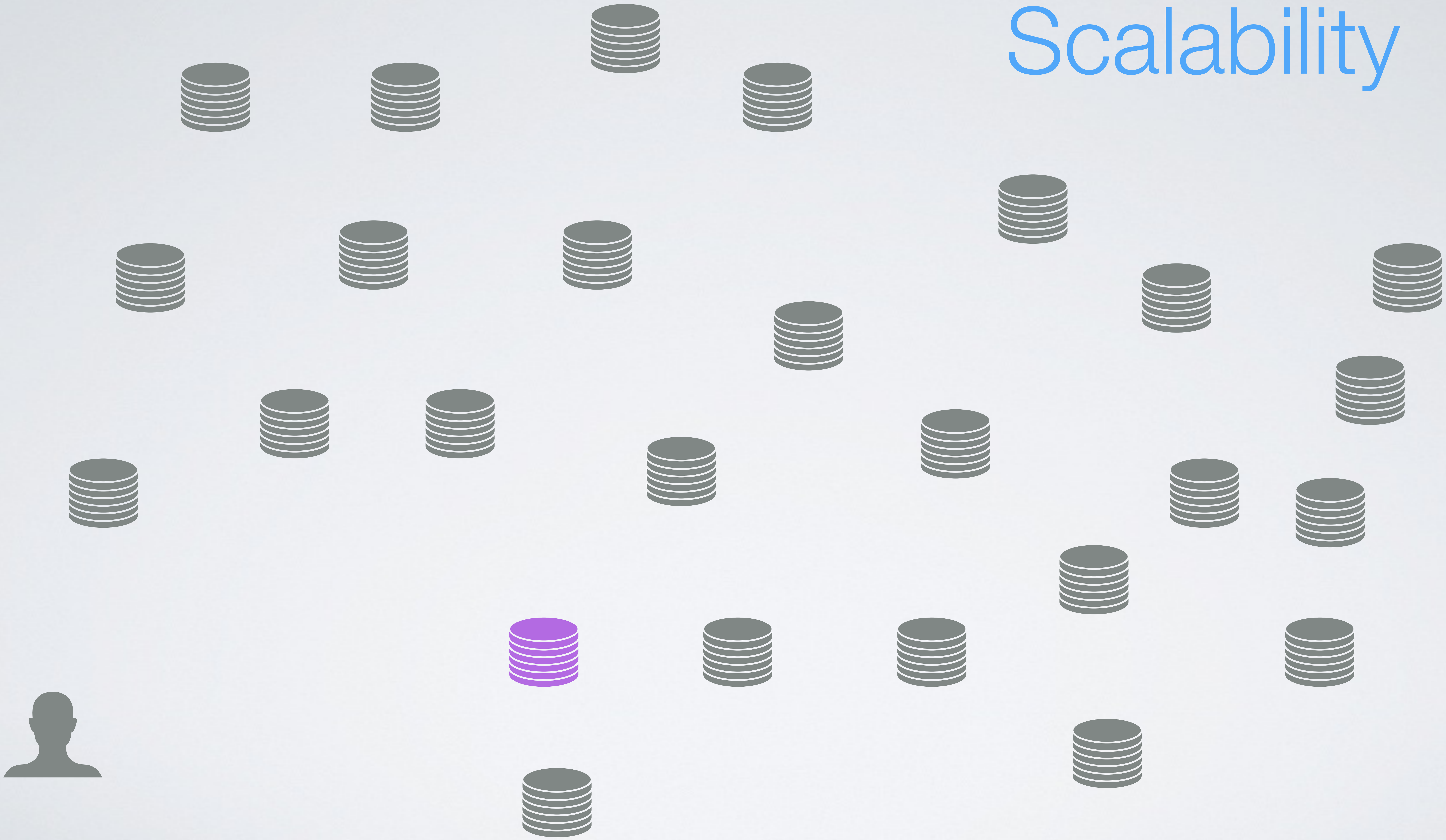
Scalability



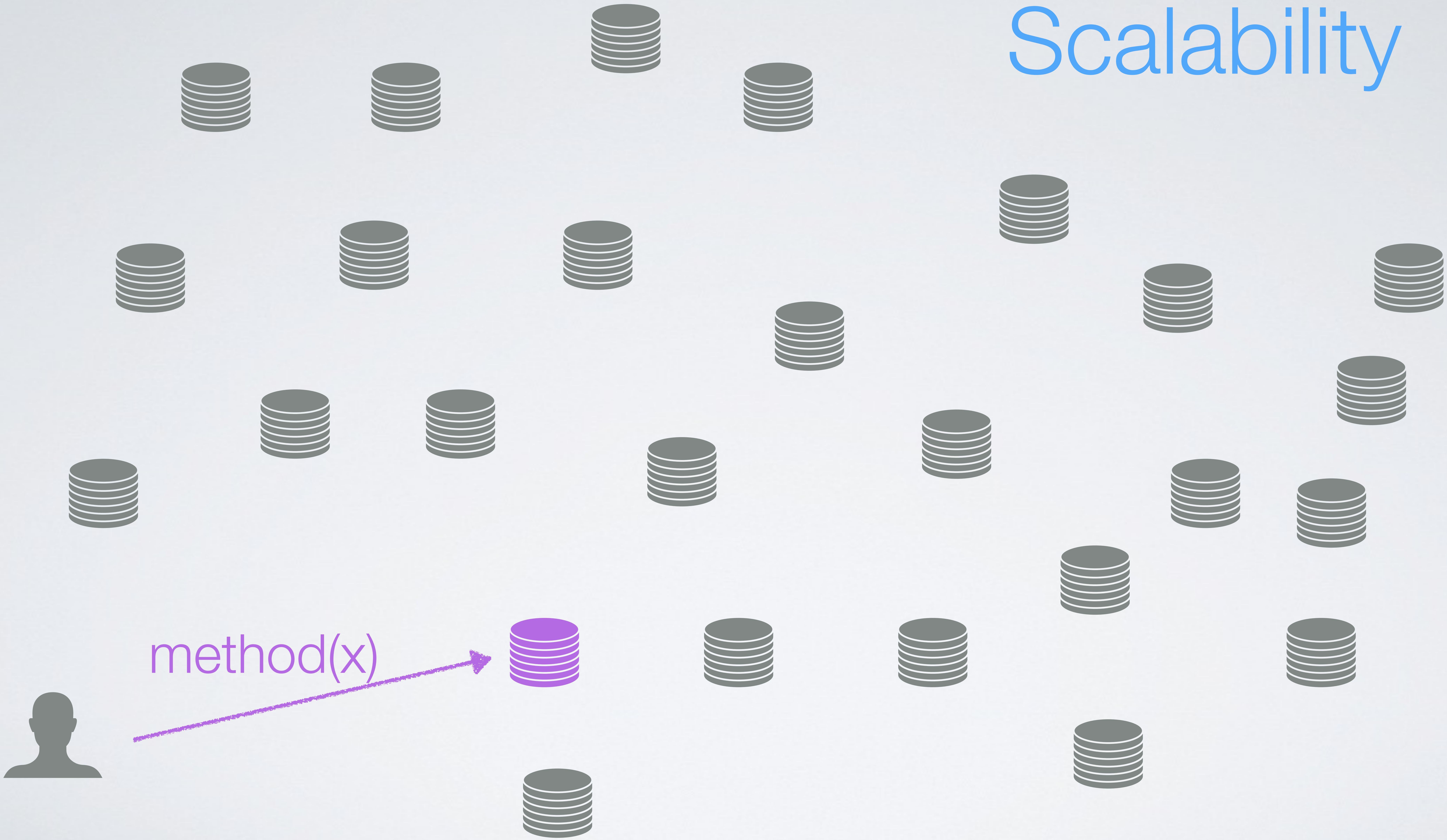
Scalability



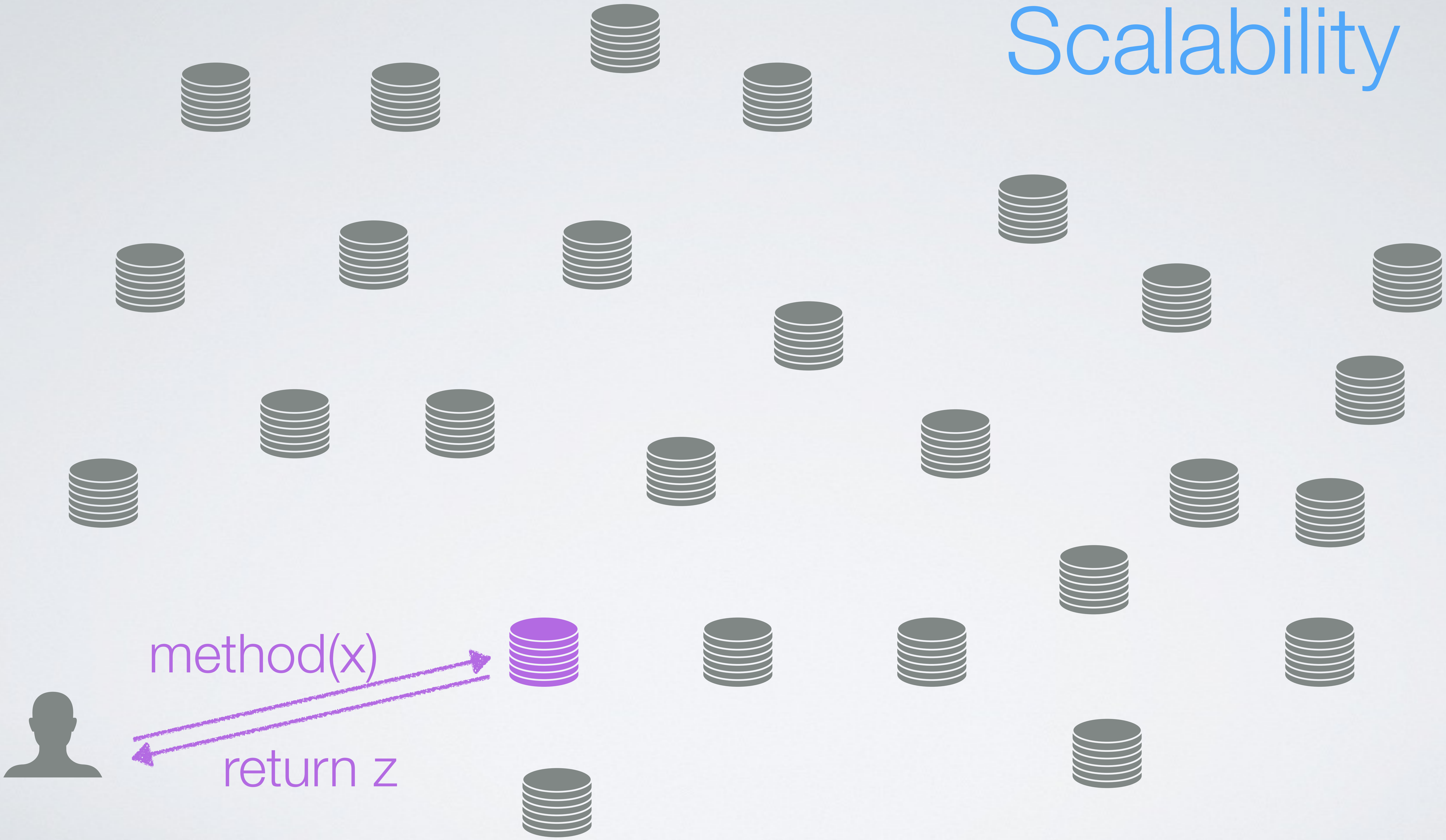
Scalability



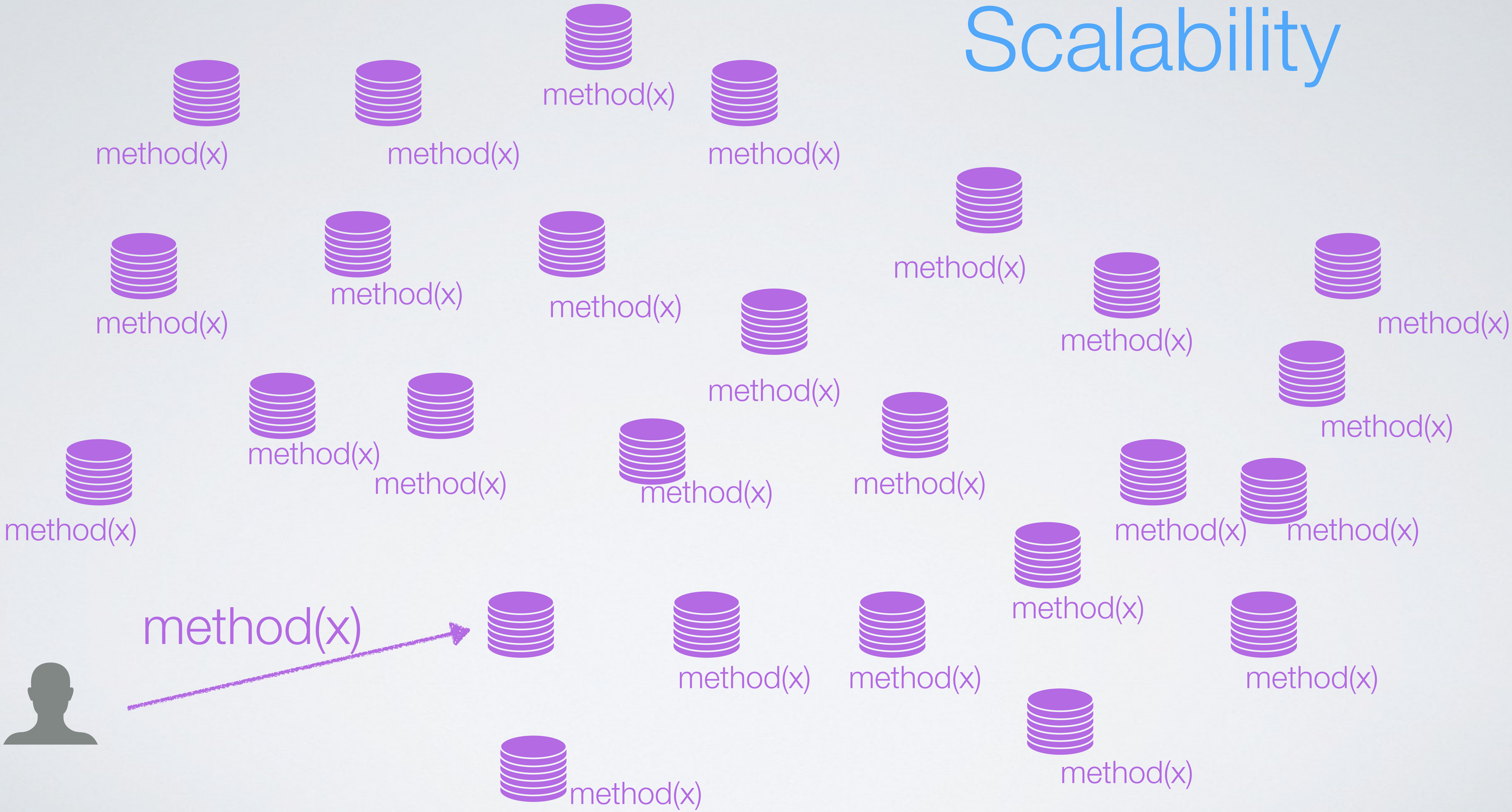
