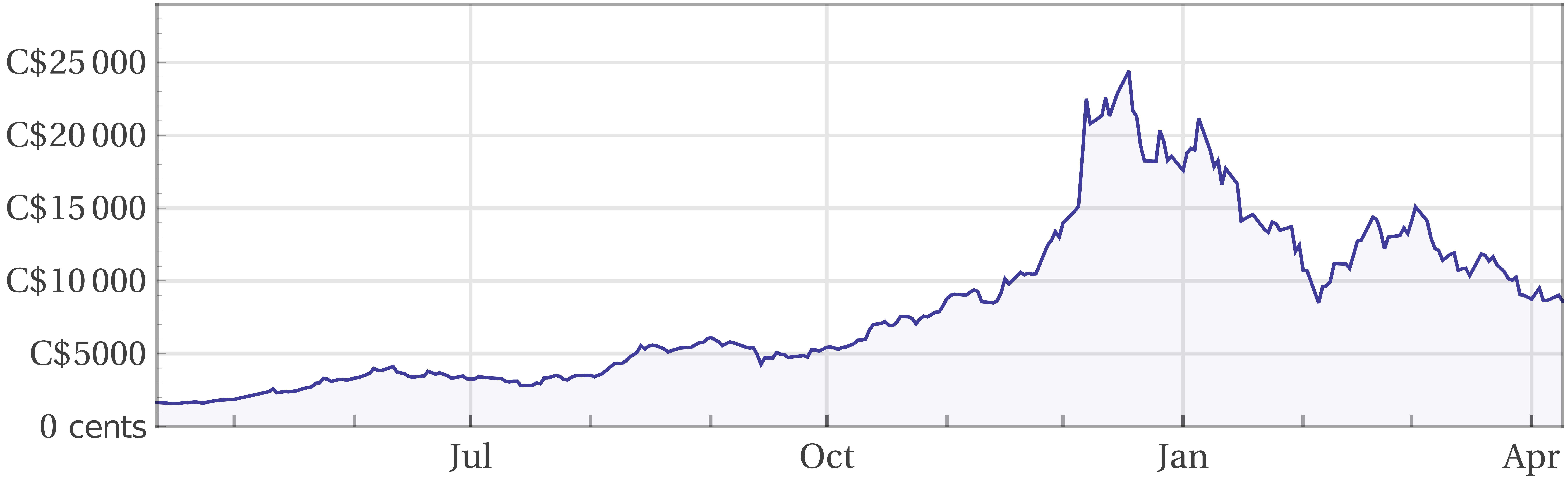
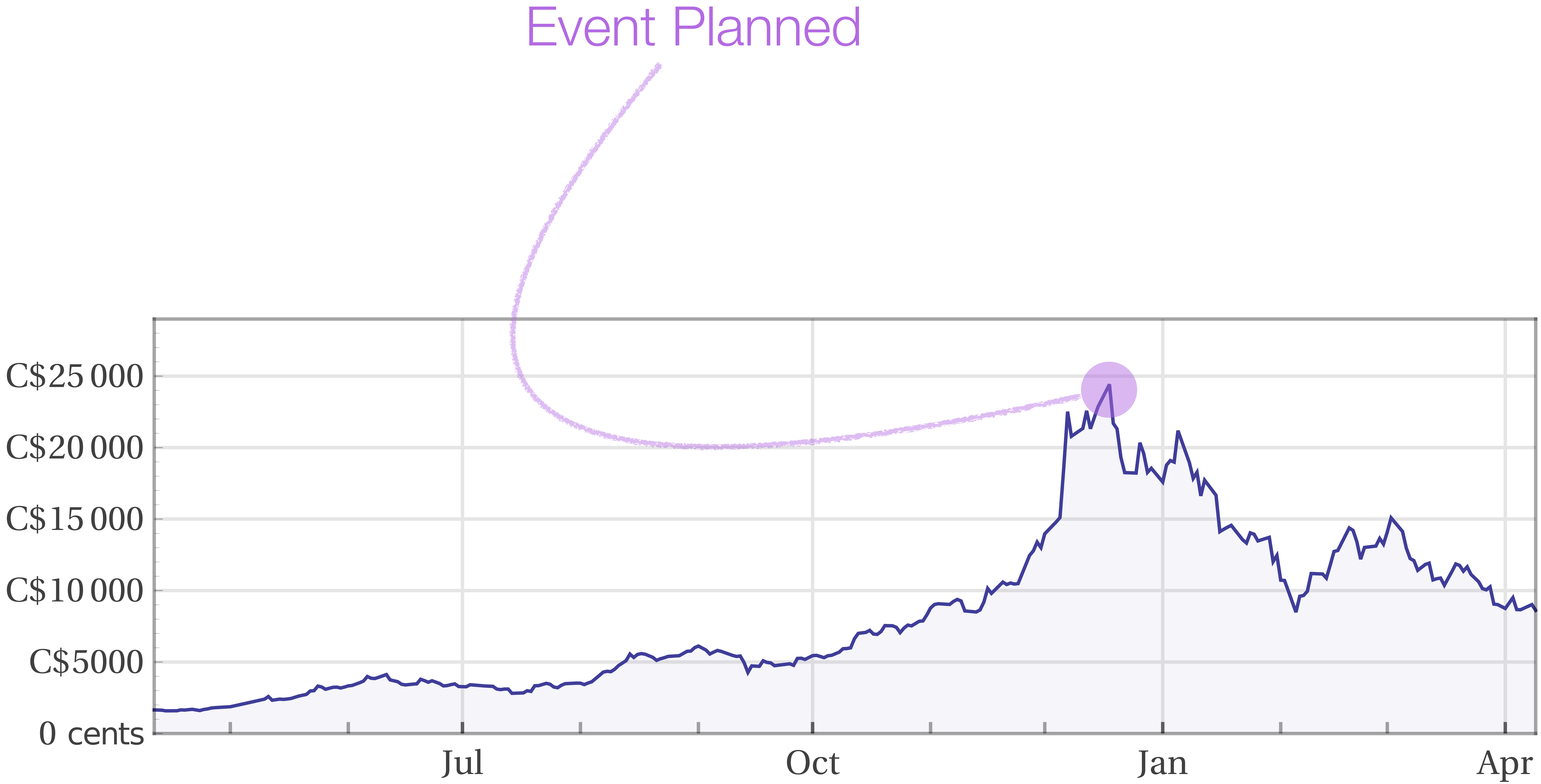
Bitcoin & Blockchain
A Quick Primer