Scalability



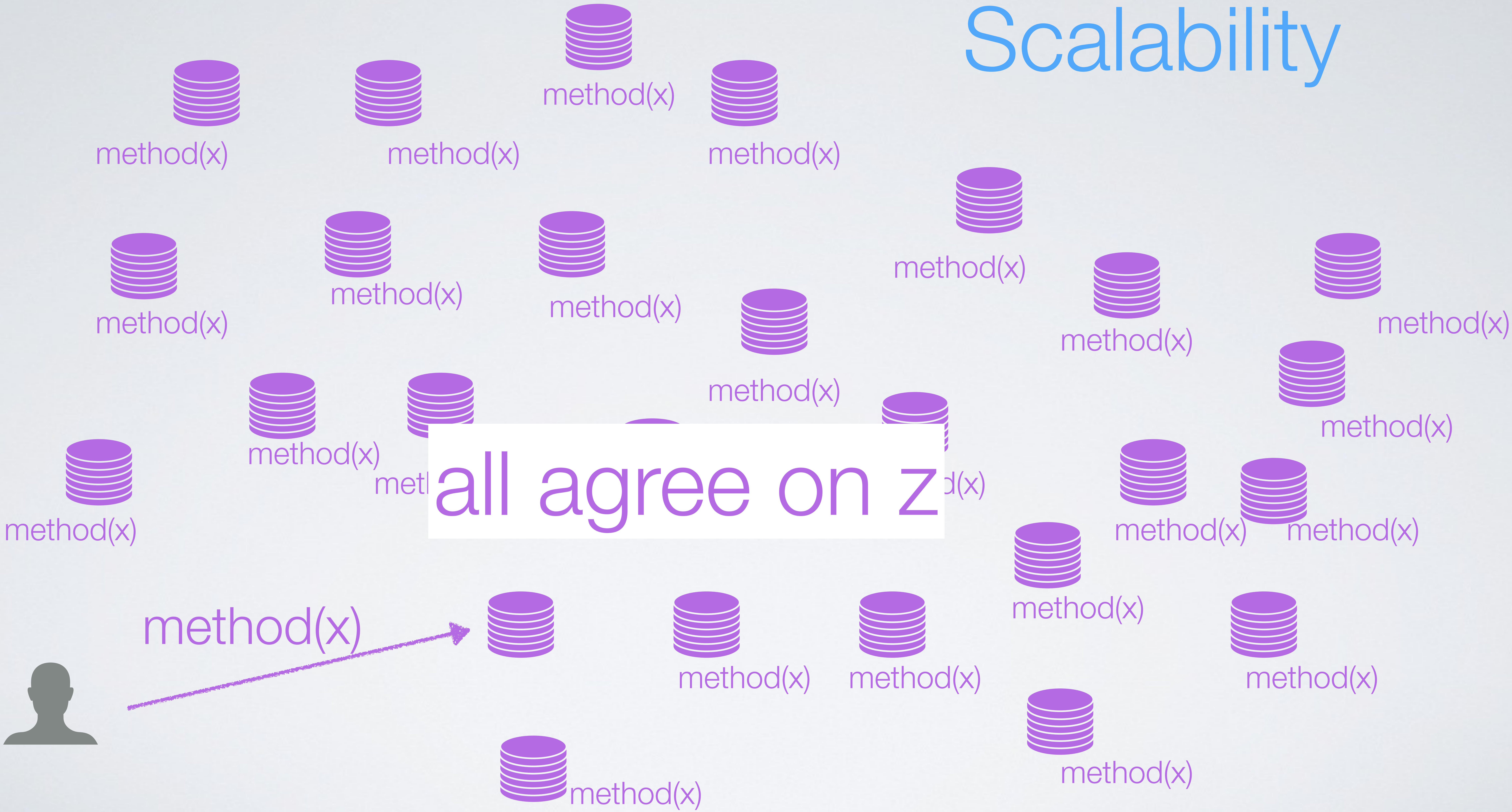
Scalability



Scalability

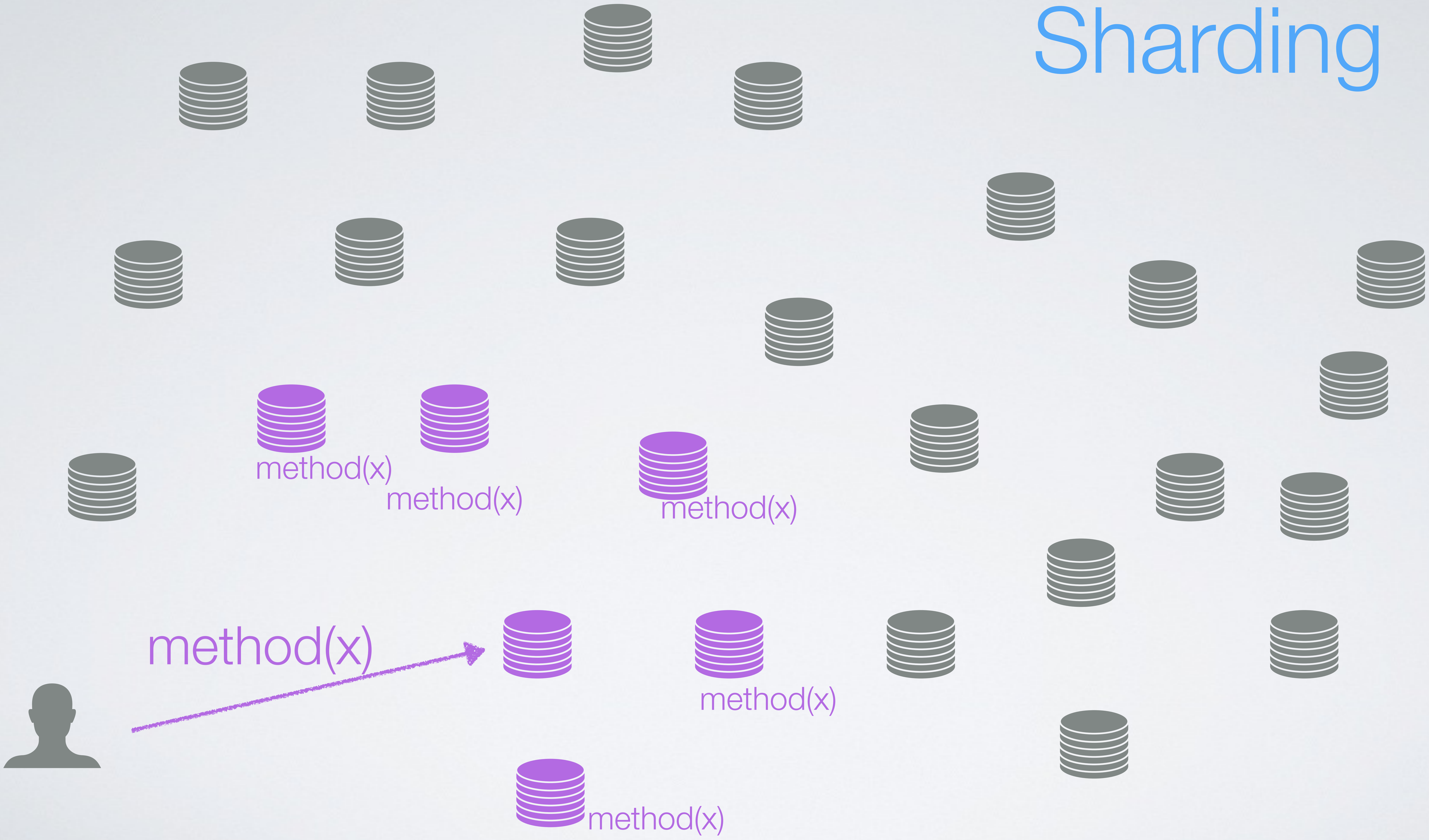


Scalability

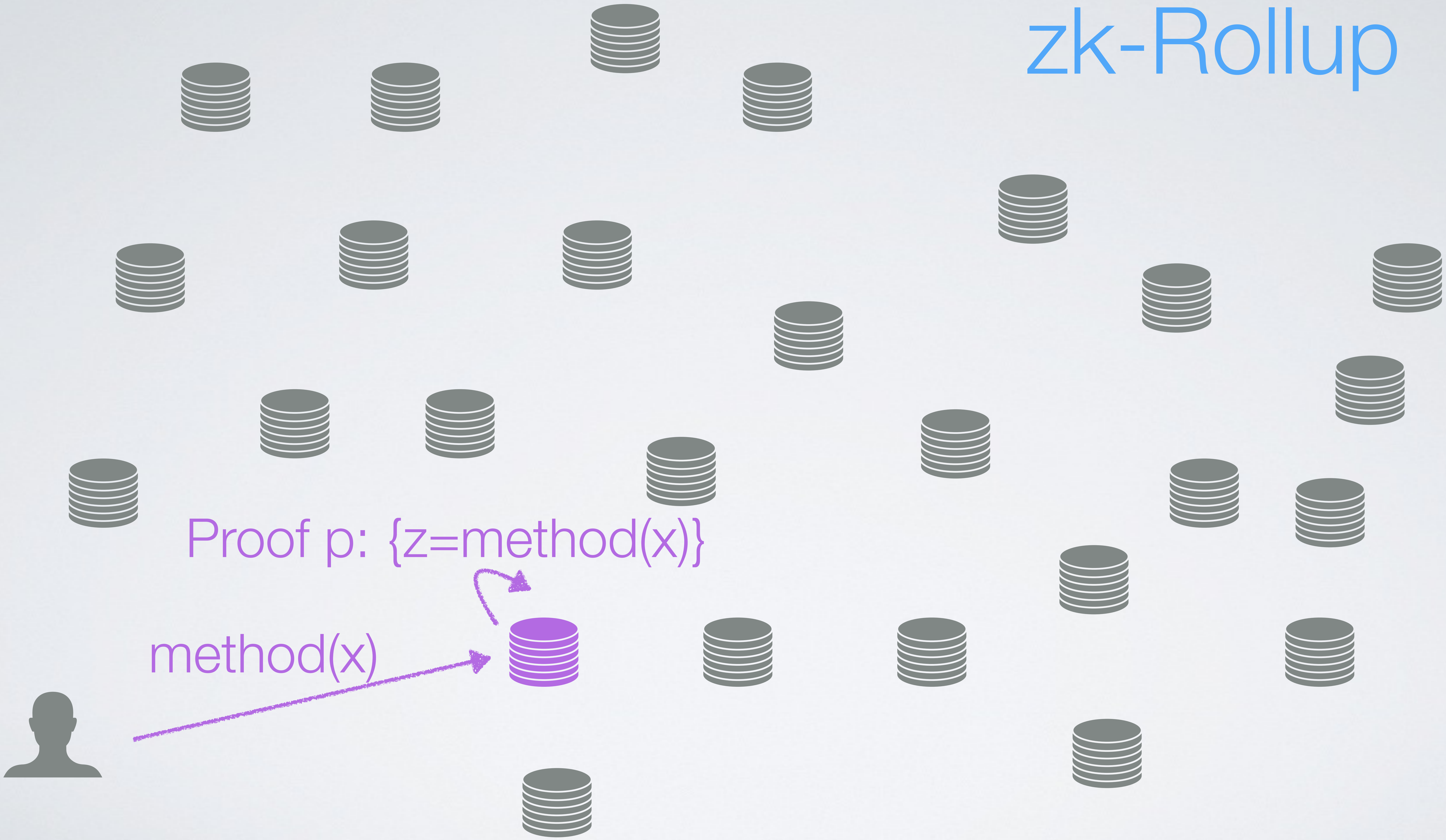