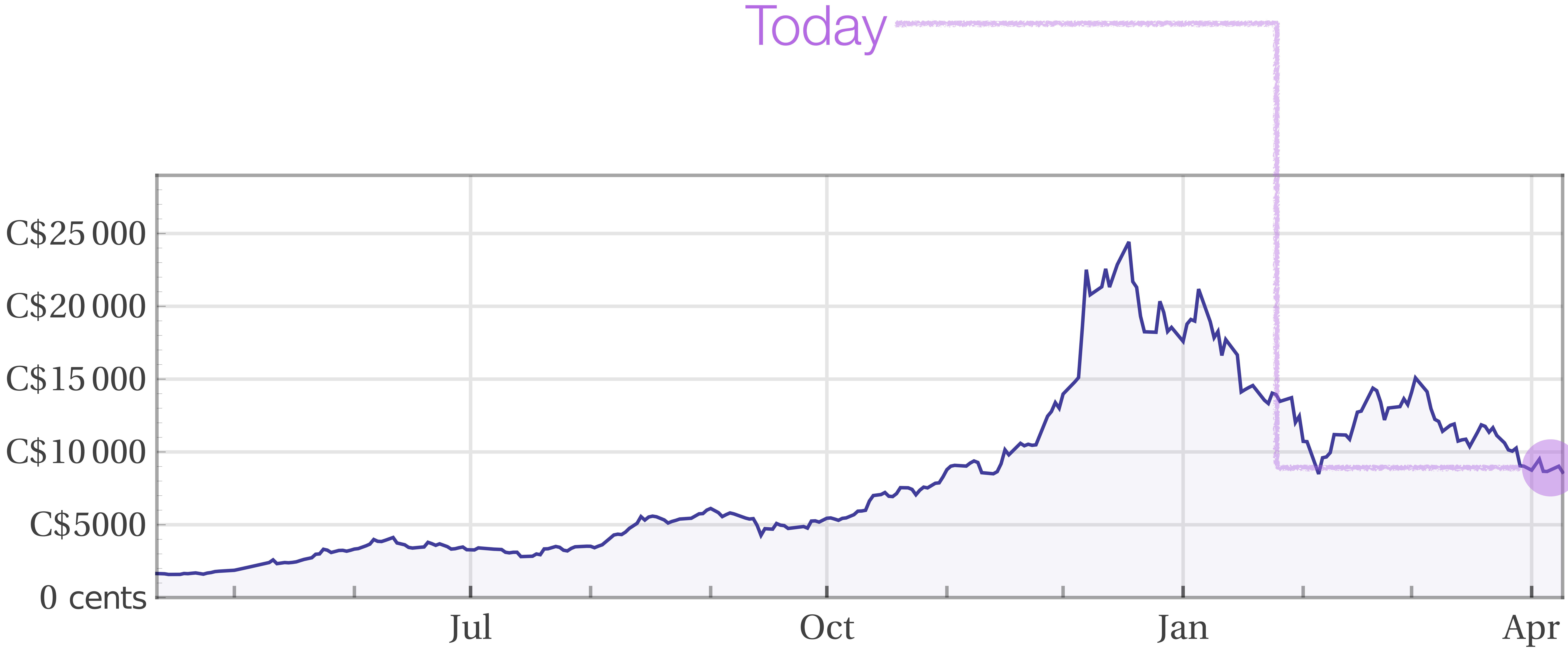
Jeremy Clark

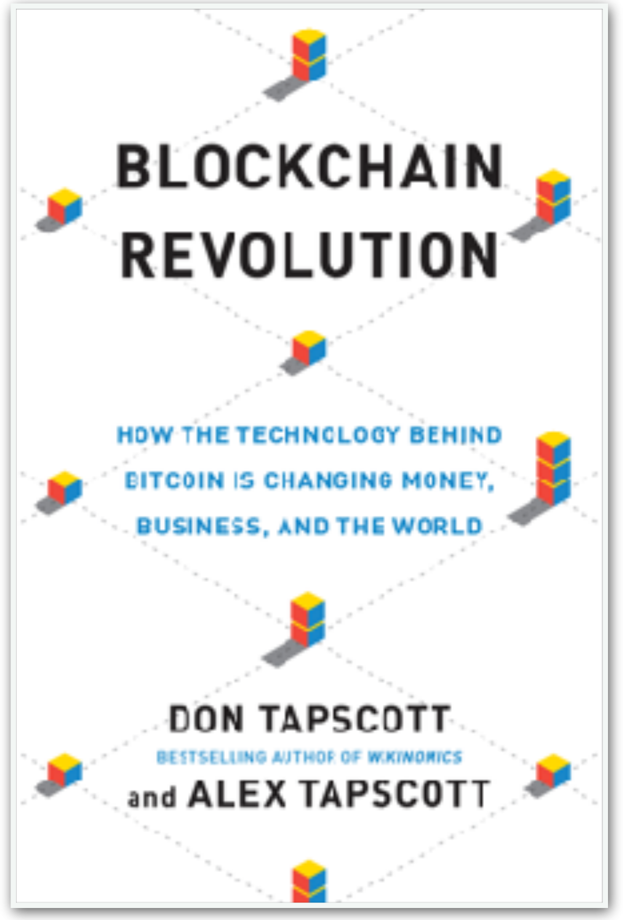
CONCORDIA


C$25 000
C$20 000
C$15 000
C$10 000
C$5000
0 cents
Jul
Oct
Jan
Apr



Event Planned
C$25 000
C$20 000
C$15 000
C$10 000
C$5000
0 cents
Jul
Oct
Jan
Apr


Today
C$25 000
C$20 000
C$15 000
C$10 000
C$5000
0 cents
Jul
Oct
Jan
Apr



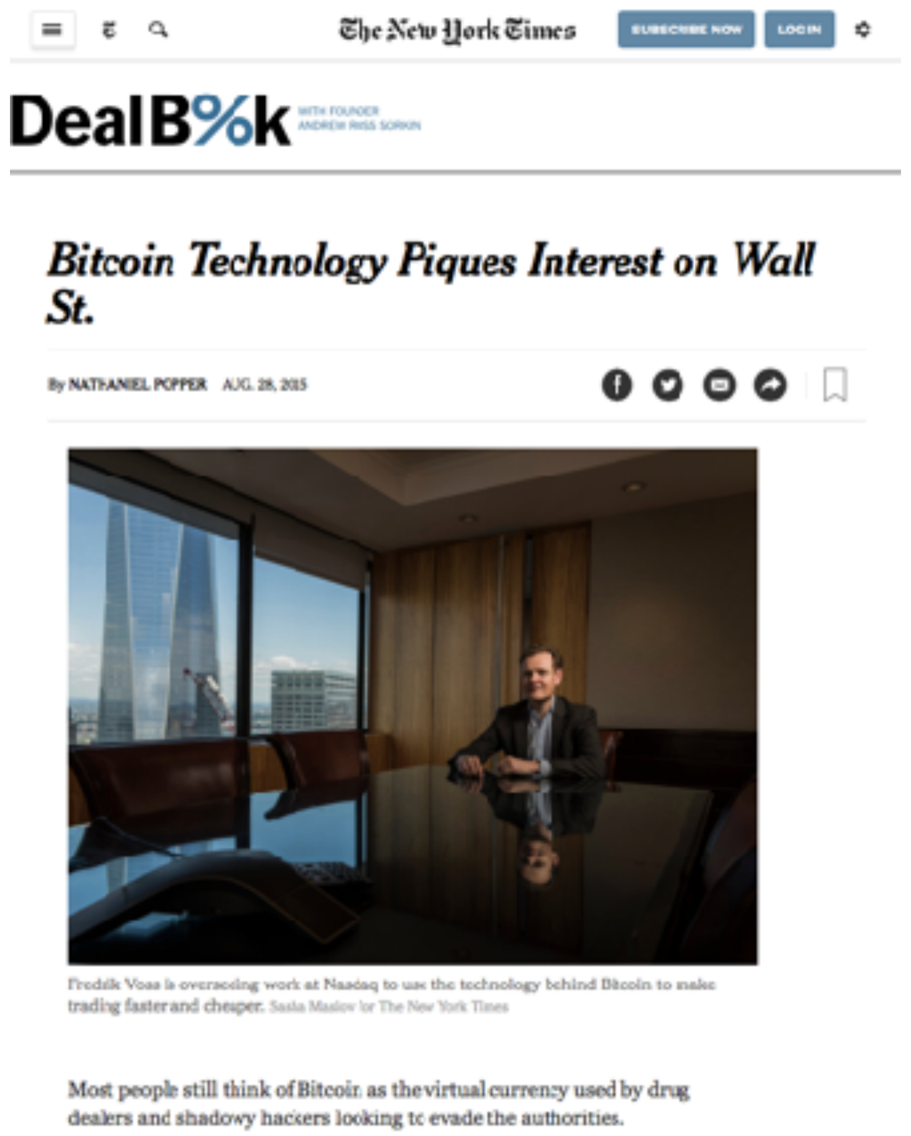
BLOCKCHAIN REVOLUTION

HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD

DON TAPSCOTT

BESTSELLING AUTHOR OF WIKINOMICS

and ALEX TAPSCOTT

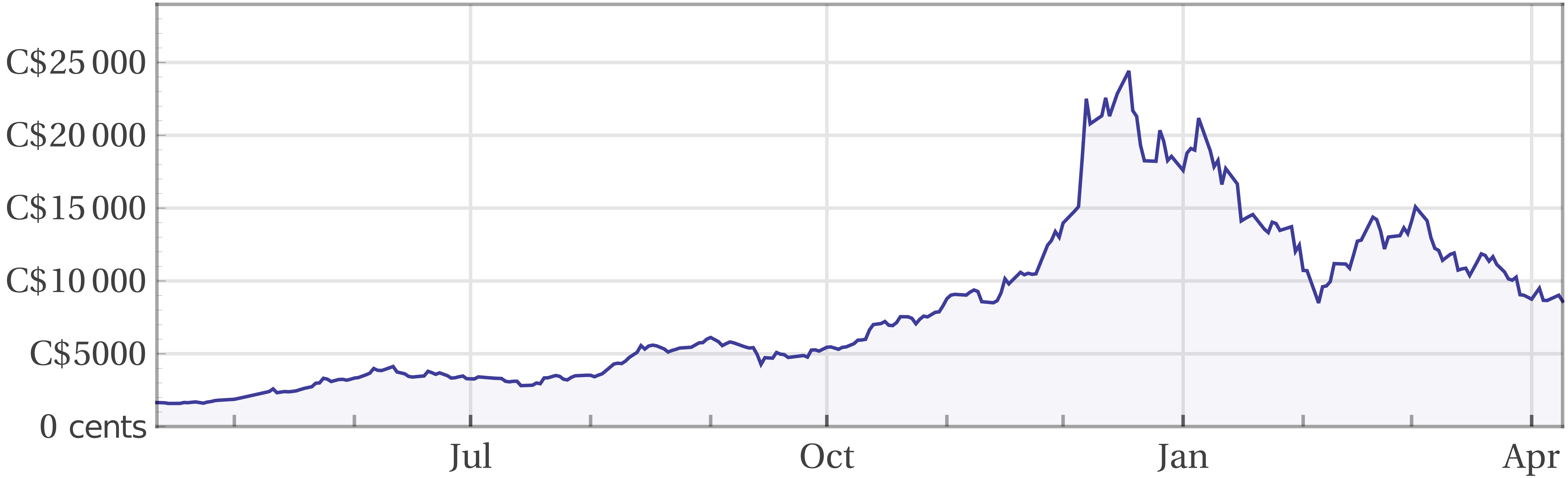


Bitcoin Technology Piques Interest on Wall St.

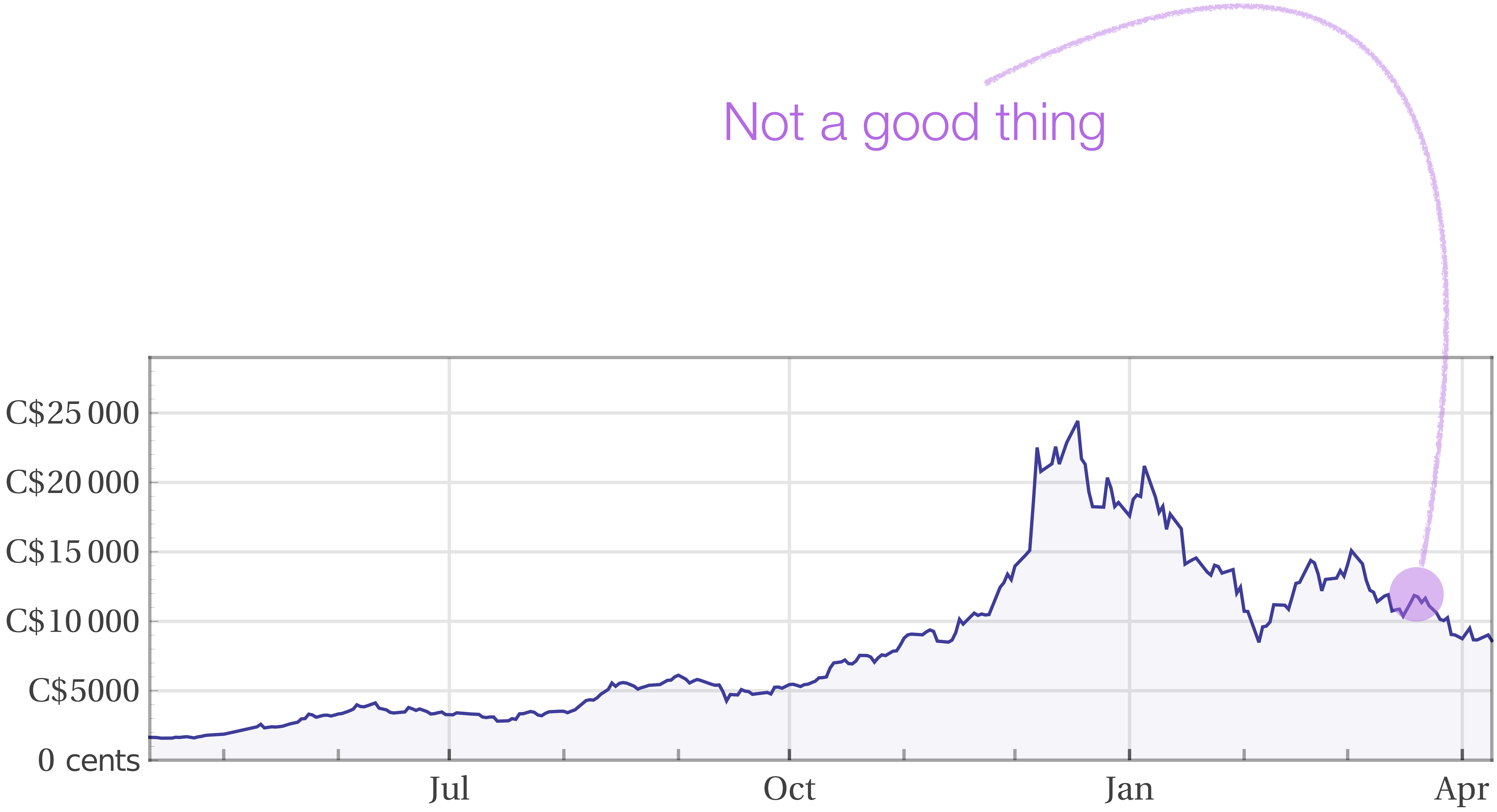
By NATHANIEL POPPER AUG. 28, 2015

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

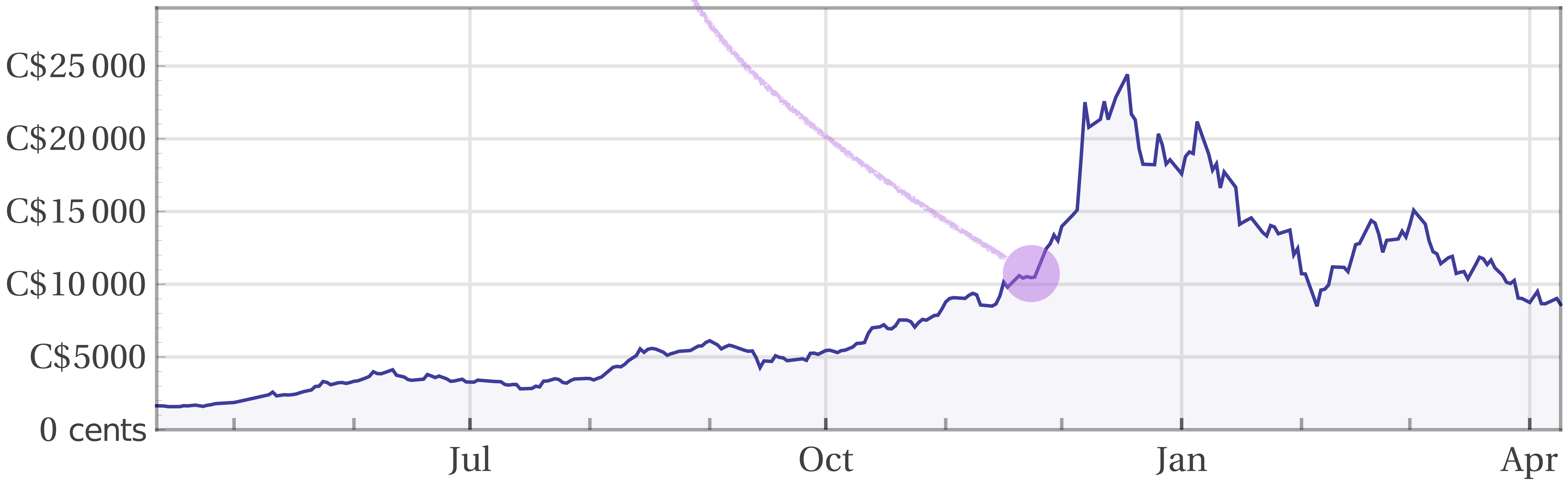
Most people still think of Bitcoin as the virtual currency used by drug dealers and shadowy hackers looking to evade the authorities.