all agree on z

Sharding



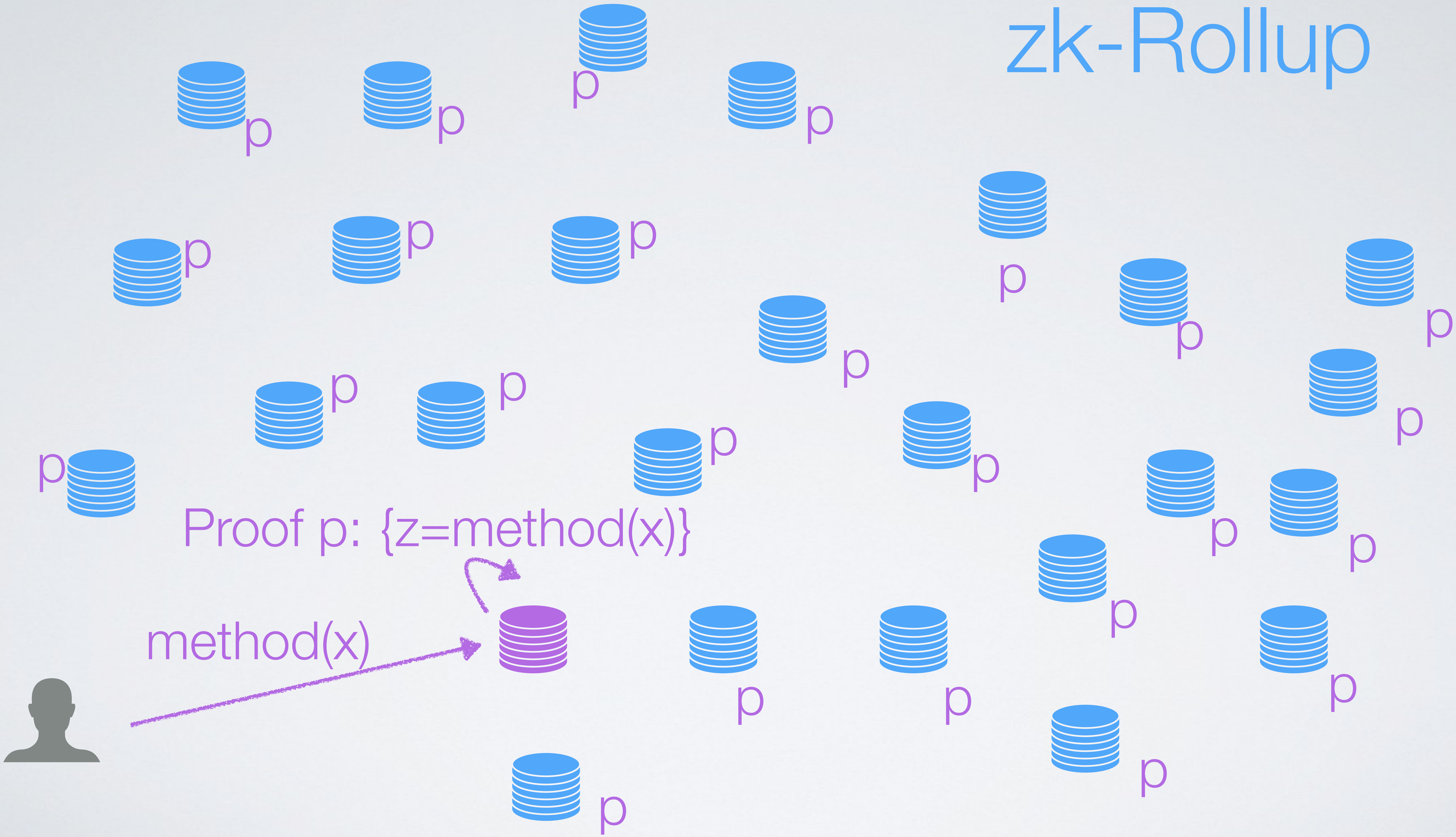
zk-Rollup



Proof p: {z=method(x)}

method(x)

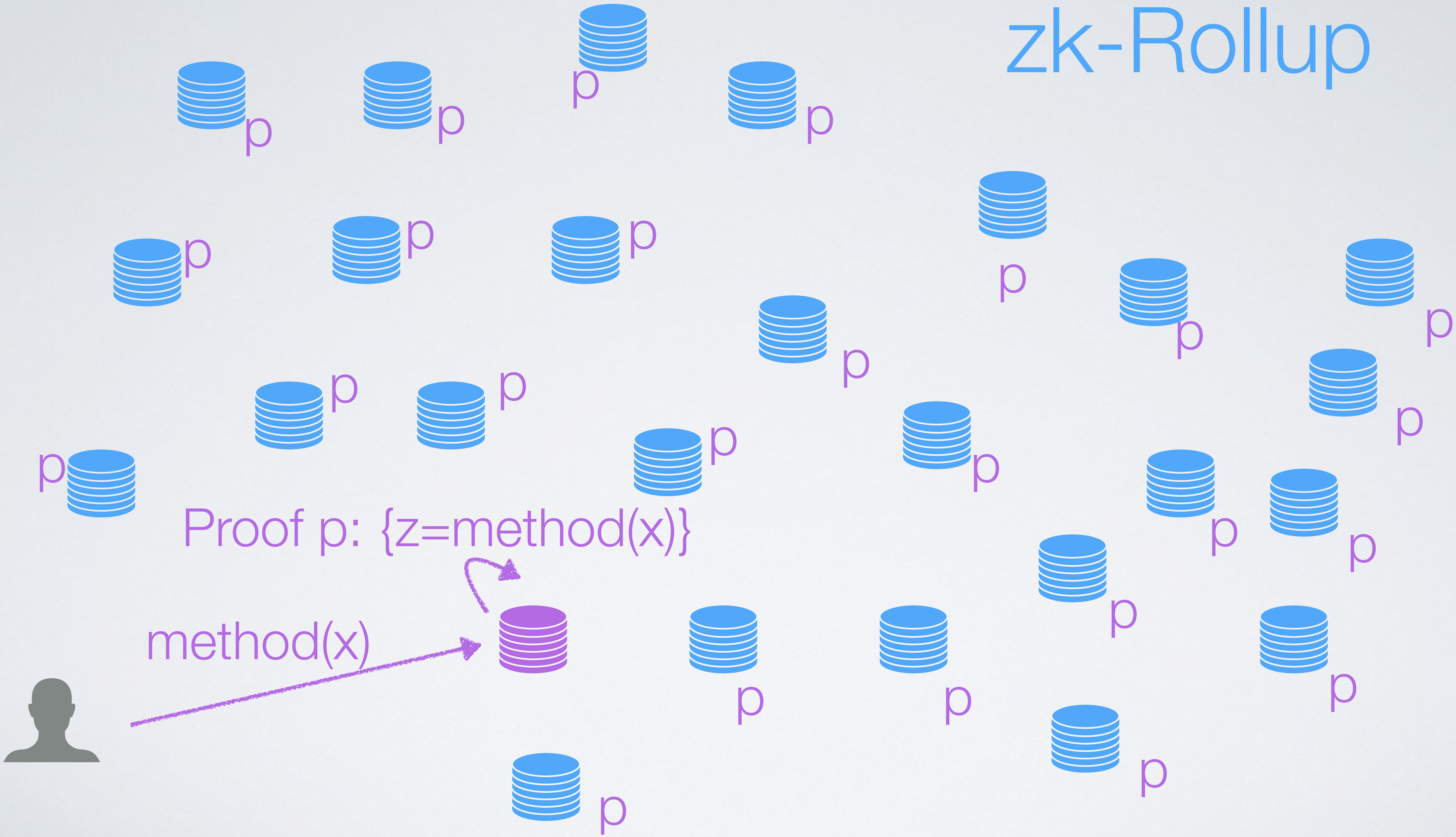
zk-Rollup



Proof p: {z=method(x)}

method(x)