Not a good thing



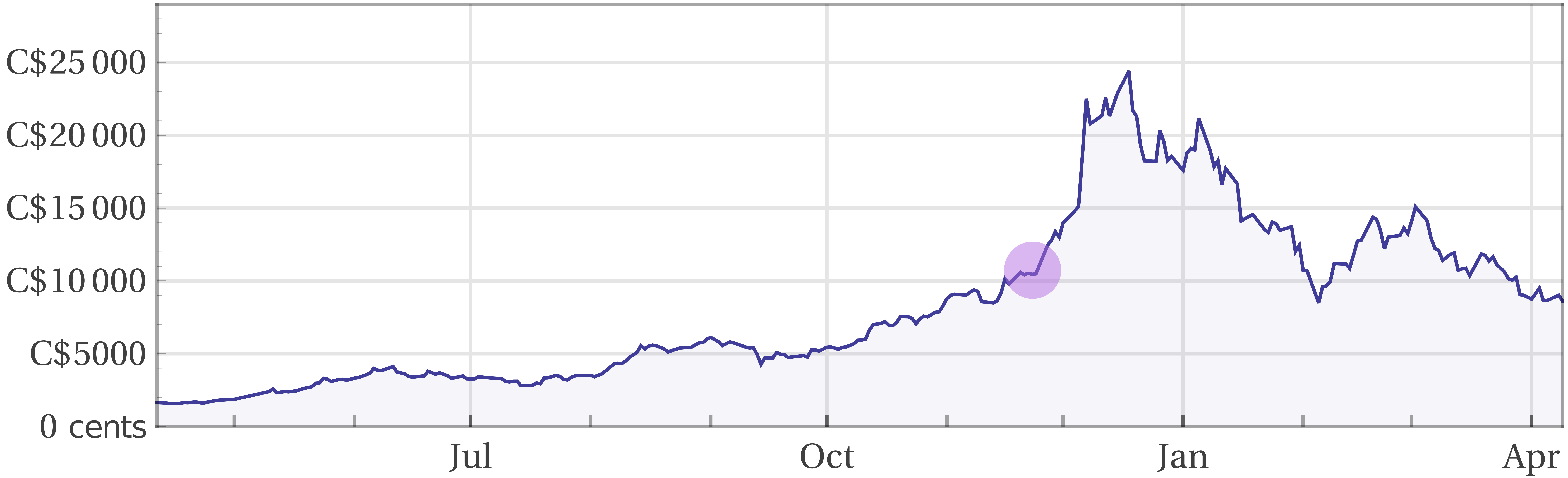
Not a good thing either



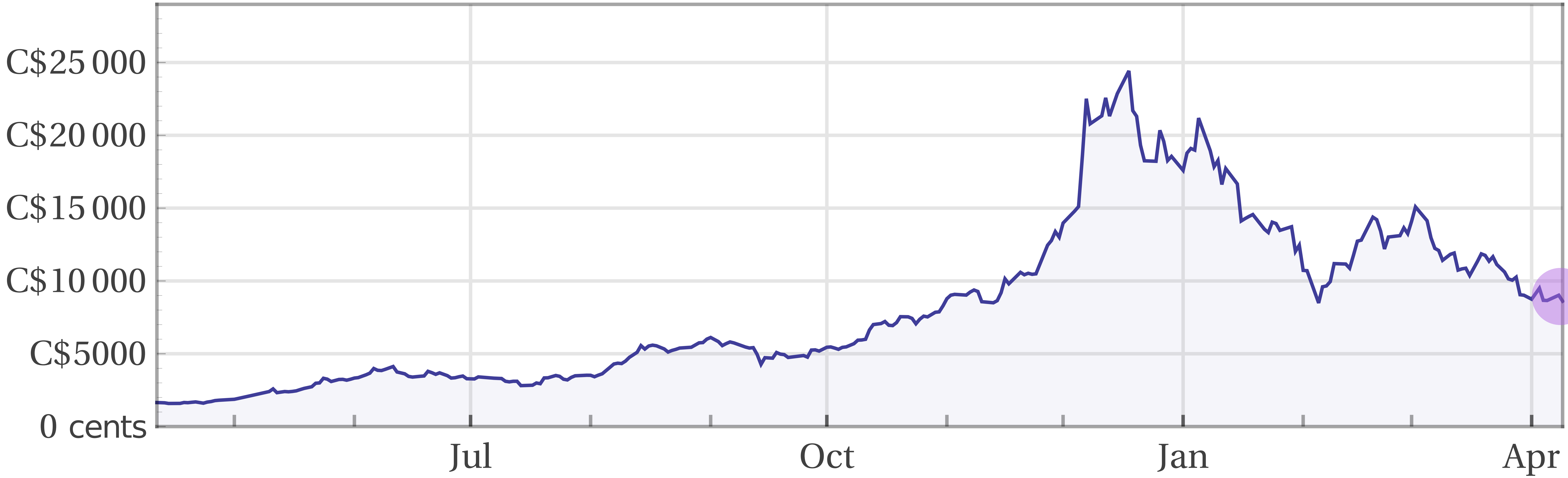
Bitcoin is a currency

Price increases:

* Cause hoarding
* Cause speculation
* Deter borrowing

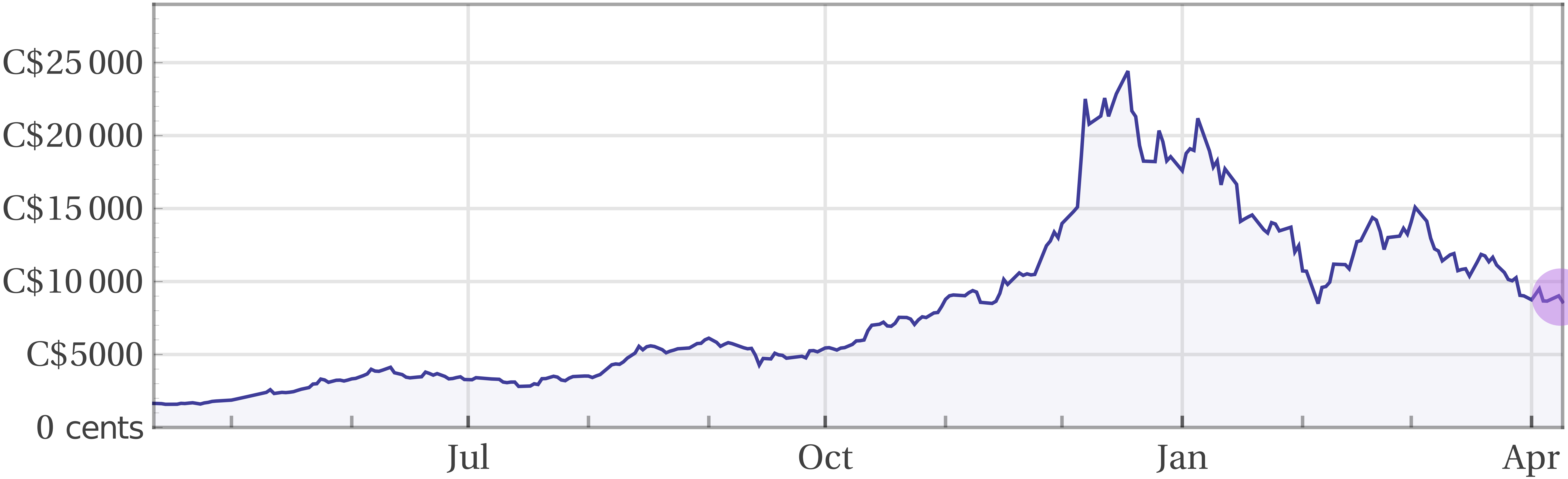


Why?

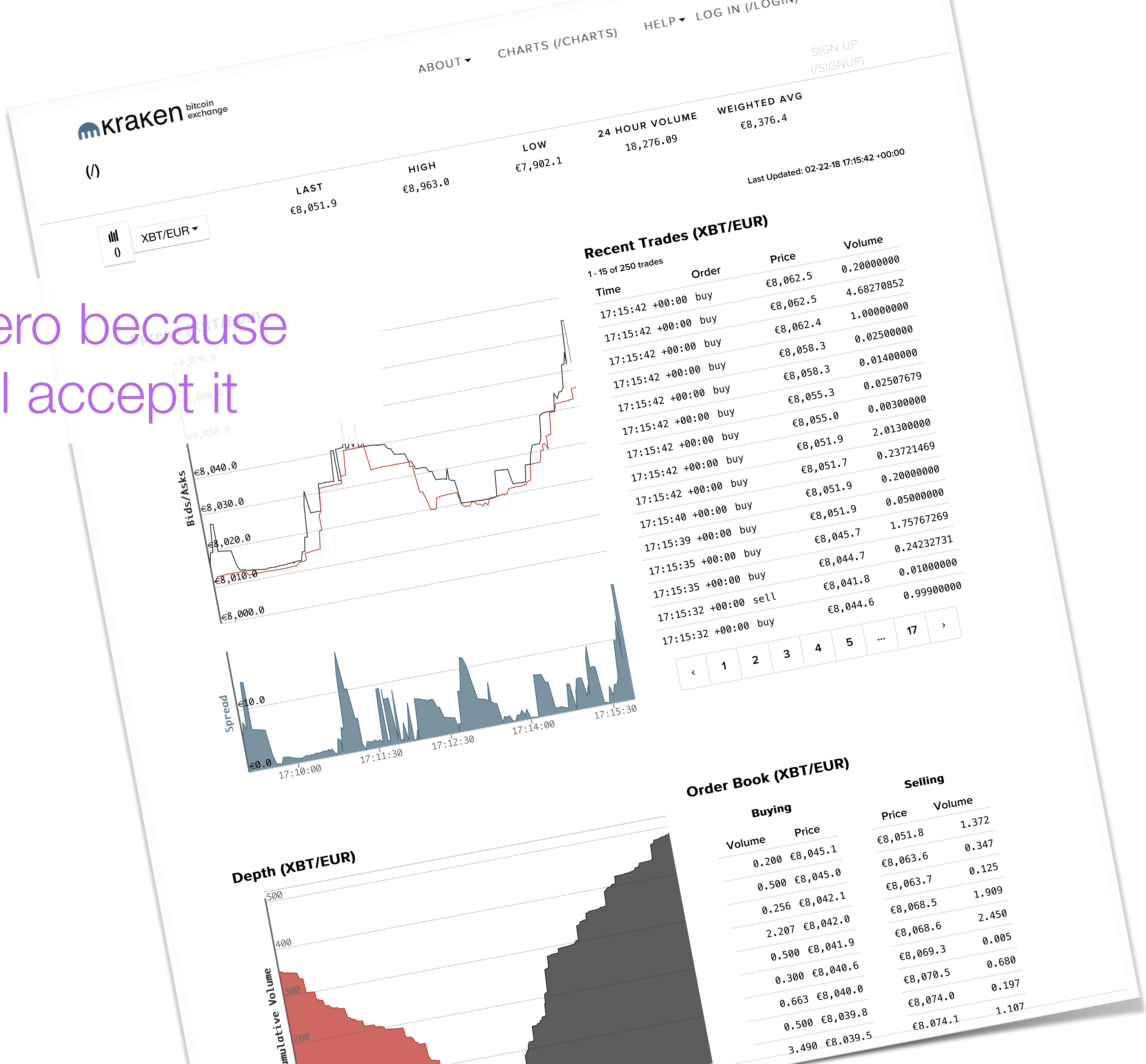


Why?

More than zero because someone will accept it



More than zero because someone will accept it



LAST	HIGH	LOW	24 HOUR VOLUME	WEIGHTED AVG
€8,051.9	€8,963.0	€7,902.1	18,276.09	€8,376.4

Last Updated: 02-22-18 17:15:42 +00:00

Recent Trades (XBT/EUR)

1 - 15 of 250 trades

Time	Order	Price	Volume
17:15:42 +00:00	buy	€8,062.5	0.20000000
17:15:42 +00:00	buy	€8,062.5	4.68270852
17:15:42 +00:00	buy	€8,062.4	1.00000000
17:15:42 +00:00	buy	€8,058.3	0.02500000
17:15:42 +00:00	buy	€8,058.3	0.01400000
17:15:42 +00:00	buy	€8,055.3	0.02507679
17:15:42 +00:00	buy	€8,055.0	0.00300000
17:15:42 +00:00	buy	€8,051.9	2.01300000
17:15:42 +00:00	buy	€8,051.7	0.23721469
17:15:42 +00:00	buy	€8,051.9	0.20000000
17:15:40 +00:00	buy	€8,051.9	0.05000000
17:15:39 +00:00	buy	€8,045.7	1.75767269
17:15:35 +00:00	buy	€8,044.7	0.24232731
17:15:35 +00:00	buy	€8,041.8	0.01000000
17:15:32 +00:00	sell	€8,044.6	0.99900000
17:15:32 +00:00	buy		

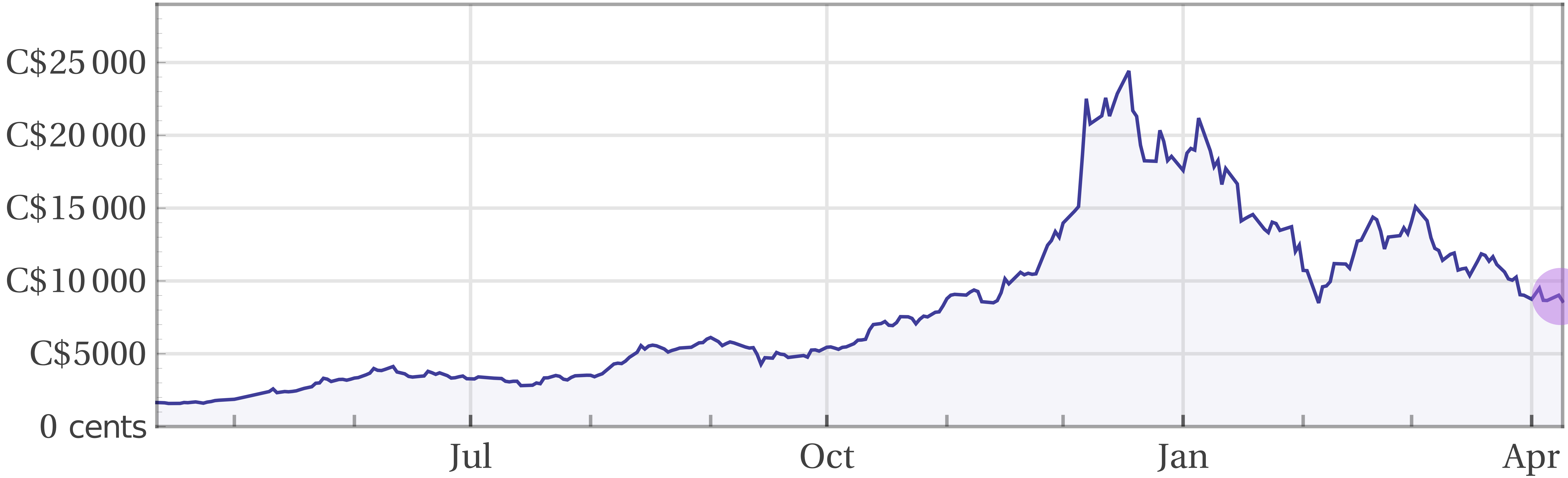
Depth (XBT/EUR)

Order Book (XBT/EUR)

Buying		Selling	
Volume	Price	Price	Volume
0.200	€8,045.1	€8,051.8	1.372
0.500	€8,045.0	€8,063.6	0.347
0.256	€8,042.1	€8,063.7	0.125
2.207	€8,042.0	€8,068.5	1.909
0.500	€8,041.9	€8,068.6	2.450
0.300	€8,040.6	€8,069.3	0.005
0.663	€8,040.0	€8,070.5	0.680
0.500	€8,039.8	€8,074.0	0.197
3.490	€8,039.5	€8,074.1	1.107

Why?