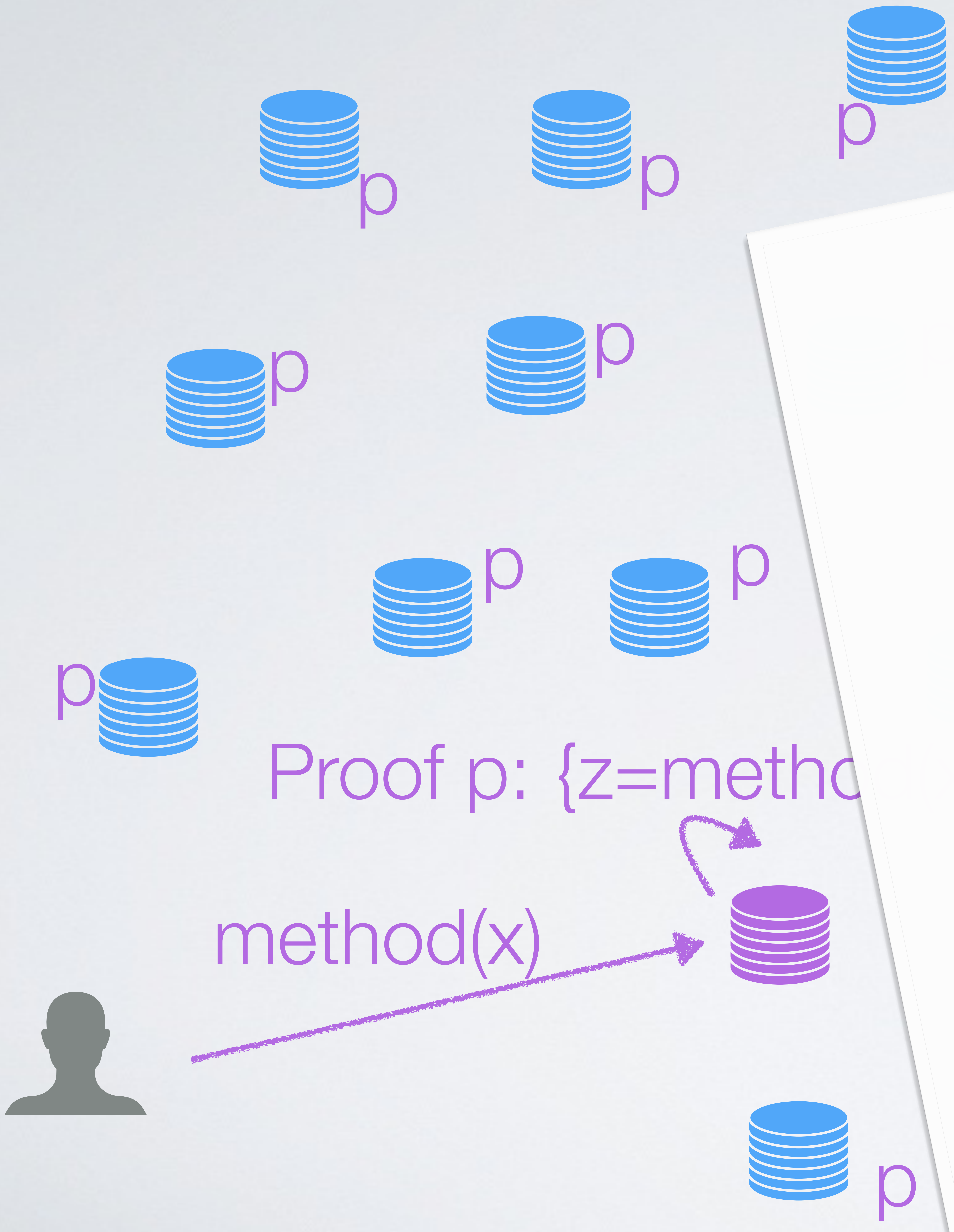
zk-Rollup

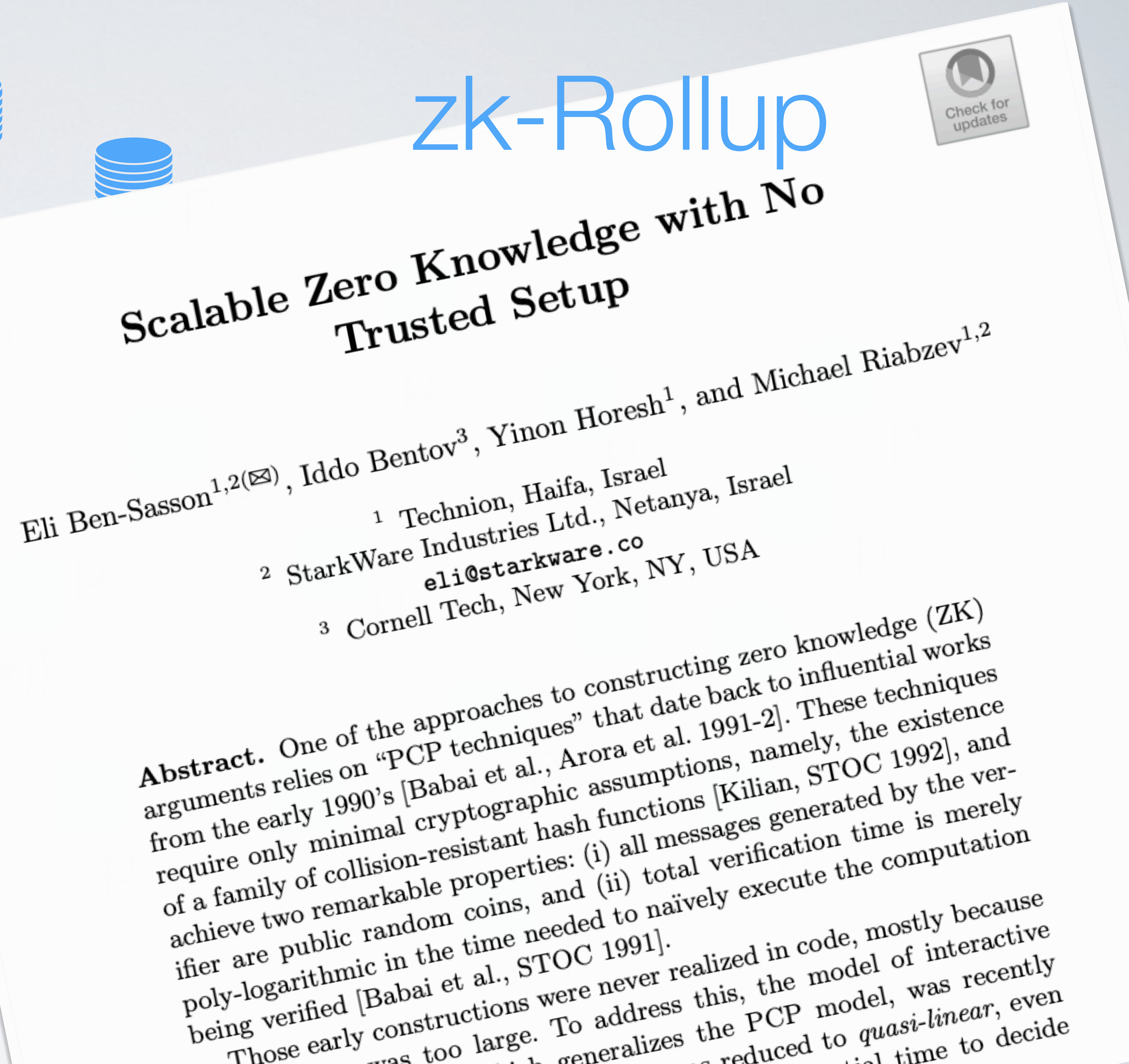


Proof p: {z=method(x)}

method(x)

zk-Rollup





Scalable Zero Knowledge with No Trusted Setup

Eli Ben-Sasson[1,2](✉), Iddo Bentov[3], Yinon Horesh[1], and Michael Riabzev[1,2]

[1] Technion, Haifa, Israel

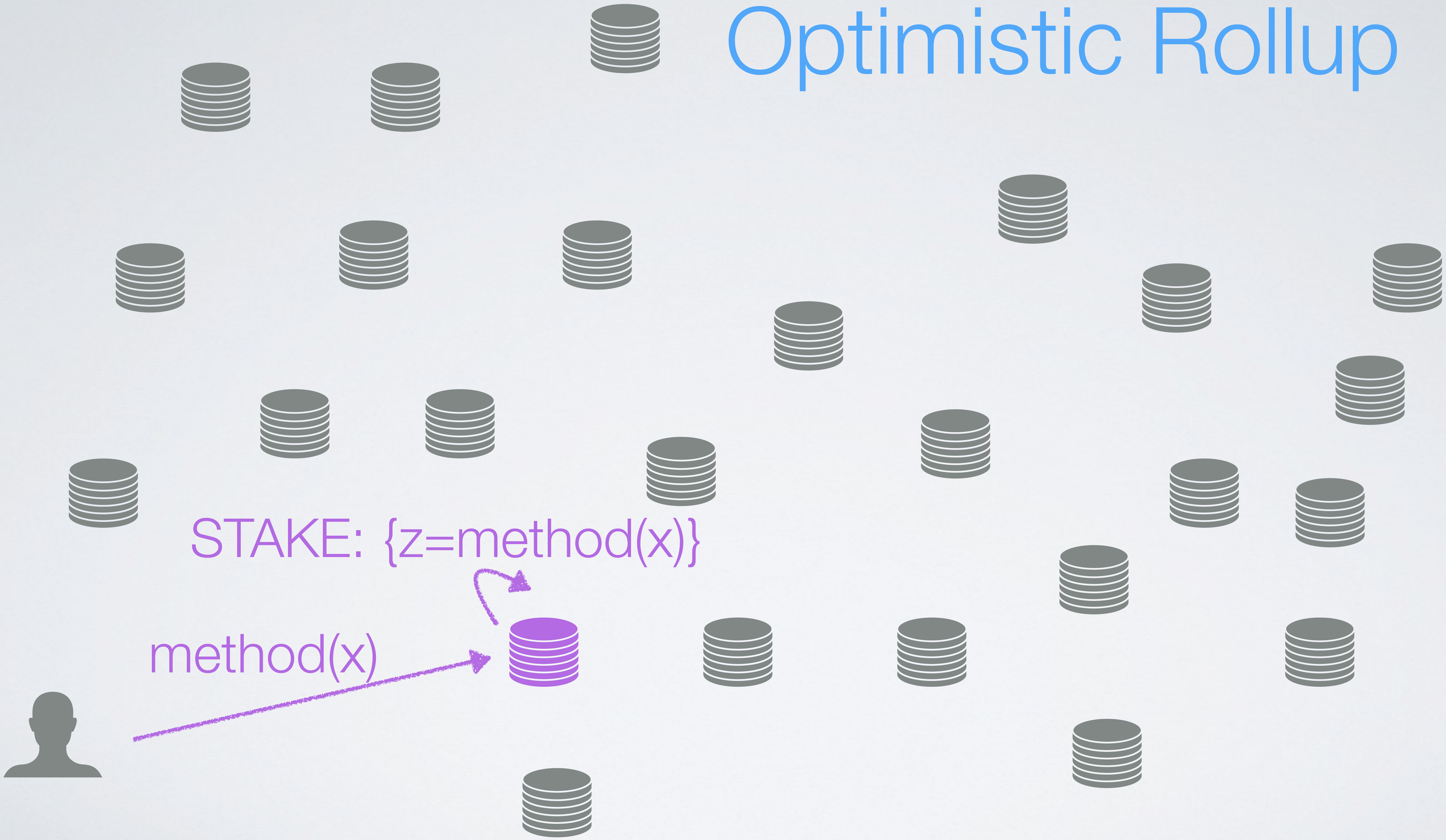
[2] StarkWare Industries Ltd., Netanya, Israel
eli@starkware.co

[3] Cornell Tech, New York, NY, USA

Abstract. One of the approaches to constructing zero knowledge (ZK) arguments relies on "PCP techniques" that date back to influential works from the early 1990's [Babai et al., Arora et al. 1991-2]. These techniques require only minimal cryptographic assumptions, namely, the existence of a family of collision-resistant hash functions [Kilian, STOC 1992], and achieve two remarkable properties: (i) all messages generated by the verifier are public random coins, and (ii) total verification time is merely poly-logarithmic in the time needed to naïvely execute the computation being verified [Babai et al., STOC 1991].

Those early constructions were never realized in code, mostly because
was too large. To address this, the model of interactive
generalizes the PCP model, was recently
reduced to *quasi-linear*, even
time to decide

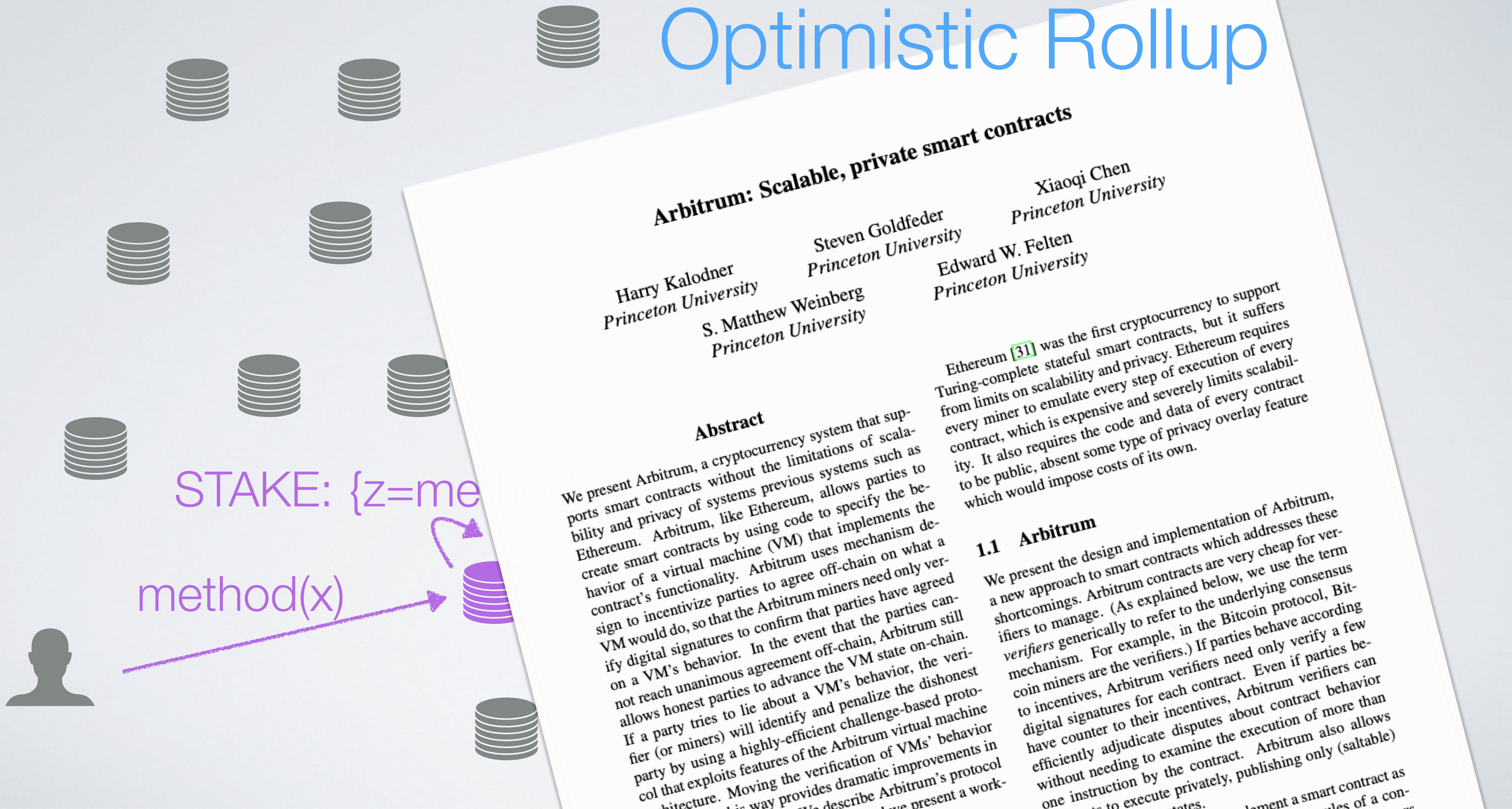
Optimistic Rollup



STAKE: {z=method(x)}

method(x)

Optimistic Rollup



Arbitrum: Scalable, private smart contracts

Harry Kalodner
Princeton University

Steven Goldfeder
Princeton University

Xiaoqi Chen
Princeton University

S. Matthew Weinberg
Princeton University

Edward W. Felten
Princeton University

Abstract

We present Arbitrum, a cryptocurrency system that supports smart contracts without the limitations of scalability and privacy of systems previous systems such as Ethereum. Arbitrum, like Ethereum, allows parties to create smart contracts by using code to specify the behavior of a virtual machine (VM) that implements the contract's functionality. Arbitrum uses mechanism design to incentivize parties to agree off-chain on what a VM would do, so that the Arbitrum miners need only verify digital signatures to confirm that parties have agreed on a VM's behavior. In the event that the parties cannot reach unanimous agreement off-chain, Arbitrum still allows honest parties to advance the VM state on-chain. If a party tries to lie about a VM's behavior, the verifier (or miners) will identify and penalize the dishonest party by using a highly-efficient challenge-based protocol that exploits features of the Arbitrum virtual machine hitecture. Moving the verification of VMs' behavior his way provides dramatic improvements in We describe Arbitrum's protocol we present a work-

Ethereum [31] was the first cryptocurrency to support Turing-complete stateful smart contracts, but it suffers from limits on scalability and privacy. Ethereum requires every miner to emulate every step of execution of every contract, which is expensive and severely limits scalability. It also requires the code and data of every contract to be public, absent some type of privacy overlay feature which would impose costs of its own.