$15K instead of $15.00 or $15M?



0.30519173 BTC

Total Transactions 4

Total Received 0.50519173 BTC

Total Sent 0.20 BTC

Final Balance 0.30519173 BTC

Bitcoin is digital currency proposed ~10 years ago

It is used via phones, computers, & websites

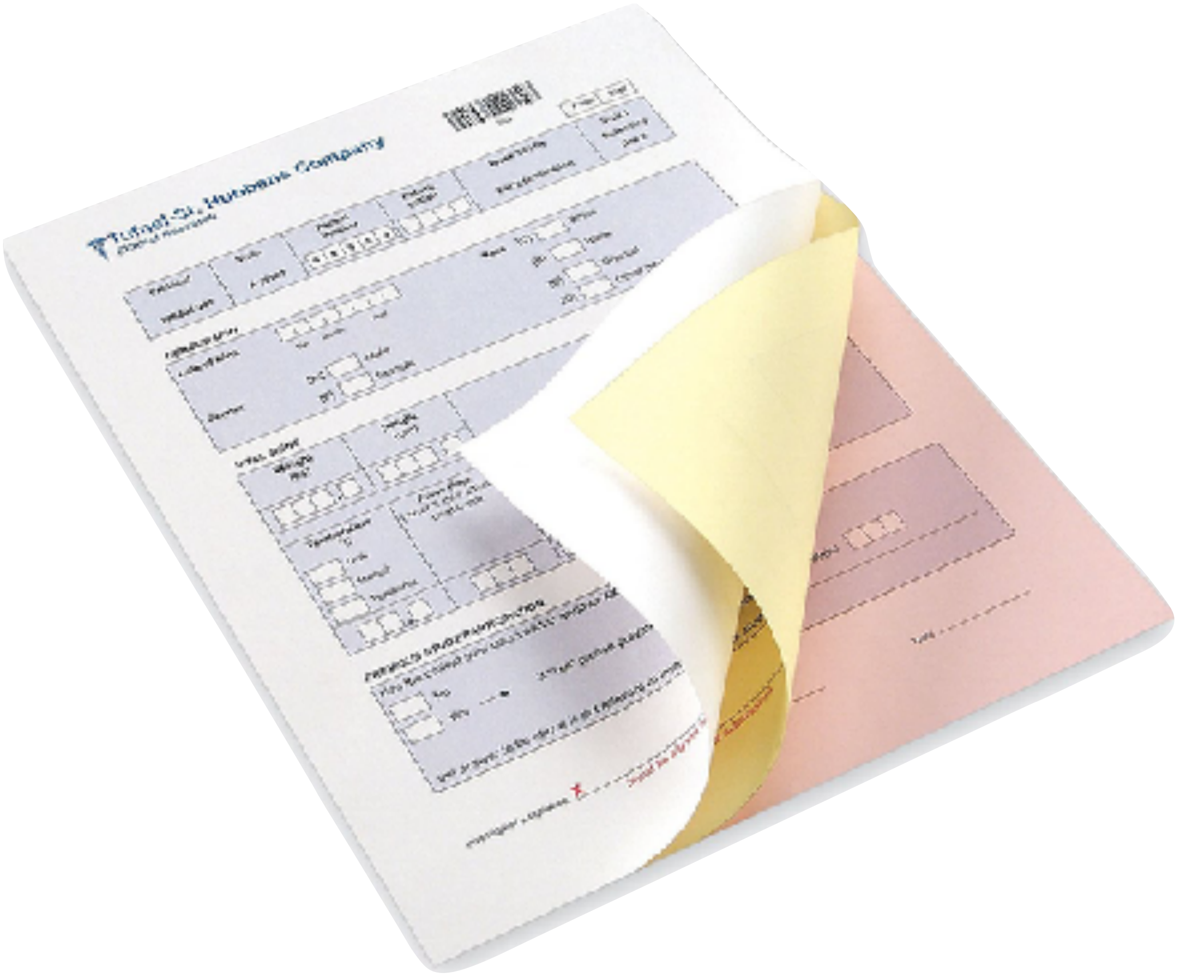
Every transaction is written into a secure ledger of called the blockchain — no one is in charge

Digital Revolution

Blockchain

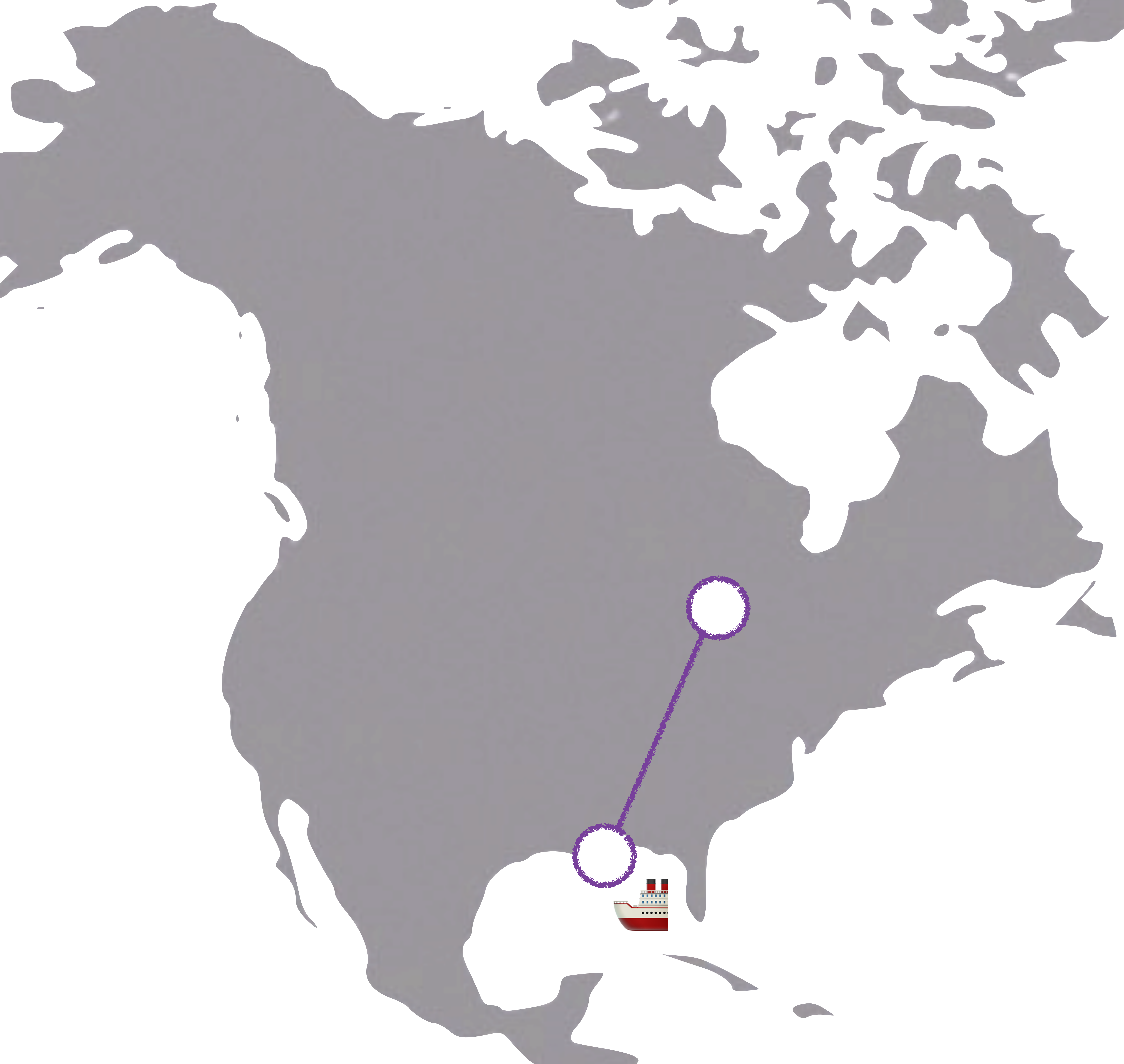
Digital Revolution

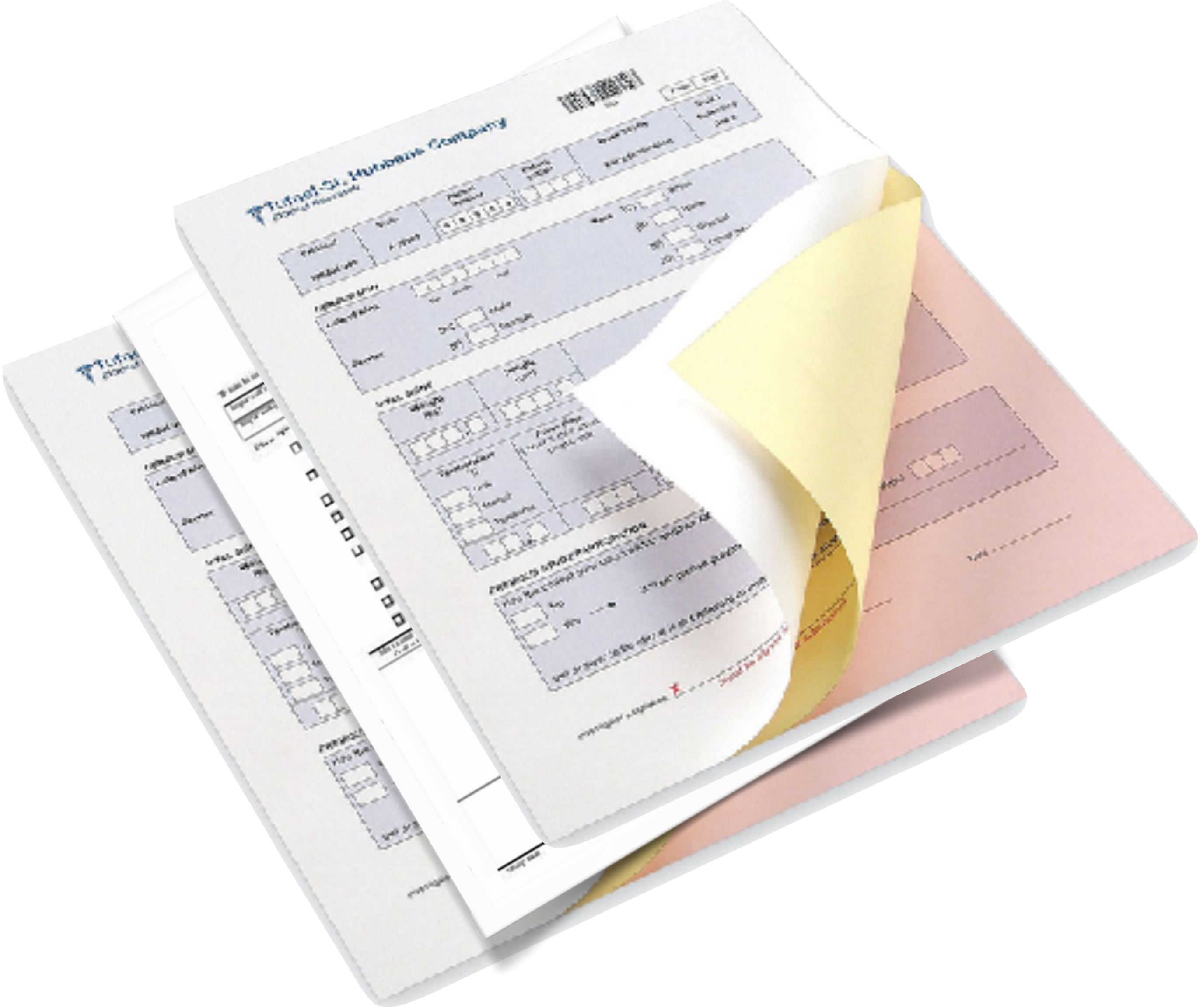
For business processes based on paper records, digitization increases efficiency

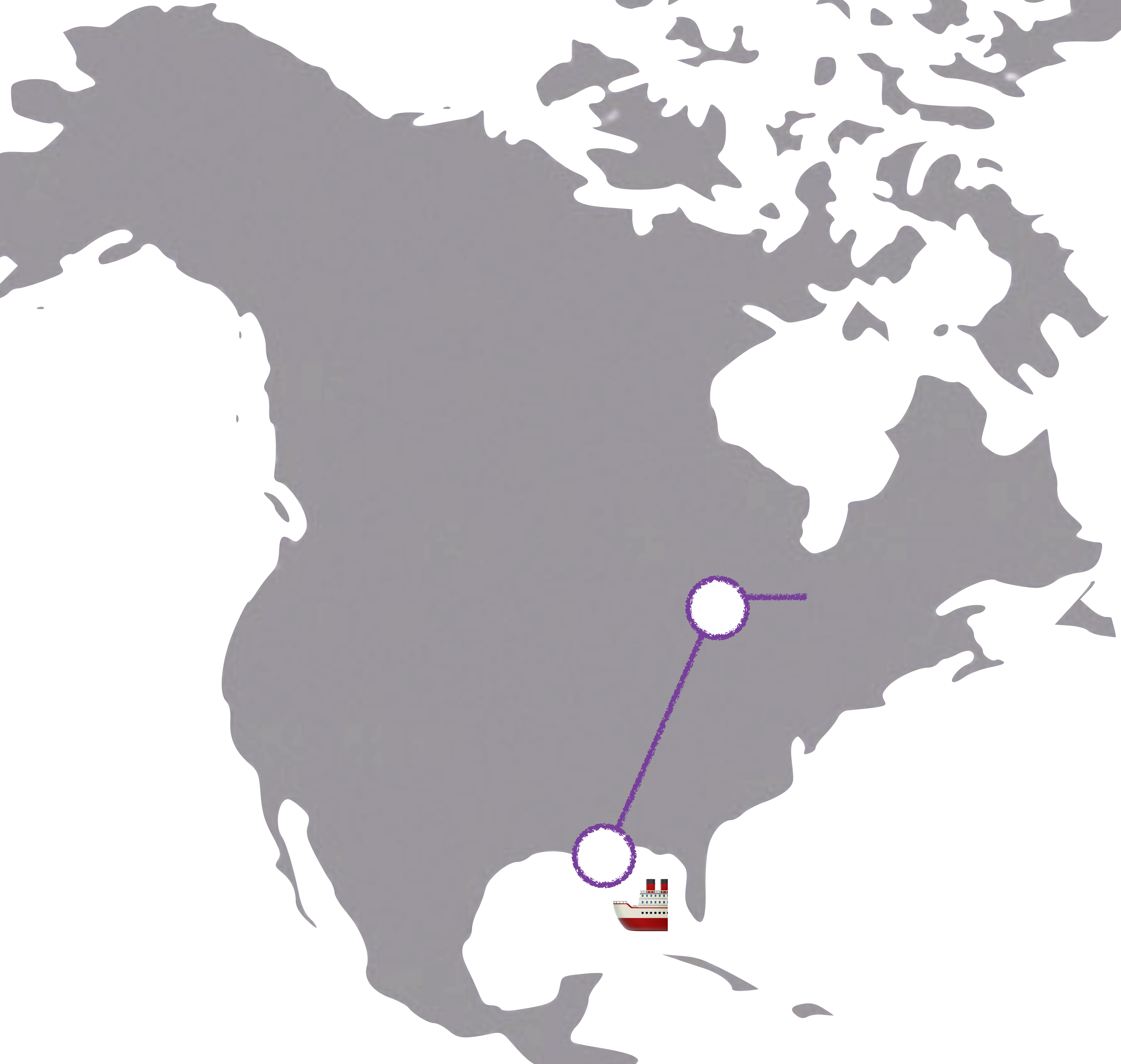


CONCORDIA

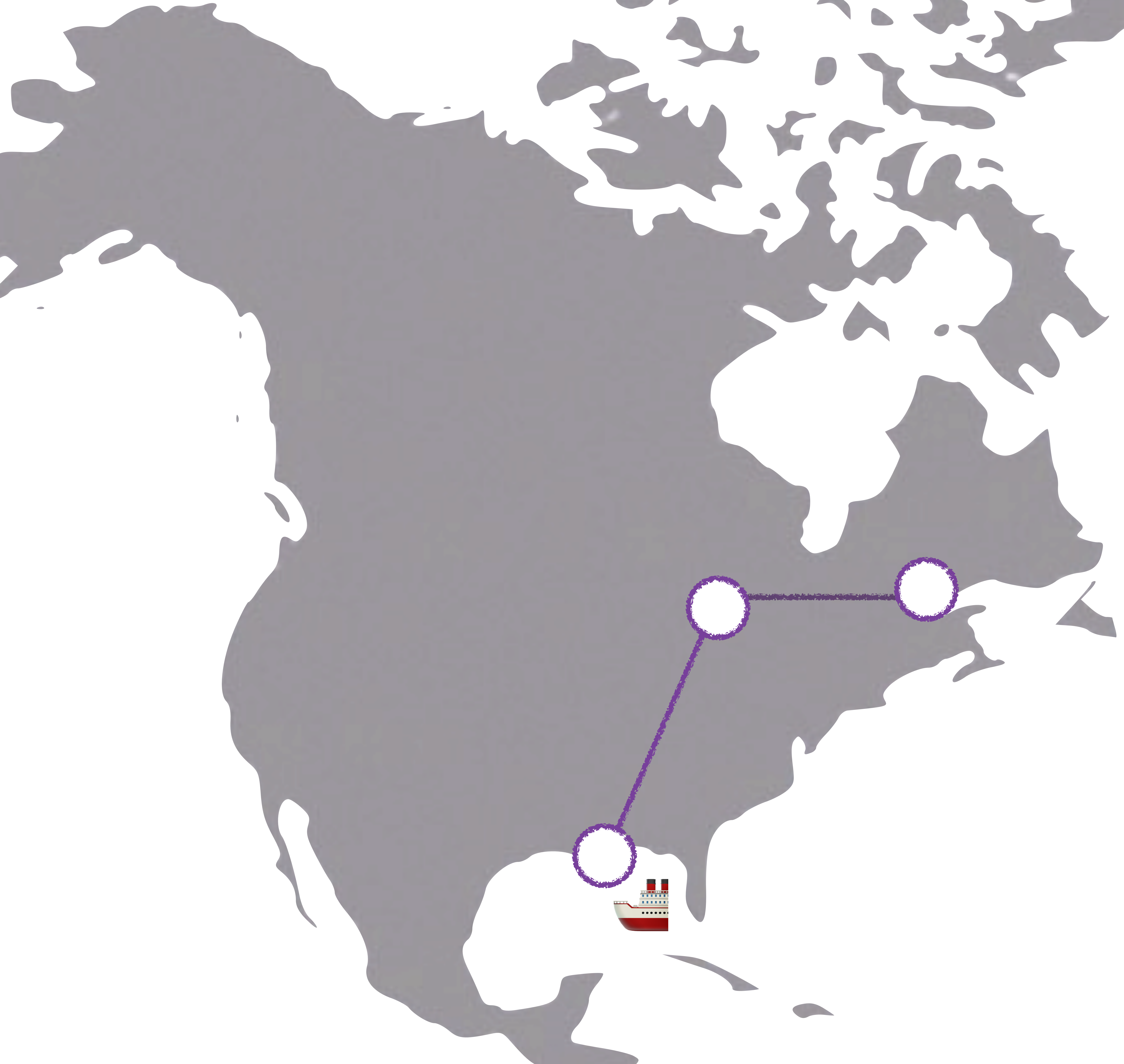
U.S. Customs and Border Protection

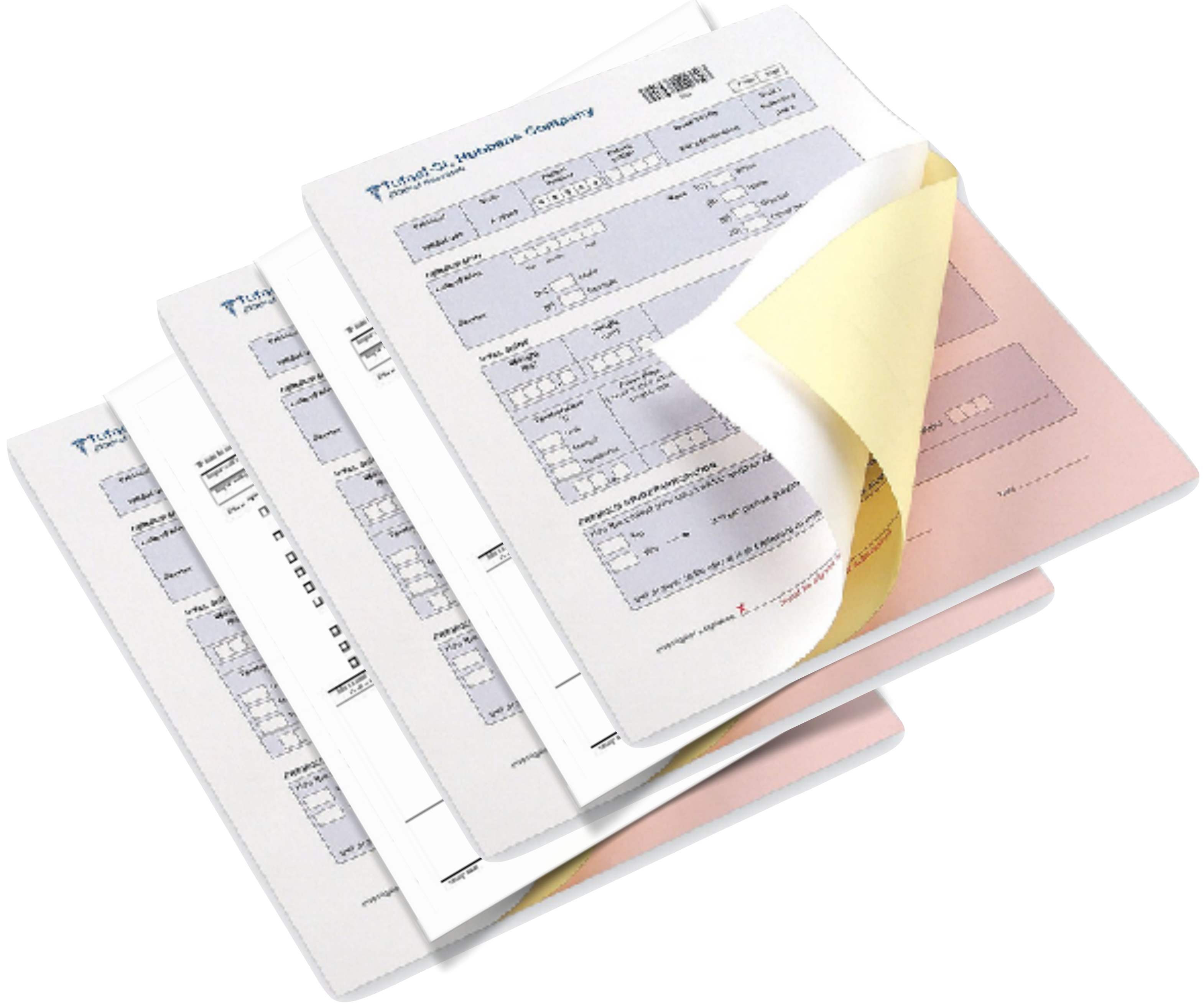






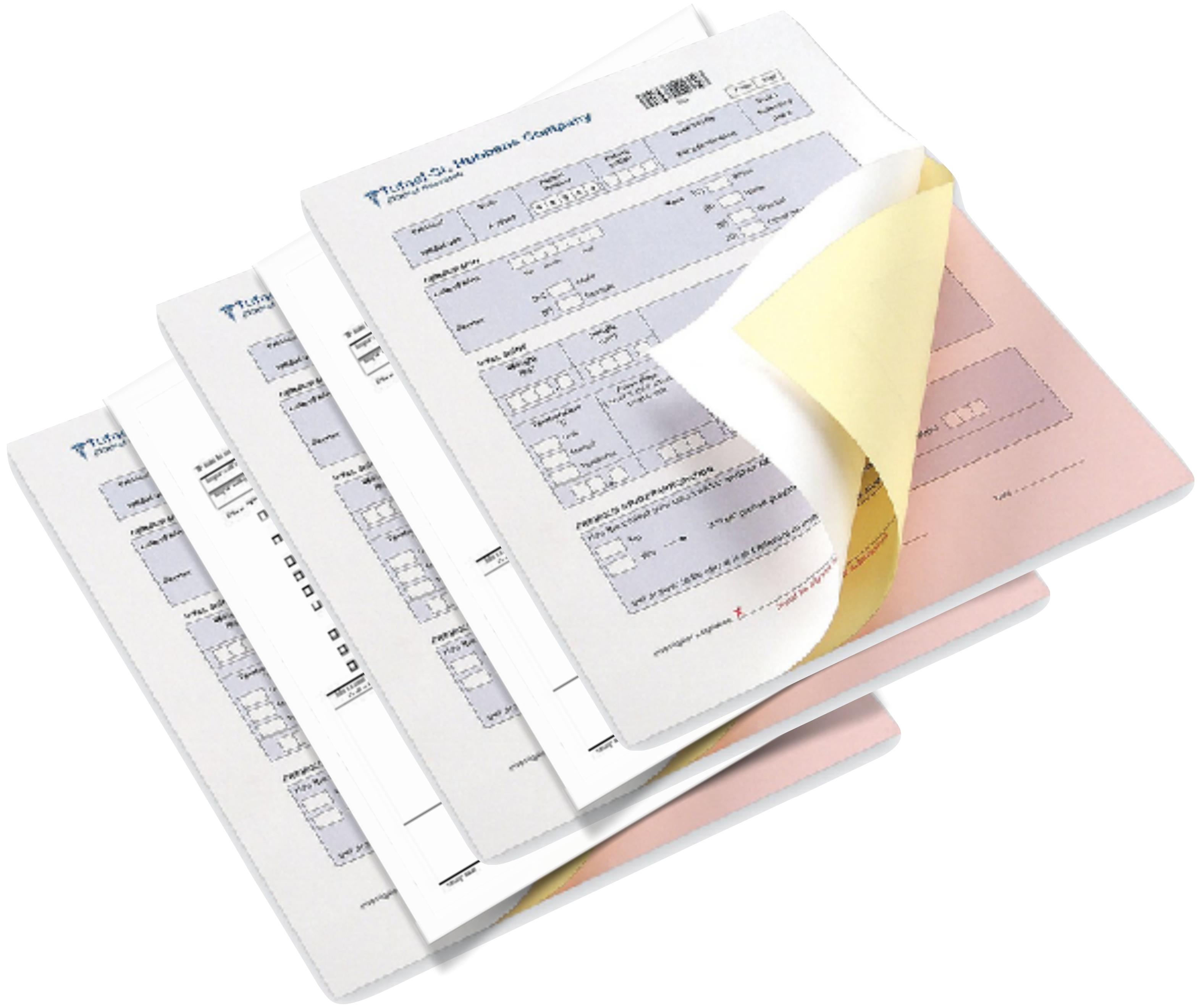
CONCORDIA



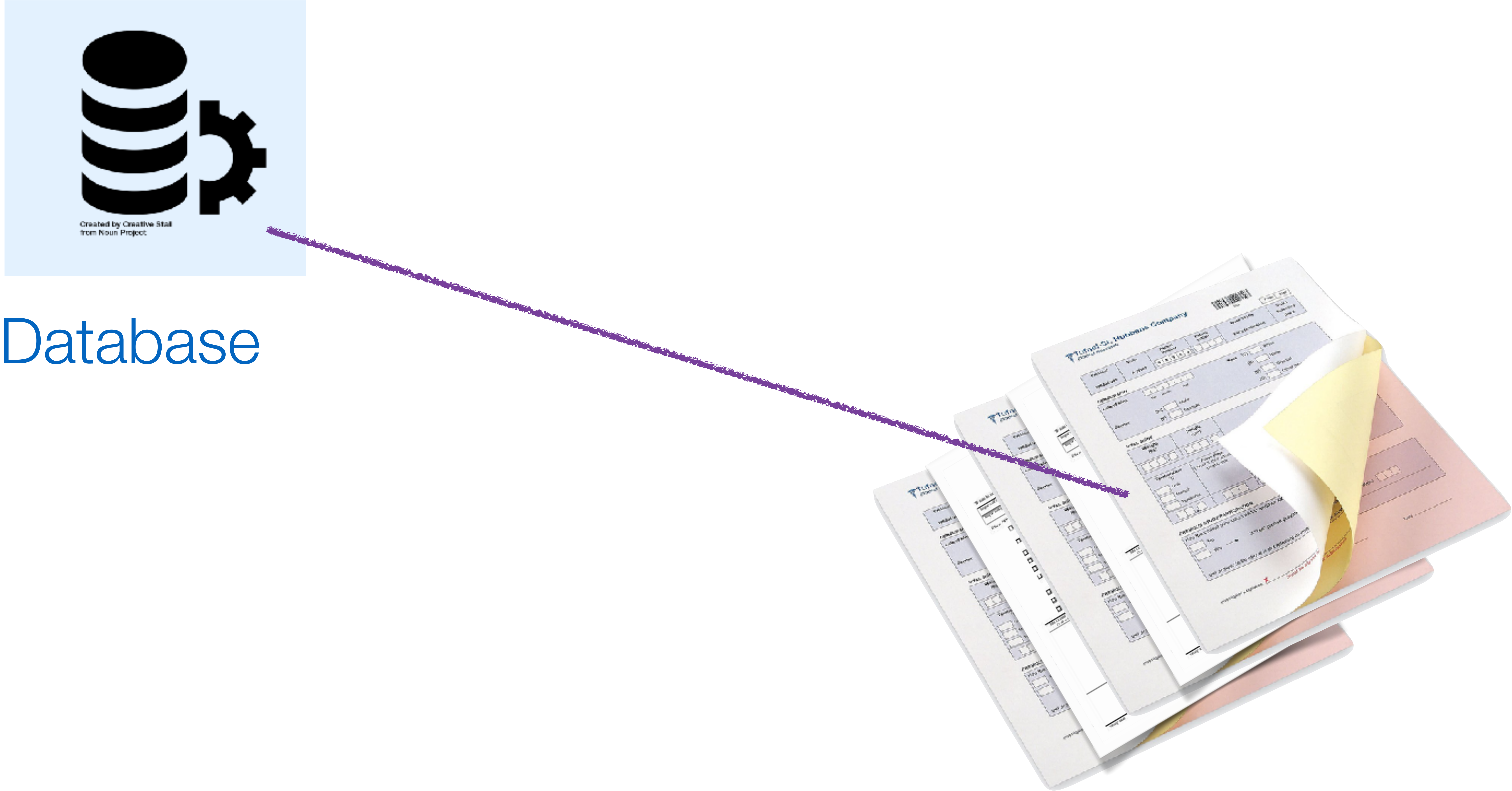


CONCORDIA

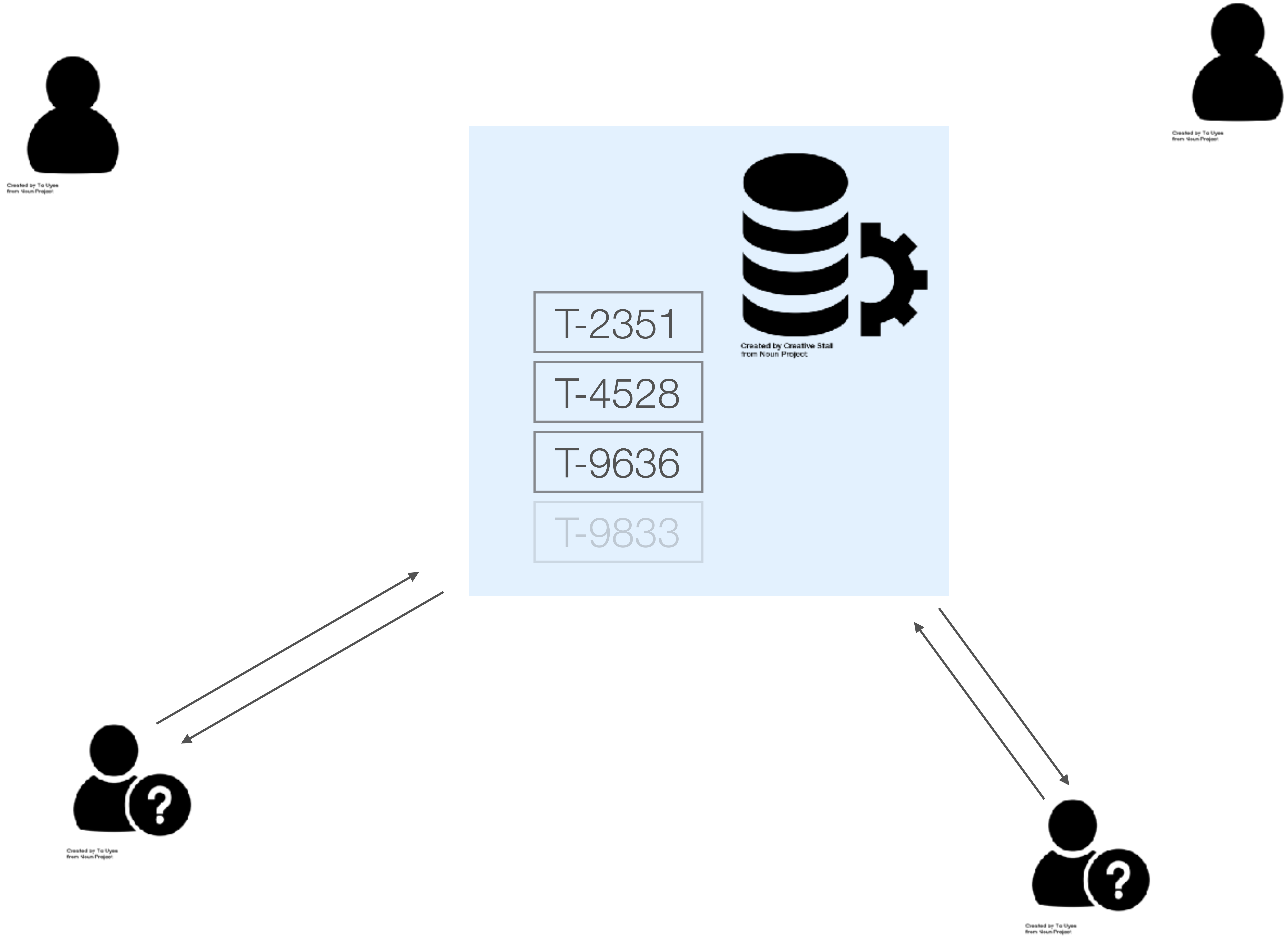
Digital Revolution