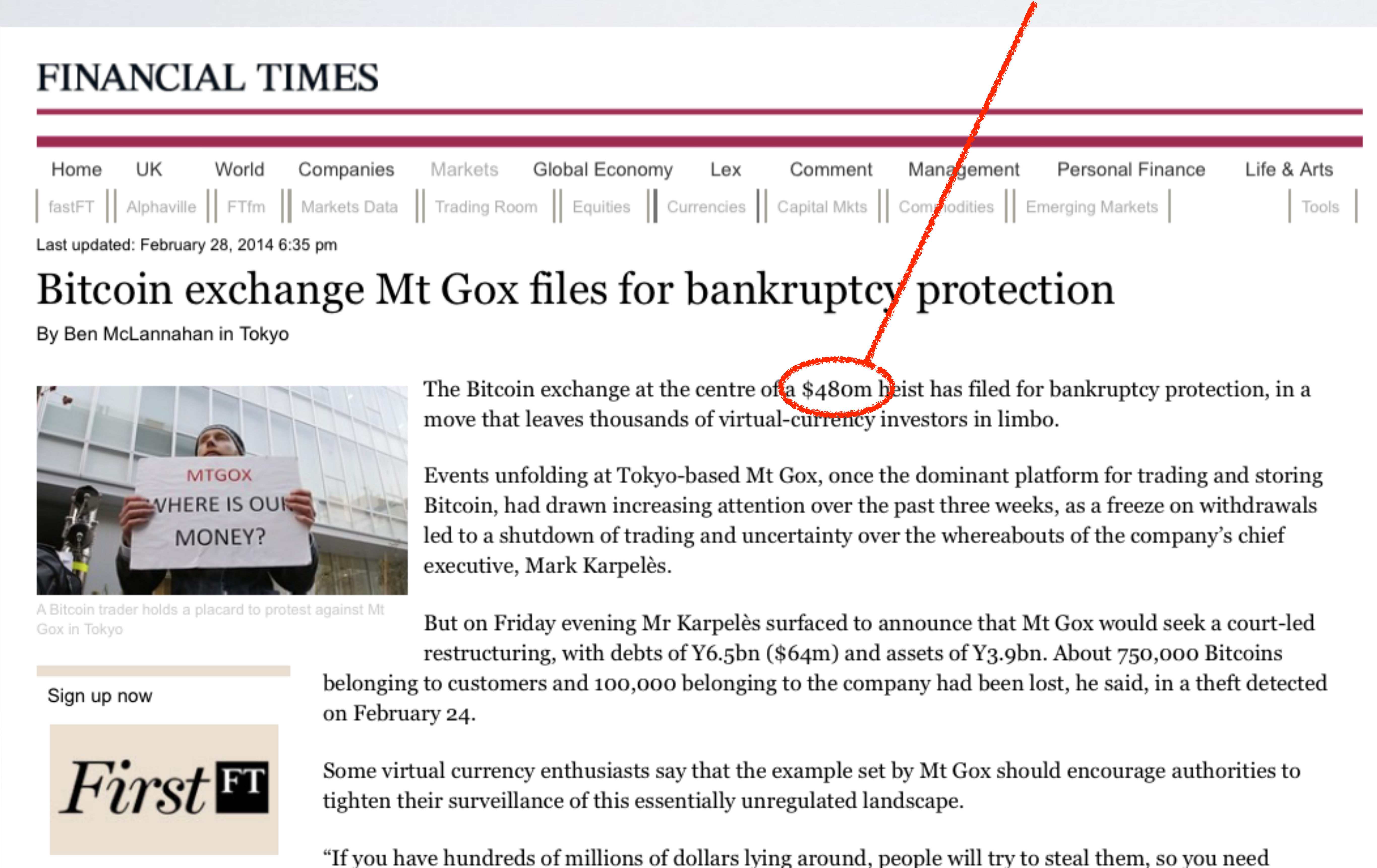
1.1 Arbitrum

We present the design and implementation of Arbitrum, a new approach to smart contracts which addresses these shortcomings. Arbitrum contracts are very cheap for verifiers to manage. (As explained below, we use the term *verifiers* generically to refer to the underlying consensus mechanism. For example, in the Bitcoin protocol, Bitcoin miners are the verifiers.) If parties behave according to incentives, Arbitrum verifiers need only verify a few digital signatures for each contract. Even if parties behave counter to their incentives, Arbitrum verifiers can efficiently adjudicate disputes about contract behavior without needing to examine the execution of more than one instruction by the contract. Arbitrum also allows ts to execute privately, publishing only (saltable) tates.

lement a smart contract as les of a con-

Proof of Solvency

$480,000,000


FINANCIAL TIMES
Home UK World Companies Markets Global Economy Lex Comment Management Personal Finance Life & Arts
fastFT Alphaville FTfm Markets Data Trading Room Equities Currencies Capital Mkts Commodities Emerging Markets Tools
MTGOX
WHERE IS OUR
MONEY?
Sign up now
First FT

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.

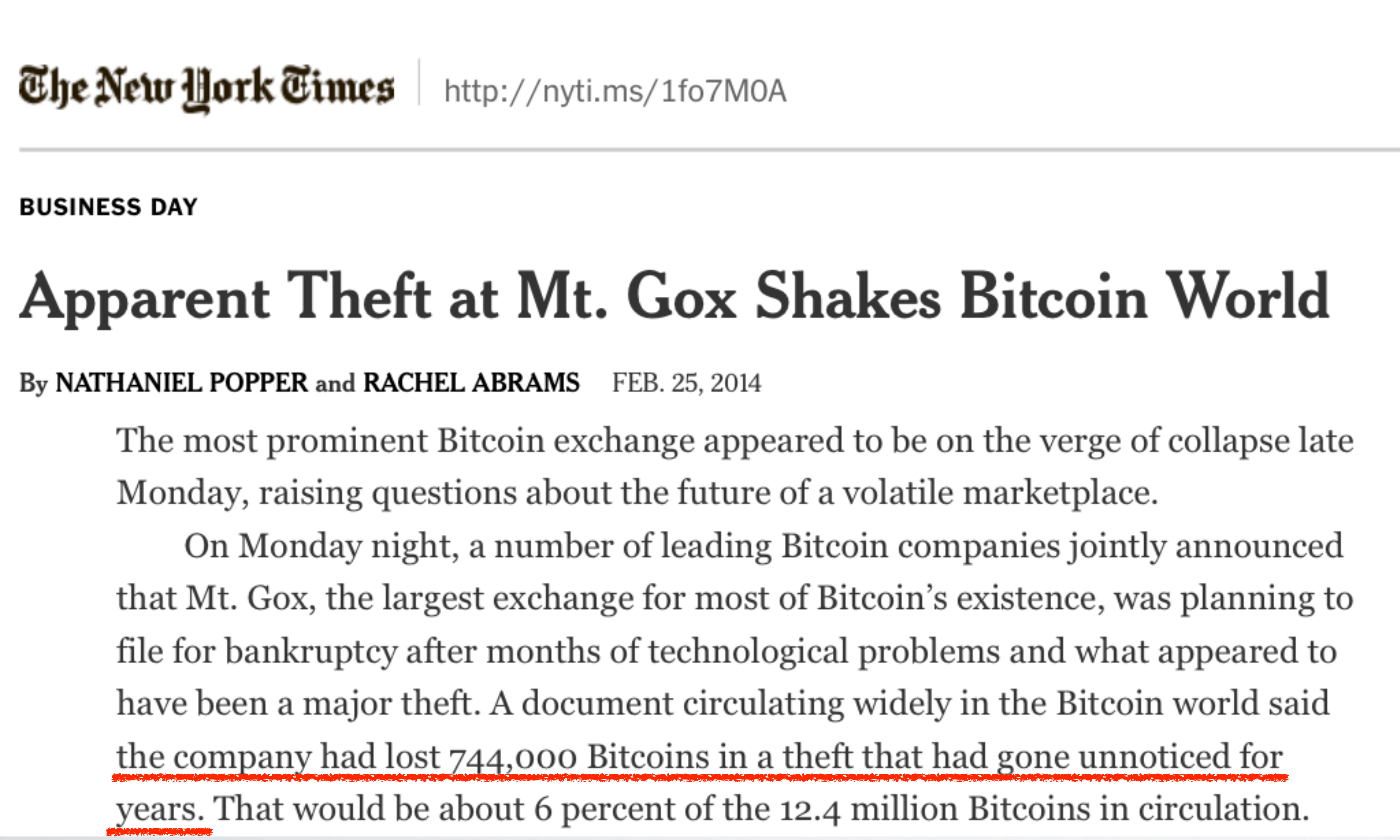
But on Friday evening Mr Karpelès surfaced to announce that Mt Gox would seek a court-led restructuring, with debts of Y6.5bn ($64m) and assets of Y3.9bn. About 750,000 Bitcoins belonging to customers and 100,000 belonging to the company had been lost, he said, in a theft detected on February 24.

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

"If you have hundreds of millions of dollars lying around, people will try to steal them, so you need

Proof of Solvency

Theft Unnoticed for Years



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

BUSINESS DAY

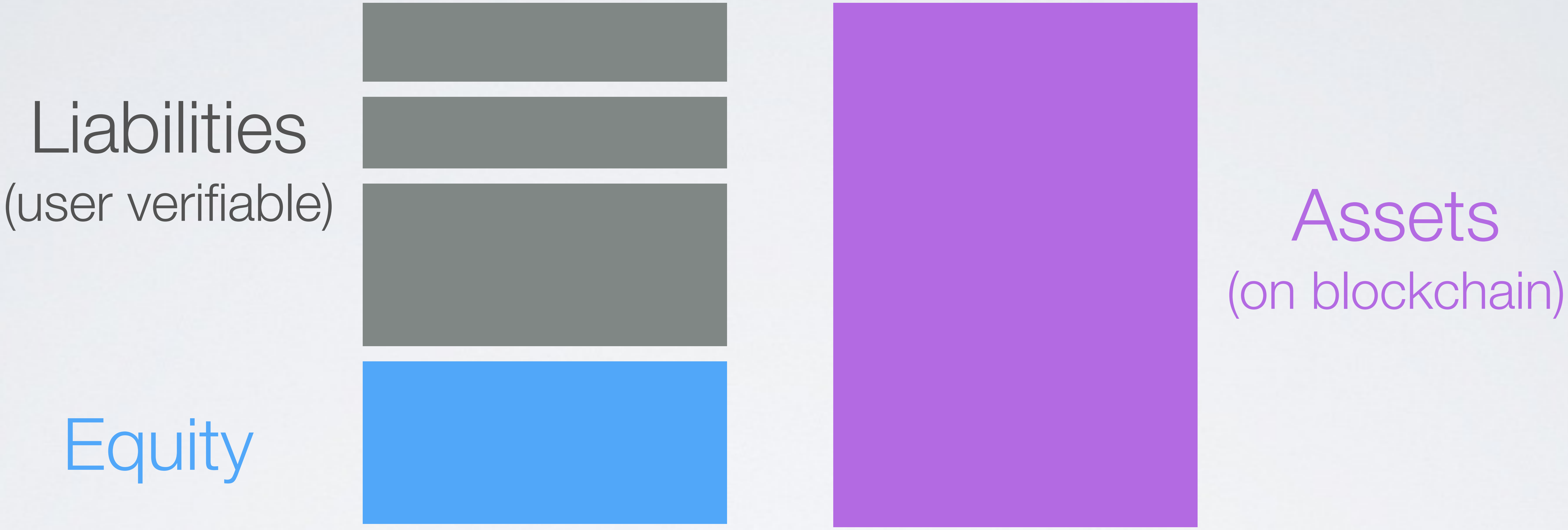
Apparent Theft at Mt. Gox Shakes Bitcoin World

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



ZKP: Equity = Assets - Liabilities >= 0

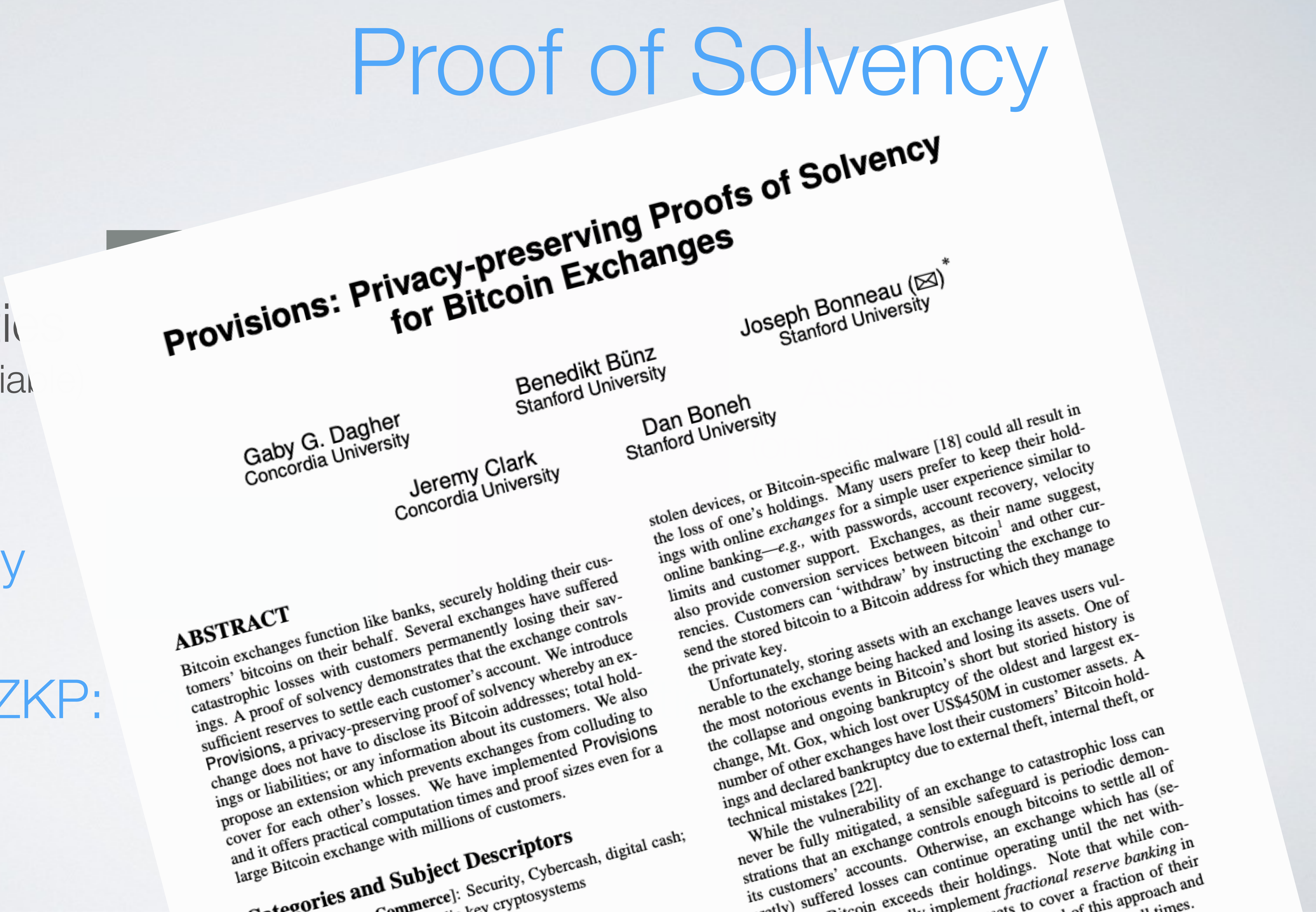
Proof of Solvency

Liabiliti

(user verifia

Equity

ZKP:



Provisions: Privacy-preserving Proofs of Solvency for Bitcoin Exchanges

Gaby G. Dagher
Concordia University

Benedikt Bünz
Stanford University

Joseph Bonneau (✉)*
Stanford University

Jeremy Clark
Concordia University

Dan Boneh
Stanford University

ABSTRACT

Bitcoin exchanges function like banks, securely holding their customers' bitcoins on their behalf. Several exchanges have suffered catastrophic losses with customers permanently losing their savings. A proof of solvency demonstrates that the exchange controls sufficient reserves to settle each customer's account. We introduce Provisions, a privacy-preserving proof of solvency whereby an exchange does not have to disclose its Bitcoin addresses; total holdings or liabilities; or any information about its customers. We also propose an extension which prevents exchanges from colluding to cover for each other's losses. We have implemented Provisions and it offers practical computation times and proof sizes even for a large Bitcoin exchange with millions of customers.

ategories and Subject Descriptors

Commerce]: Security, Cybercash, digital cash;
ic key cryptosystems

stolen devices, or Bitcoin-specific malware [18] could all result in the loss of one's holdings. Many users prefer to keep their holdings with online *exchanges* for a simple user experience similar to online banking—*e.g.*, with passwords, account recovery, velocity limits and customer support. Exchanges, as their name suggest, also provide conversion services between bitcoin[1] and other currencies. Customers can 'withdraw' by instructing the exchange to send the stored bitcoin to a Bitcoin address for which they manage the private key.

Unfortunately, storing assets with an exchange leaves users vulnerable to the exchange being hacked and losing its assets. One of the most notorious events in Bitcoin's short but storied history is the collapse and ongoing bankruptcy of the oldest and largest exchange, Mt. Gox, which lost over US$450M in customer assets. A number of other exchanges have lost their customers' Bitcoin holdings and declared bankruptcy due to external theft, internal theft, or technical mistakes [22].

While the vulnerability of an exchange to catastrophic loss can never be fully mitigated, a sensible safeguard is periodic demonstrations that an exchange controls enough bitcoins to settle all of its customers' accounts. Otherwise, an exchange which has (secretly) suffered losses can continue operating until the net with- Bitcoin exceeds their holdings. Note that while con- lly implement *fractional reserve banking* in ets to cover a fraction of their l of this approach and ll times.

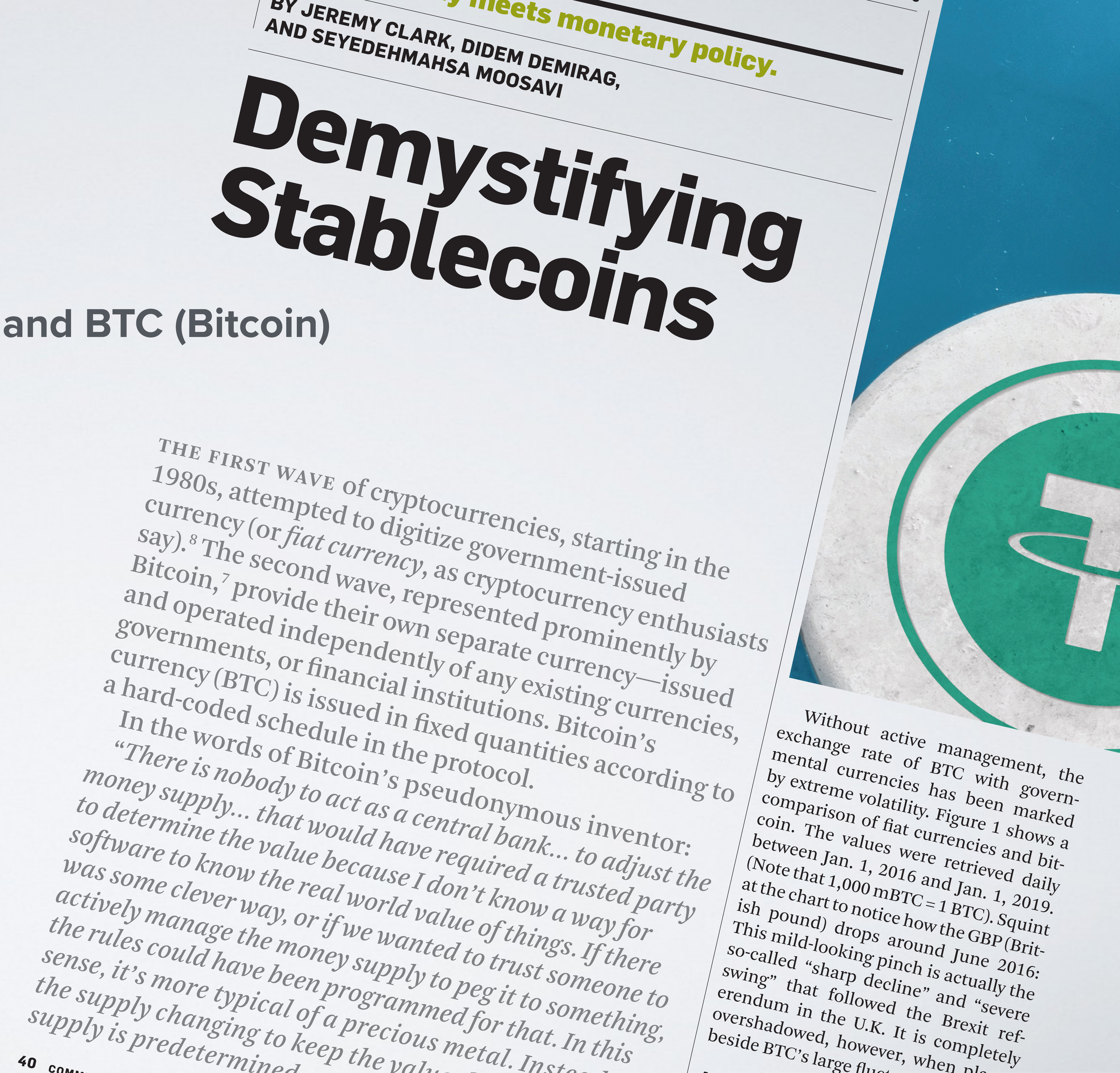
Decentralized Finance (DeFi)

- You code your financial service and push it to a public blockchain like Ethereum
- The Ethereum's global network of servers runs your code for you
- While it is slow and can only run (relatively) simple code, it will run exactly as coded
- Anyone who can code a DApp can make a financial service

- In 2020, decentralized finance (DeFI) services hold $10B USD on Ethereum

Stablecoins

- Cryptocurrencies like ETH (Ether) and BTC (Bitcoin)
- Stablecoins like USDT or Dai



y meets monetary policy.

BY JEREMY CLARK, DIDEM DEMIRAG,
AND SEYEDEHMAHSA MOOSAVI

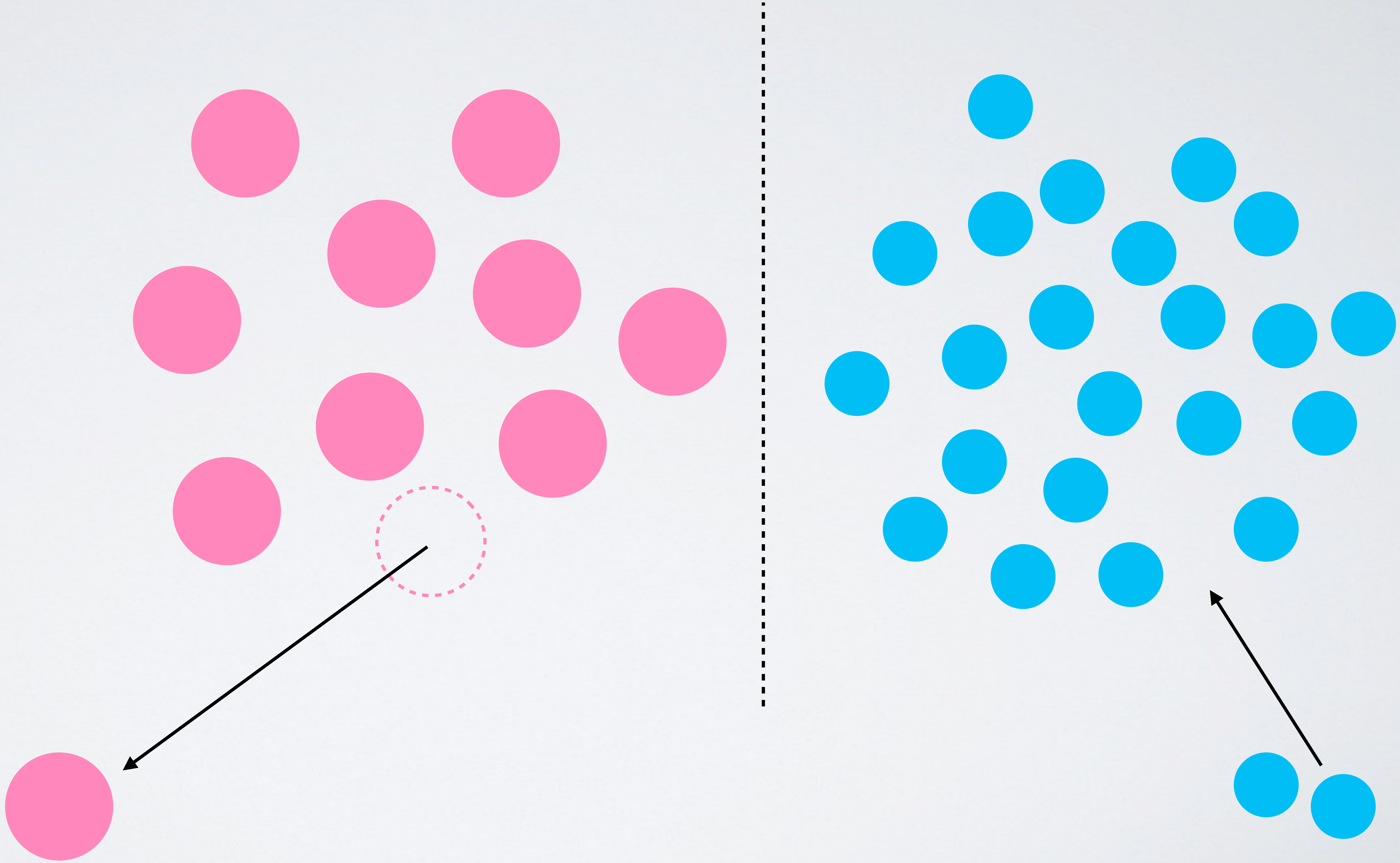
Demystifying Stablecoins

THE FIRST WAVE of cryptocurrencies, starting in the 1980s, attempted to digitize government-issued currency (or *fiat currency*, as cryptocurrency enthusiasts say).[8] The second wave, represented prominently by Bitcoin,[7] provide their own separate currency—issued and operated independently of any existing currencies, governments, or financial institutions. Bitcoin's currency (BTC) is issued in fixed quantities according to a hard-coded schedule in the protocol.