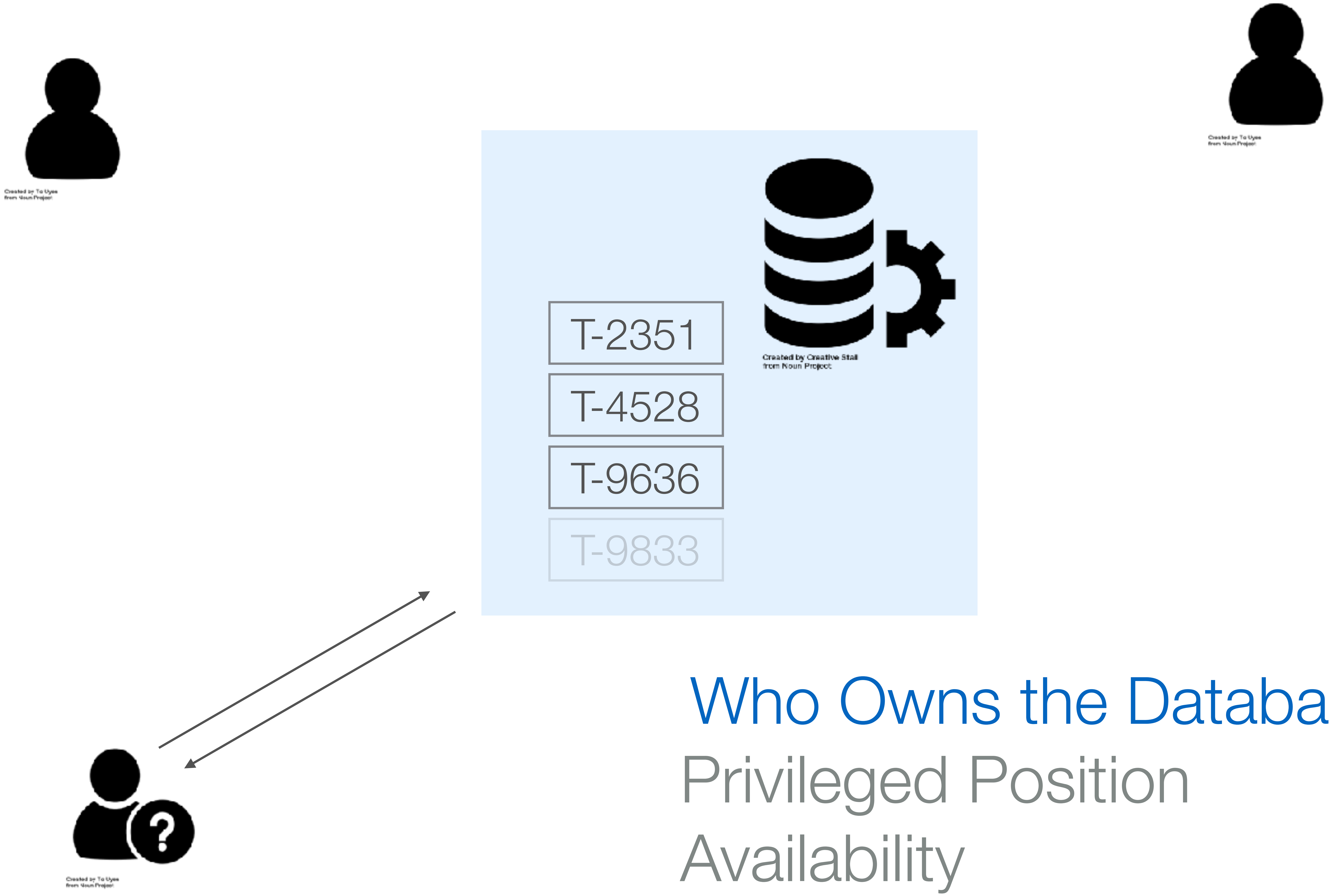


Digital Revolution



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

Created by Creative Stall from Noun Project

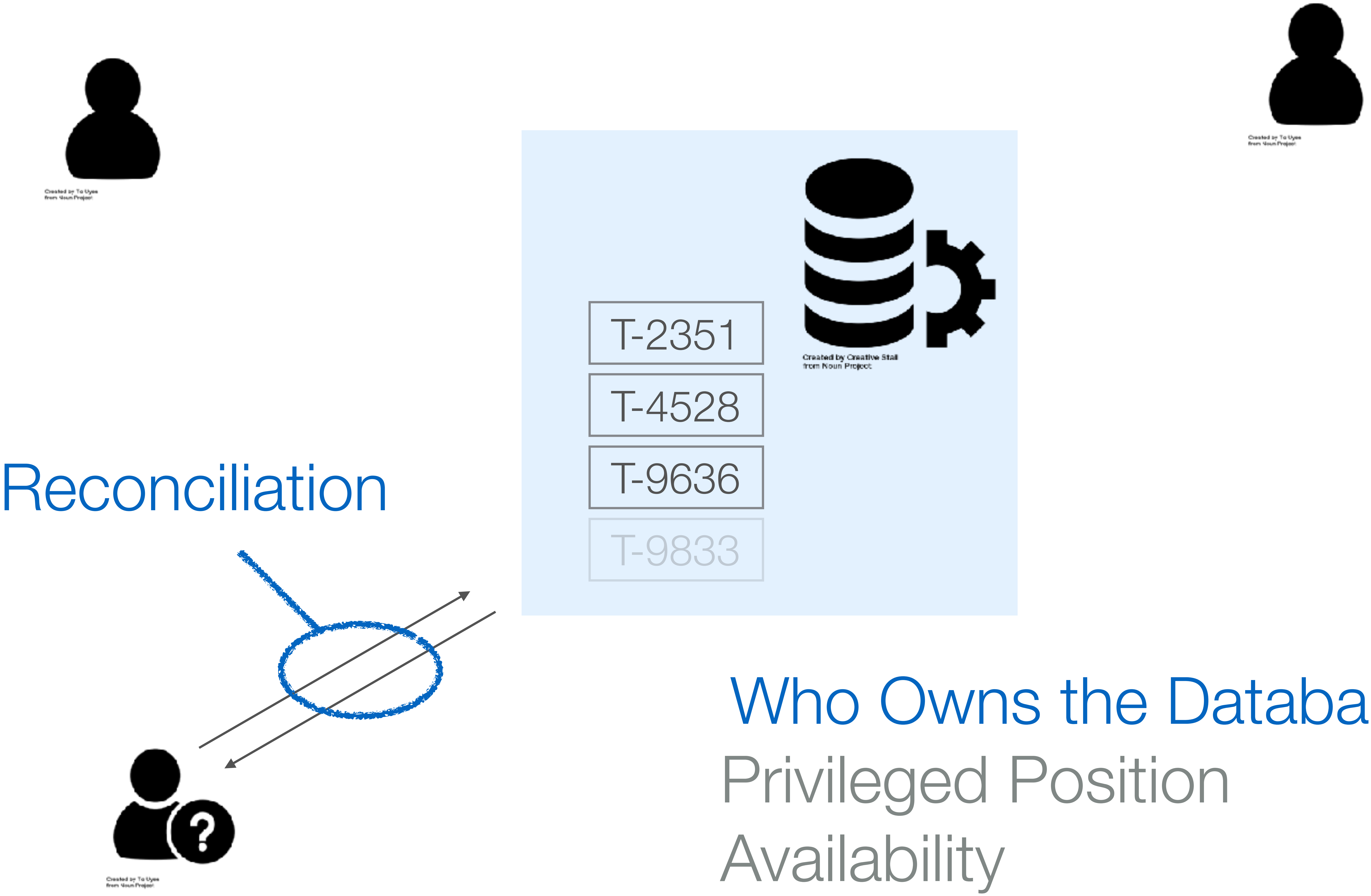
Created by To Uyen from Noun Project

Who Owns the Database?

Privileged Position

Availability

Manage Access

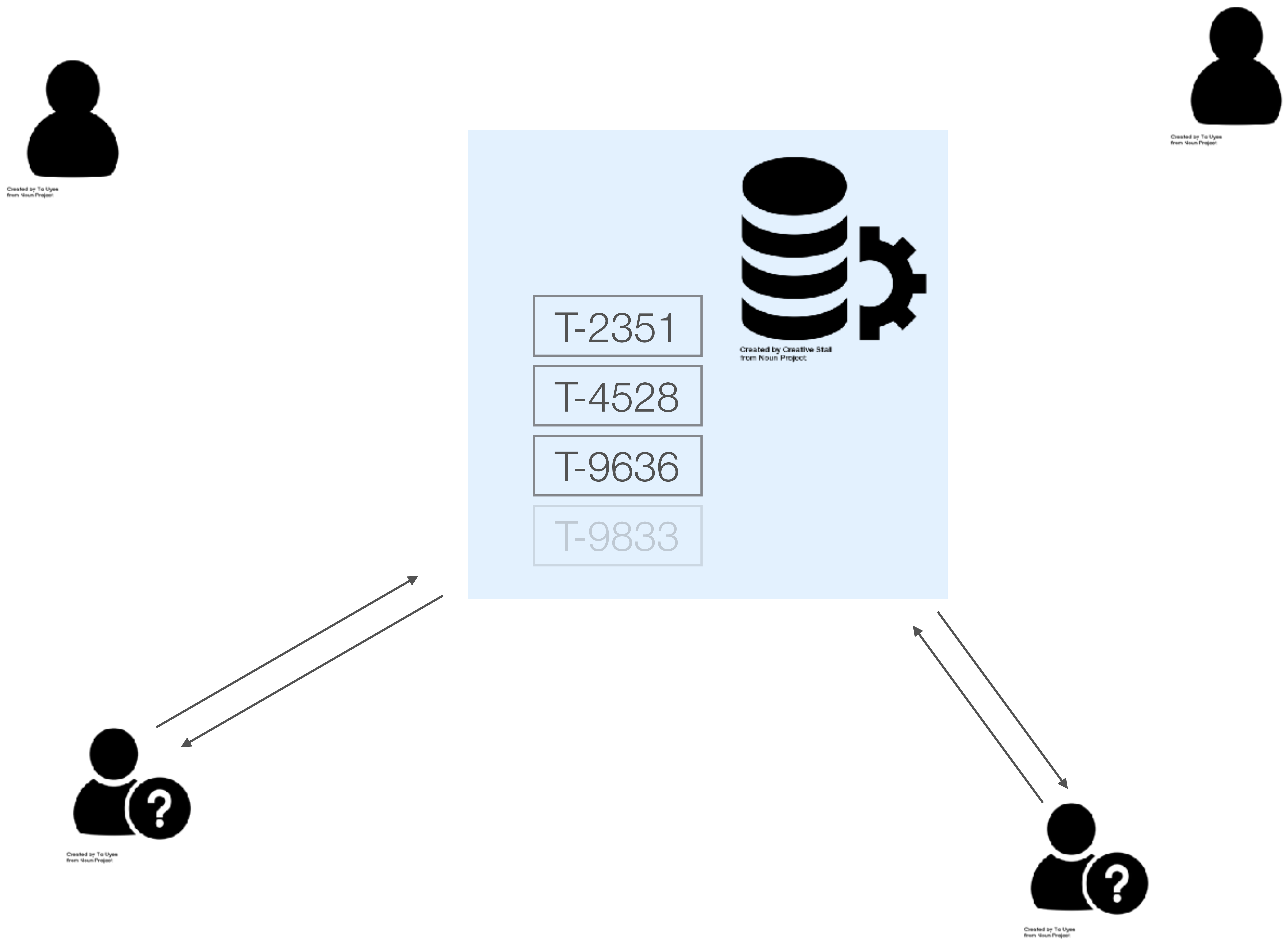


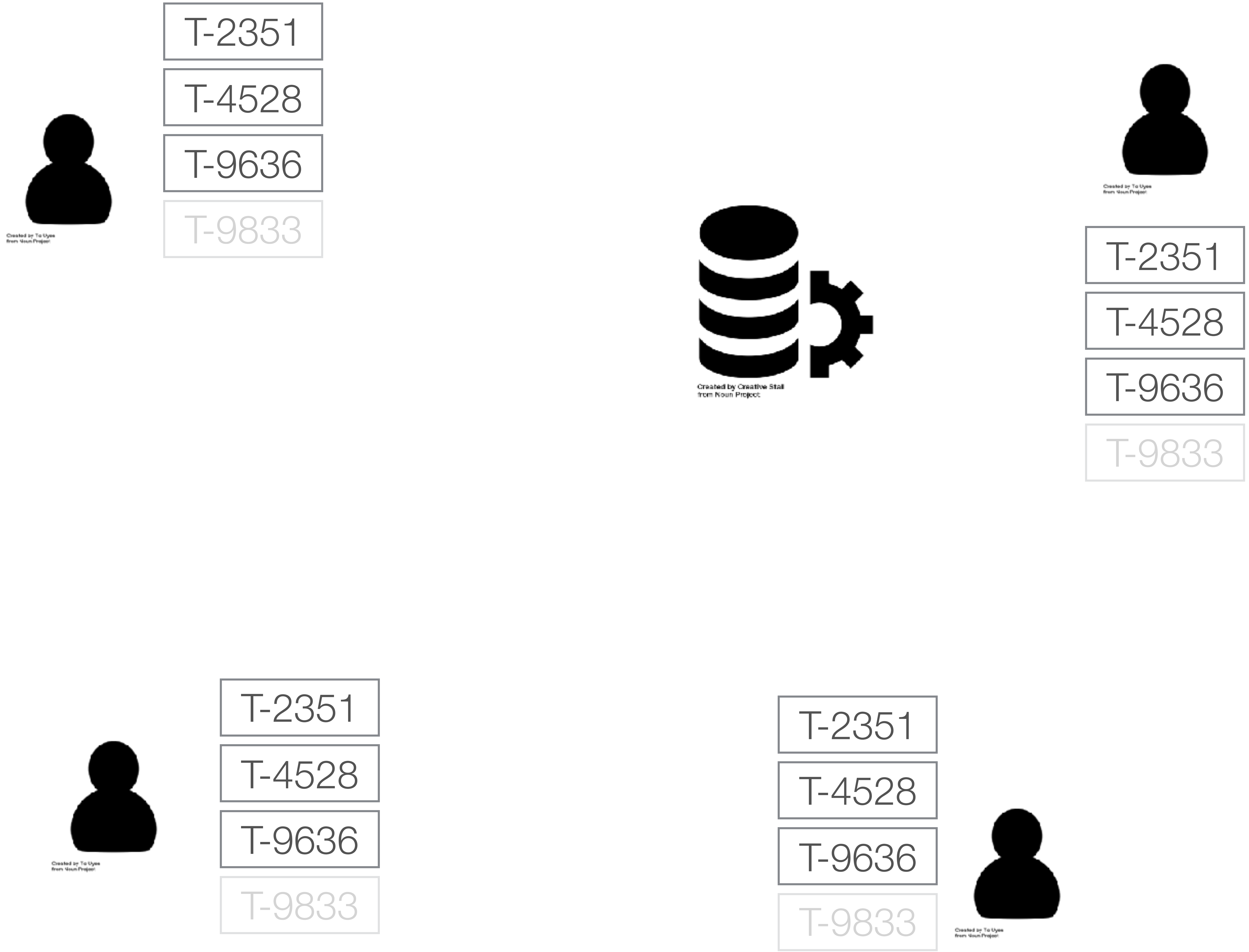
Who Owns the Database?

Privileged Position

Availability

Manage Access


Created by Tu Uyen
from Noun Project
Created by Tu Uyen
from Noun Project
T-2351
T-4528
T-9636
T-9833
Created by Creative Stall
from Noun Project
Created by Tu Uyen
from Noun Project
Created by Tu Uyen
from Noun Project