In the words of Bitcoin's pseudonymous inventor: *"There is nobody to act as a central bank… to adjust the money supply… that would have required a trusted party to determine the value because I don't know a way for software to know the real world value of things. If there was some clever way, or if we wanted to trust someone to actively manage the money supply to peg it to something, the rules could have been programmed for that. In this sense, it's more typical of a precious metal. Instea the supply changing to keep the valu supply is predetermined*

Without active management, the exchange rate of BTC with governmental currencies has been marked by extreme volatility. Figure 1 shows a comparison of fiat currencies and bitcoin. The values were retrieved daily between Jan. 1, 2016 and Jan. 1, 2019. (Note that 1,000 mBTC = 1 BTC). Squint at the chart to notice how the GBP (British pound) drops around June 2016: This mild-looking pinch is actually the so-called "sharp decline" and "severe swing" that followed the Brexit referendum in the U.K. It is completely overshadowed, however, when pla beside BTC's large fluct

Exchanges



Lending

- Margin trading
- Borrowing one kind of asset by collateralizing a different kind
- Flash loans

Flash Loans

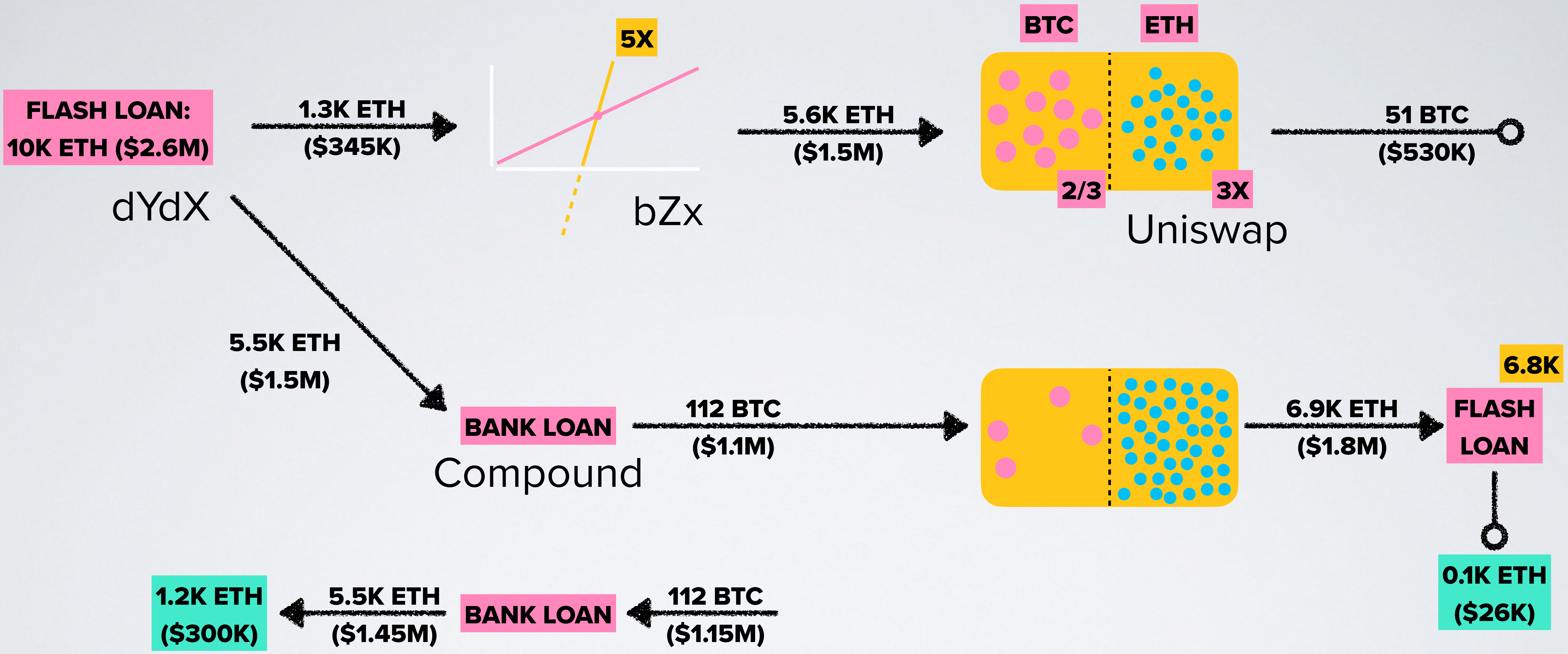
```
{

  TRANSACTION:

    BORROW XXX ETH
    DO WHATEVER YOU WANT
    REPAY XXX ETH
    REPAY COMPLETE? => REVERT IF FAIL

}
```

- Not possible in the real world!
- One transaction runs at a time
- No risk, no collateral, anonymous, borrow maximum amount available (no one can use it while your transaction is running)



FLASH LOAN:
10K ETH ($2.6M)

dYdX

1.3K ETH
($345K)

5X

bZx

5.6K ETH
($1.5M)

BTC

ETH

2/3

3X

Uniswap

51 BTC
($530K)

5.5K ETH
($1.5M)

BANK LOAN

Compound

112 BTC
($1.1M)

6.8K

6.9K ETH
($1.8M)

FLASH
LOAN

0.1K ETH
($26K)

1.2K ETH
($300K)

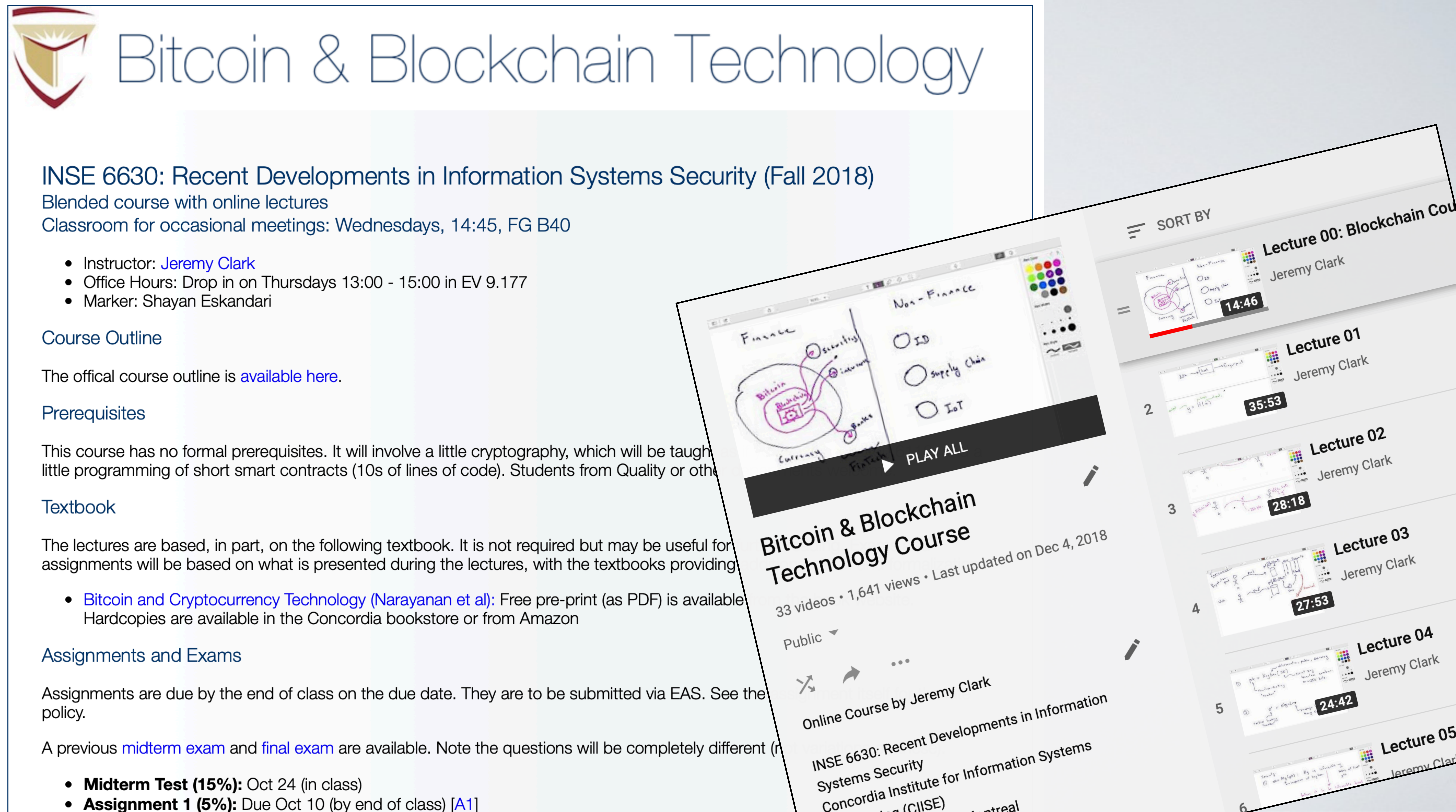
5.5K ETH
($1.45M)

BANK LOAN

112 BTC
($1.15M)

FEES: 0.5 ETH ($135)

More resources



Bitcoin & Blockchain Technology

INSE 6630: Recent Developments in Information Systems Security (Fall 2018)

Blended course with online lectures

Classroom for occasional meetings: Wednesdays, 14:45, FG B40

- Instructor: Jeremy Clark
- Office Hours: Drop in on Thursdays 13:00 - 15:00 in EV 9.177
- Marker: Shayan Eskandari

Course Outline

The offical course outline is available here.

Prerequisites

This course has no formal prerequisites. It will involve a little cryptography, which will be taugh
little programming of short smart contracts (10s of lines of code). Students from Quality or othe

Textbook

The lectures are based, in part, on the following textbook. It is not required but may be useful for
assignments will be based on what is presented during the lectures, with the textbooks providing

- Bitcoin and Cryptocurrency Technology (Narayanan et al): Free pre-print (as PDF) is available
Hardcopies are available in the Concordia bookstore or from Amazon

Assignments and Exams

Assignments are due by the end of class on the due date. They are to be submitted via EAS. See the
policy.

A previous midterm exam and final exam are available. Note the questions will be completely different (r

- **Midterm Test (15%):** Oct 24 (in class)
- **Assignment 1 (5%):** Due Oct 10 (by end of class) [A1]

Bitcoin & Blockchain Technology Course

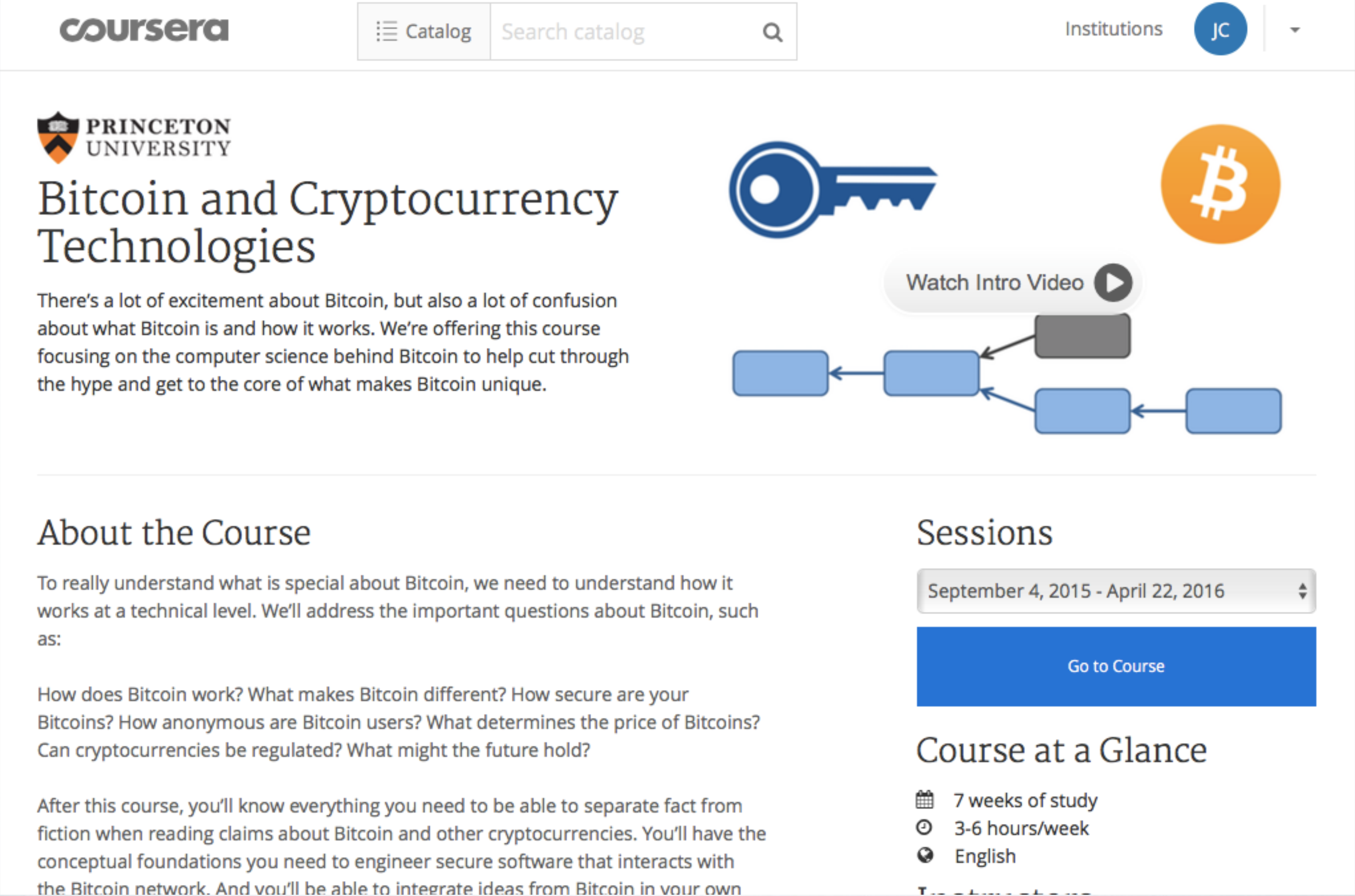
33 videos • 1,641 views • Last updated on Dec 4, 2018