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

Created by To Uyen from Noun Project

Created by Creative Stall 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

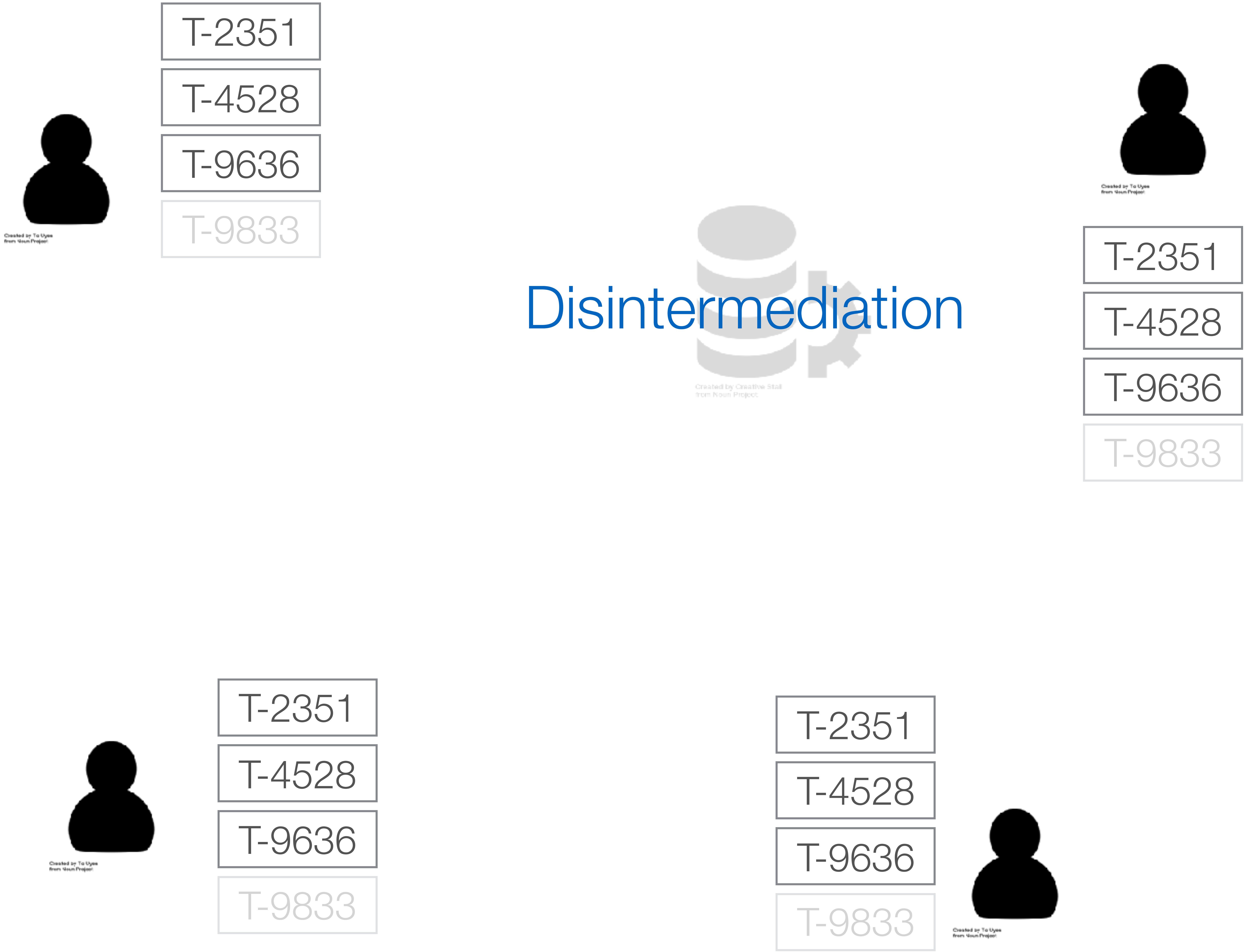
Created by To Uyen from Noun Project

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

Created by To Uyen from Noun Project

Created by To Uyen from Noun Project

Disintermediation



T-2351

T-4528

T-9636

T-9833

Created by Tu Uyen
from Noun Project

Created by Creative Stall
from Noun Project

Created by Tu Uyen
from Noun Project

T-2351

T-4528

T-9636

T-9833

T-2351

T-4528

T-9636

T-9833

Created by Tu Uyen
from Noun Project

T-2351

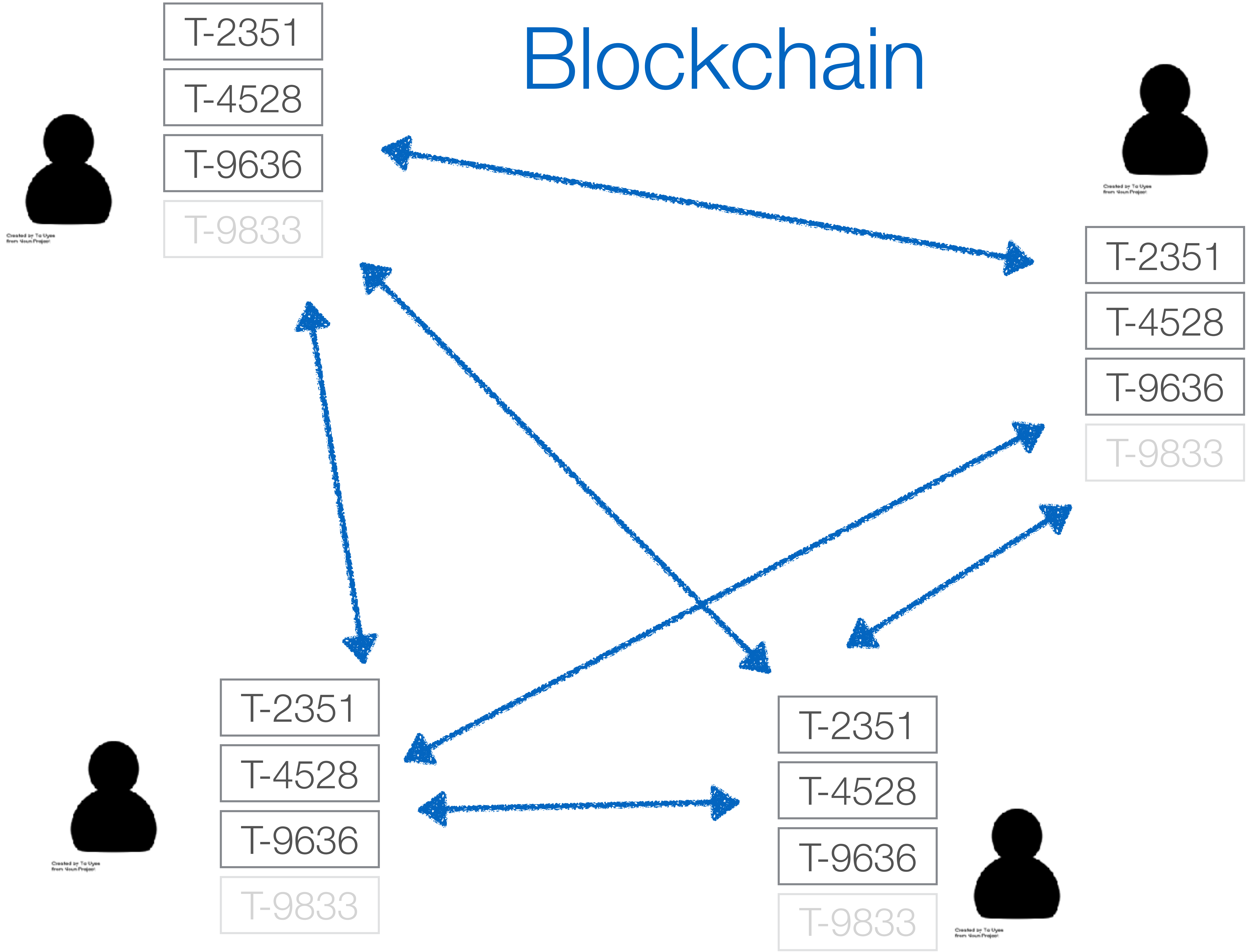
T-4528

T-9636

T-9833

Created by Tu Uyen
from Noun Project

Blockchain



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

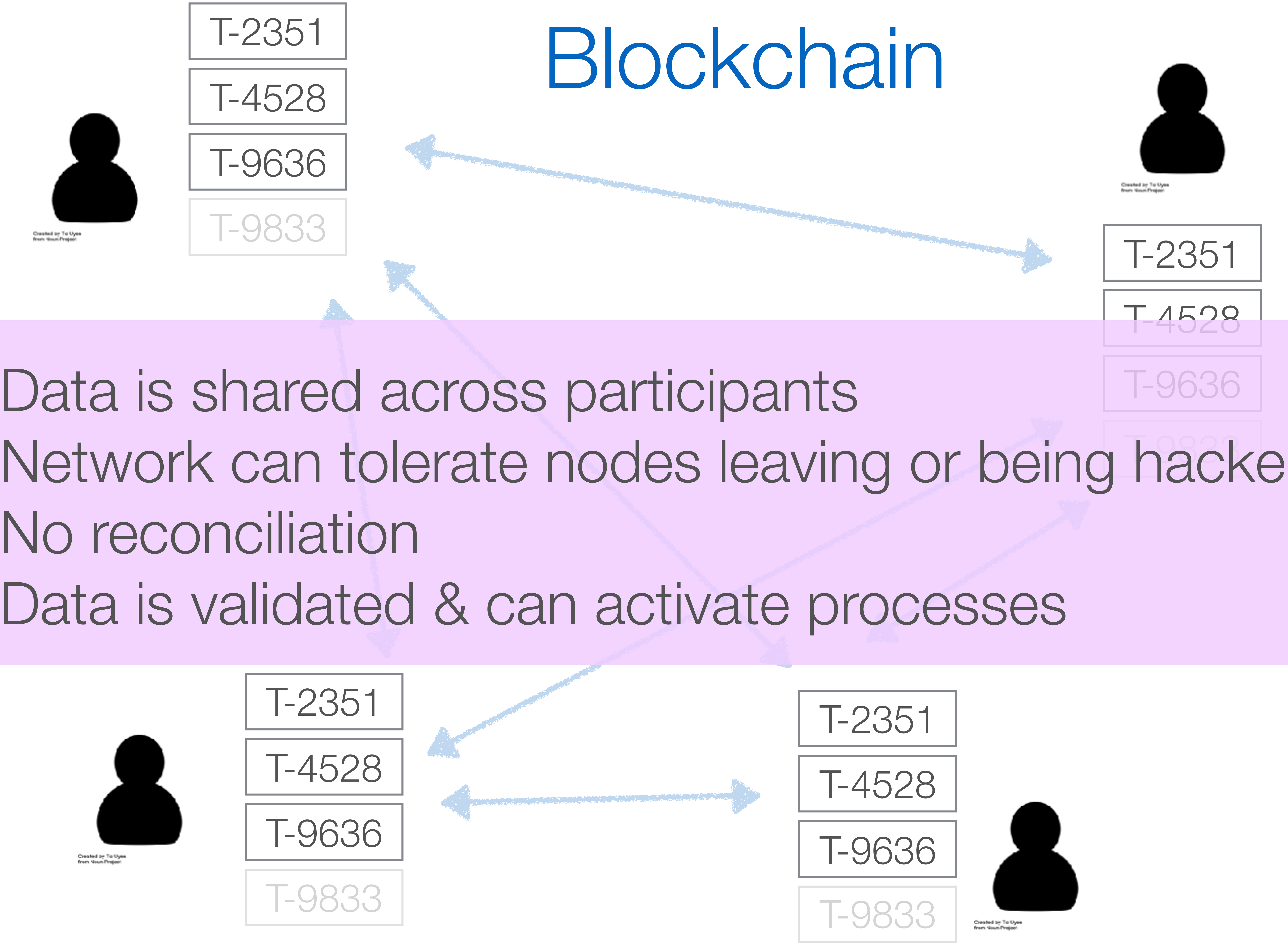
T-2351
T-4528
T-9636
T-9833

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

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

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

Blockchain



Data is shared across participants

Network can tolerate nodes leaving or being hacked

No reconciliation

Data is validated & can activate processes

Use Cases

Lending

There is very little lending in cryptocurrencies

We show how a lending market could be designed for peer-to-peer lending up to commercial paper

We provide a variety of instruments for mitigating counter-party risk including collateral, insurance, & credit default swaps

Toward Cryptocurrency Lending.
Chidinma Okoye, Jeremy Clark. WTSC 2018

HTTPS

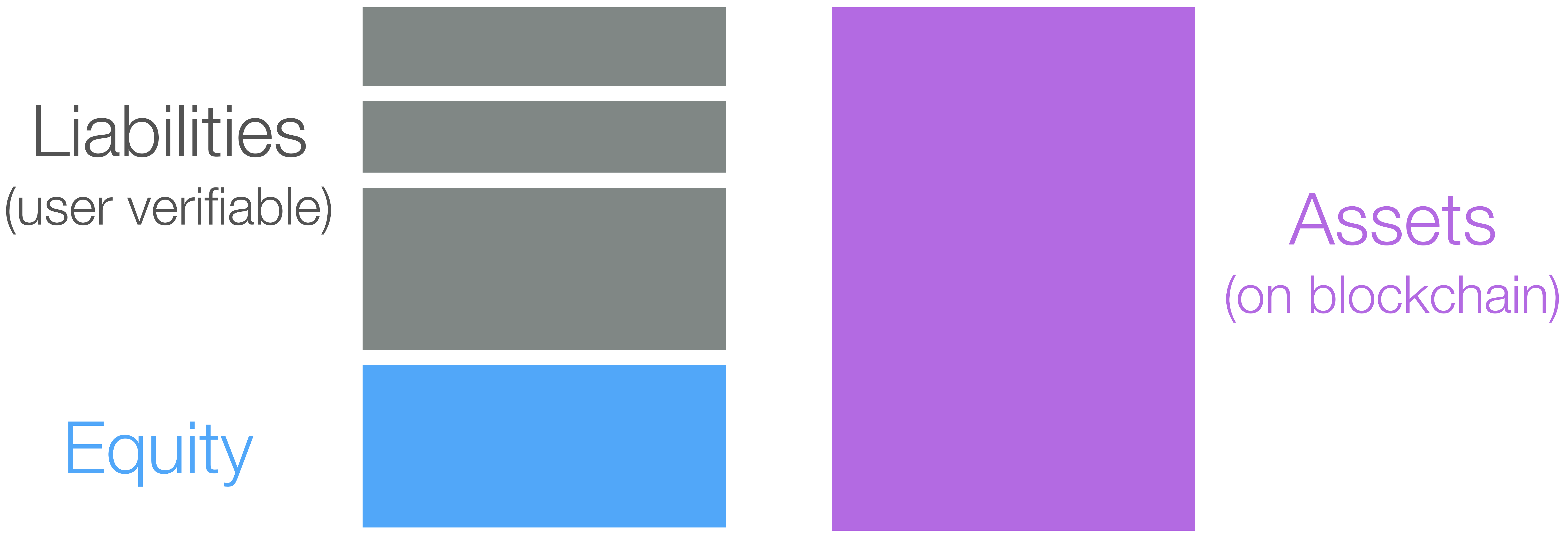
Using passwords, credit card numbers, cookies, and other private user data on the web requires privacy

HTTPS gives your computer a secure tunnel

Where does the tunnel end?

Ghazal: toward truly authoritative web certificates using Ethereum. Chidinma Okoye, Jeremy Clark. WTSC 2018

Solvency Proofs



Liabilities
(user verifiable)

Equity

Assets
(on blockchain)

ZKP: Equity = Assets - Liabilities >= 0

Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges.
G Dagher, B Bünz, J Bonneau, J Clark, D Boneh. CCS 2015

AUTORITÉ DES MARCHÉS FINANCIERS

Markets

Excitement around replacing post-trade settlement for securities with a blockchain

We designed a decentralized order book based on a call market design

Nuances play a large roll: timing, speed, front-running, incentives

Take-away 1: Bitcoin-style digital cash is here to stay

Take-away 2: the Blockchain hype is (somewhat) real

Take-away 3: Blockchain success = invisibility

Take-away 4: Don’t invest