Public

Online Course by Jeremy Clark

INSE 6630: Recent Developments in Information Systems Security
Concordia Institute for Information Systems
[…](CIISE) […]ntreal

	Video	Length
	Lecture 00: Blockchain Cou Jeremy Clark	14:46
2	Lecture 01 Jeremy Clark	35:53
3	Lecture 02 Jeremy Clark	28:18
4	Lecture 03 Jeremy Clark	27:53
5	Lecture 04 Jeremy Clark	24:42
6	Lecture 05 Jeremy Clar	



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

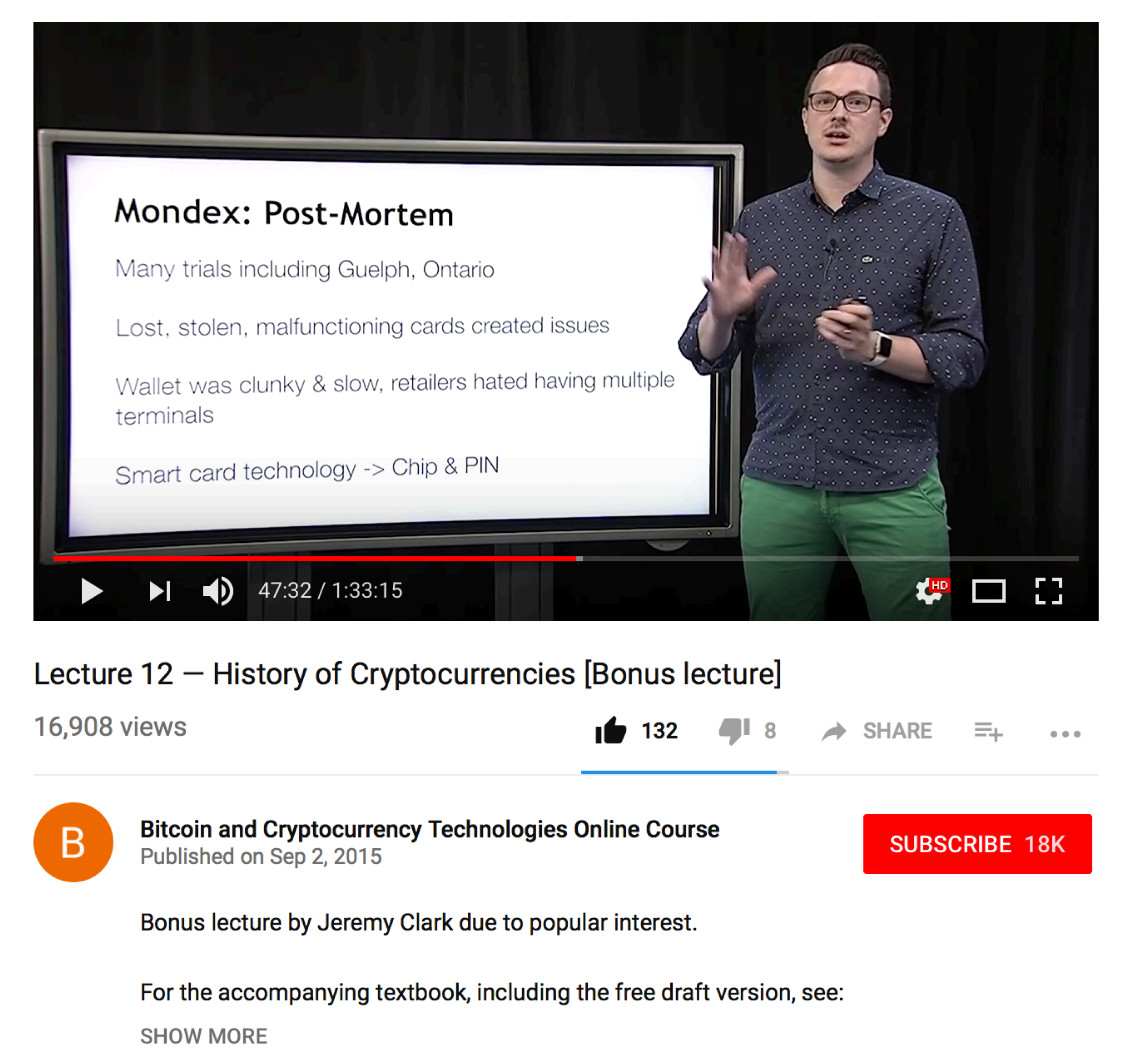
Sessions

September 4, 2015 - April 22, 2016

Course at a Glance

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

Instructors



Mondex: Post-Mortem

Many trials including Guelph, Ontario

Lost, stolen, malfunctioning cards created issues

Wallet was clunky & slow, retailers hated having multiple terminals

Smart card technology -> Chip & PIN

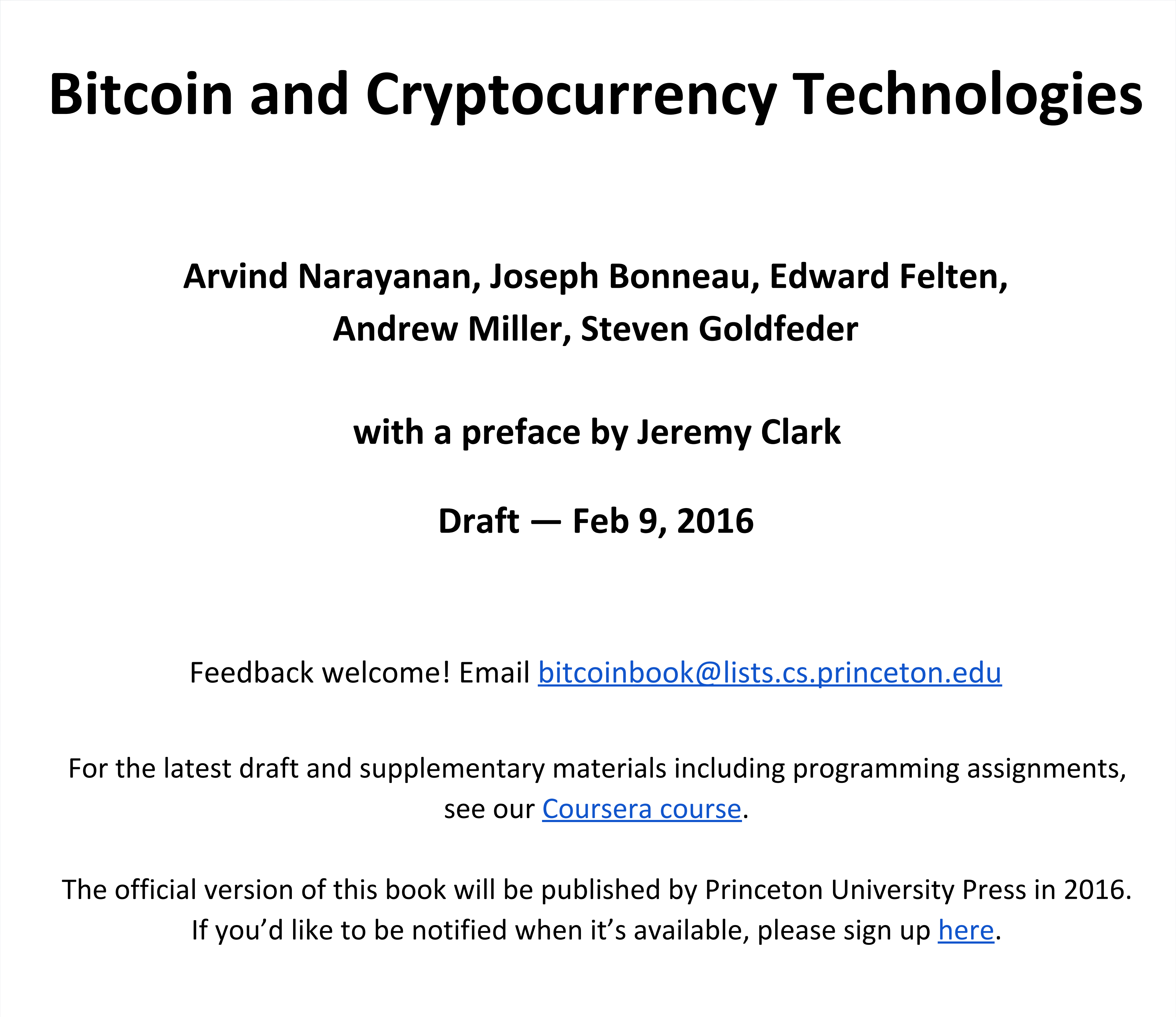
Lecture 12 — History of Cryptocurrencies [Bonus lecture]

16,908 views

Bitcoin and Cryptocurrency Technologies Online Course
Published on Sep 2, 2015

Bonus lecture by Jeremy Clark due to popular interest.

For the accompanying textbook, including the free draft version, see:



Bitcoin and Cryptocurrency Technologies

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

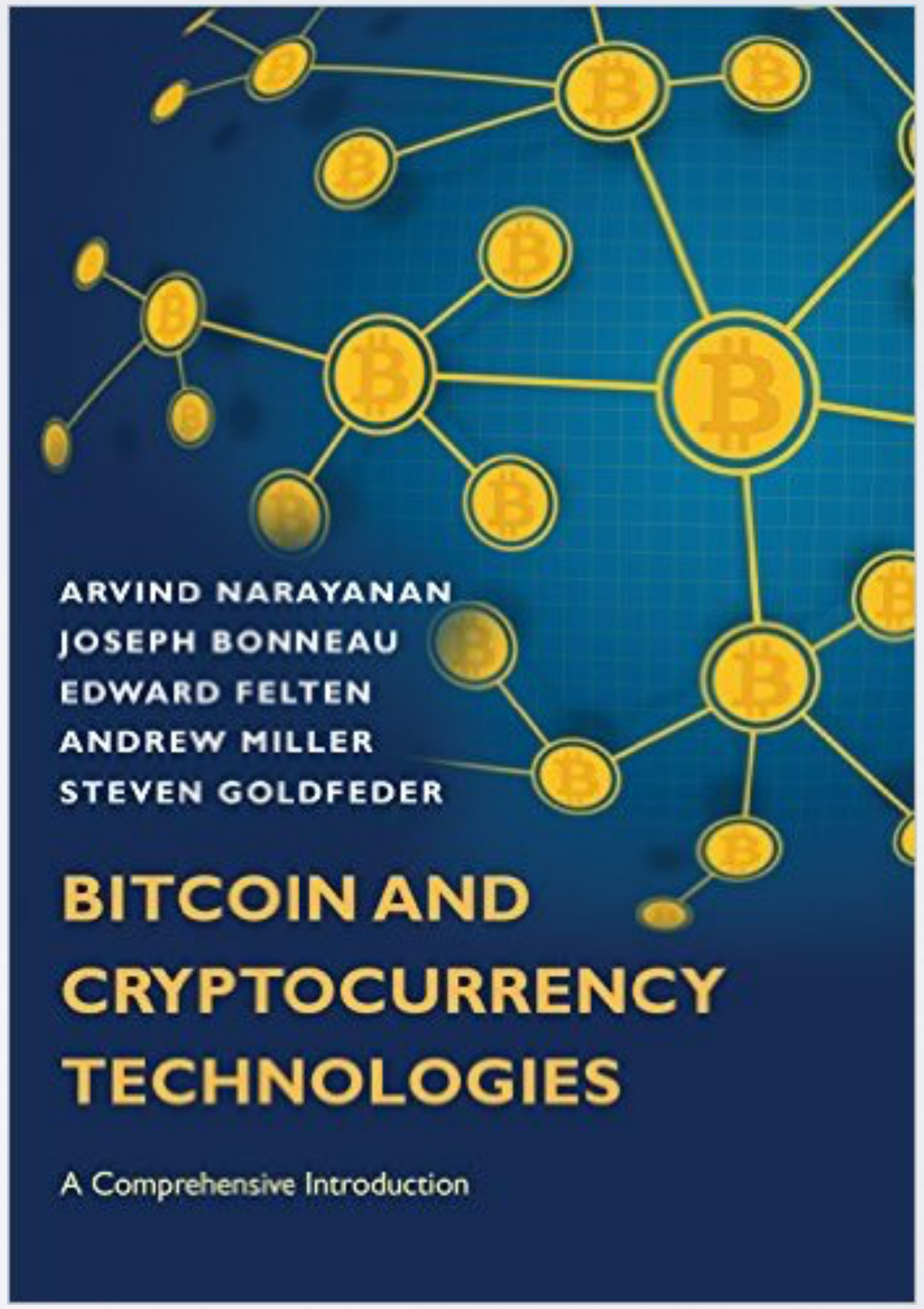
with a preface by Jeremy Clark

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.



ARVIND NARAYANAN
JOSEPH BONNEAU
EDWARD FELTEN
ANDREW MILLER
STEVEN GOLDFEDER

BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES

A Comprehensive Introduction

Q

@PulpSpy

Q

@PulpSpy

Legality and Regulation

- Illicit uses: monitored by law enforcement agency (cybercrimes)
- Taxation: CRA guidelines (capital gain)
- Financial tracking: FINTRAC guidelines (MSB)
- Securities law: AMF guidelines and sandbox
- Accounting standards: No IFRS standards yet (convention: intangible asset)