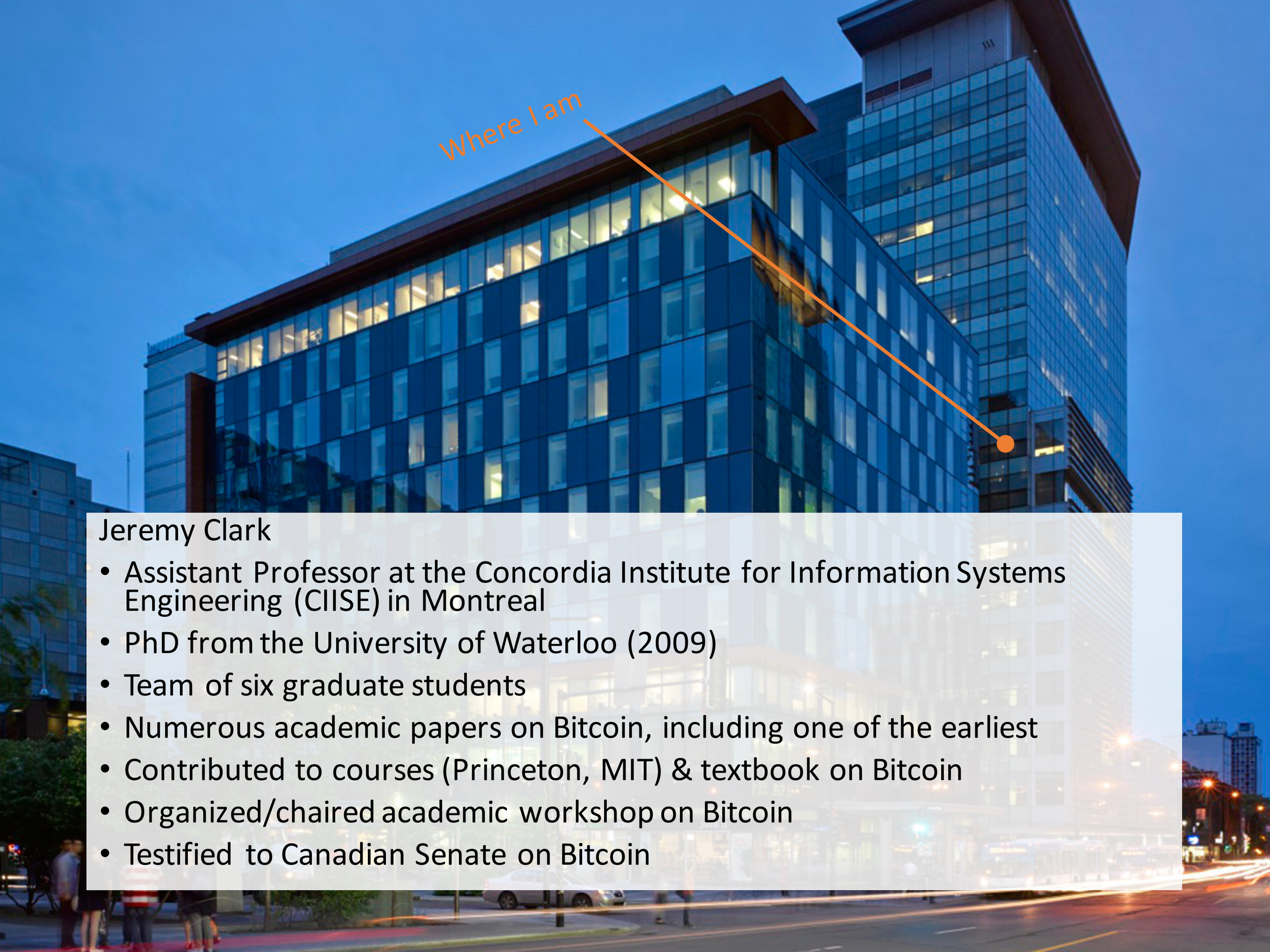
Provisions
Privacy Preserving Proof of Solvency

Jeremy Clark



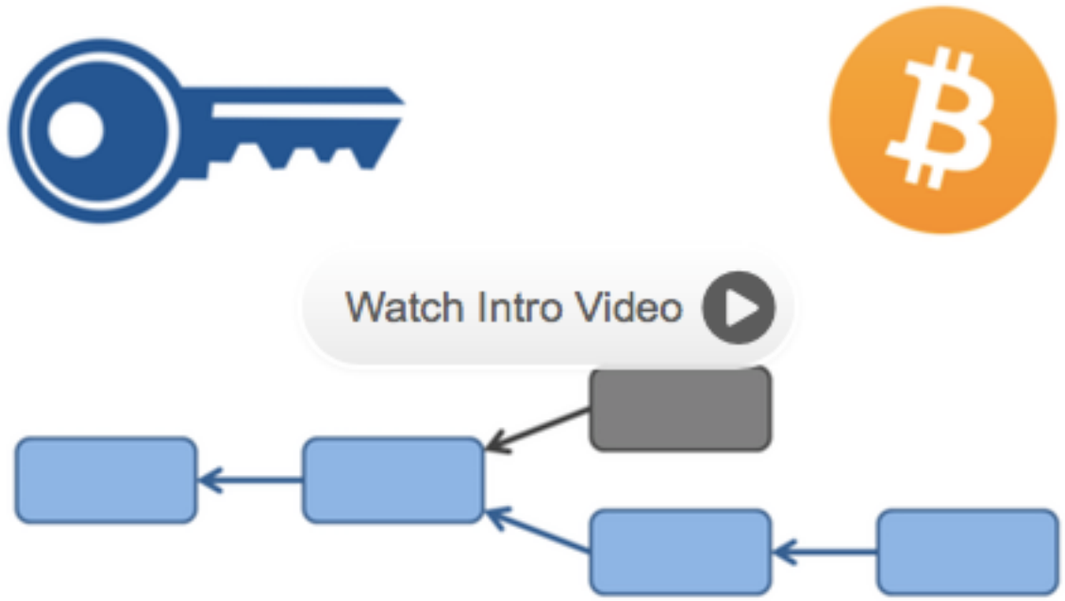
Jeremy Clark

- 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

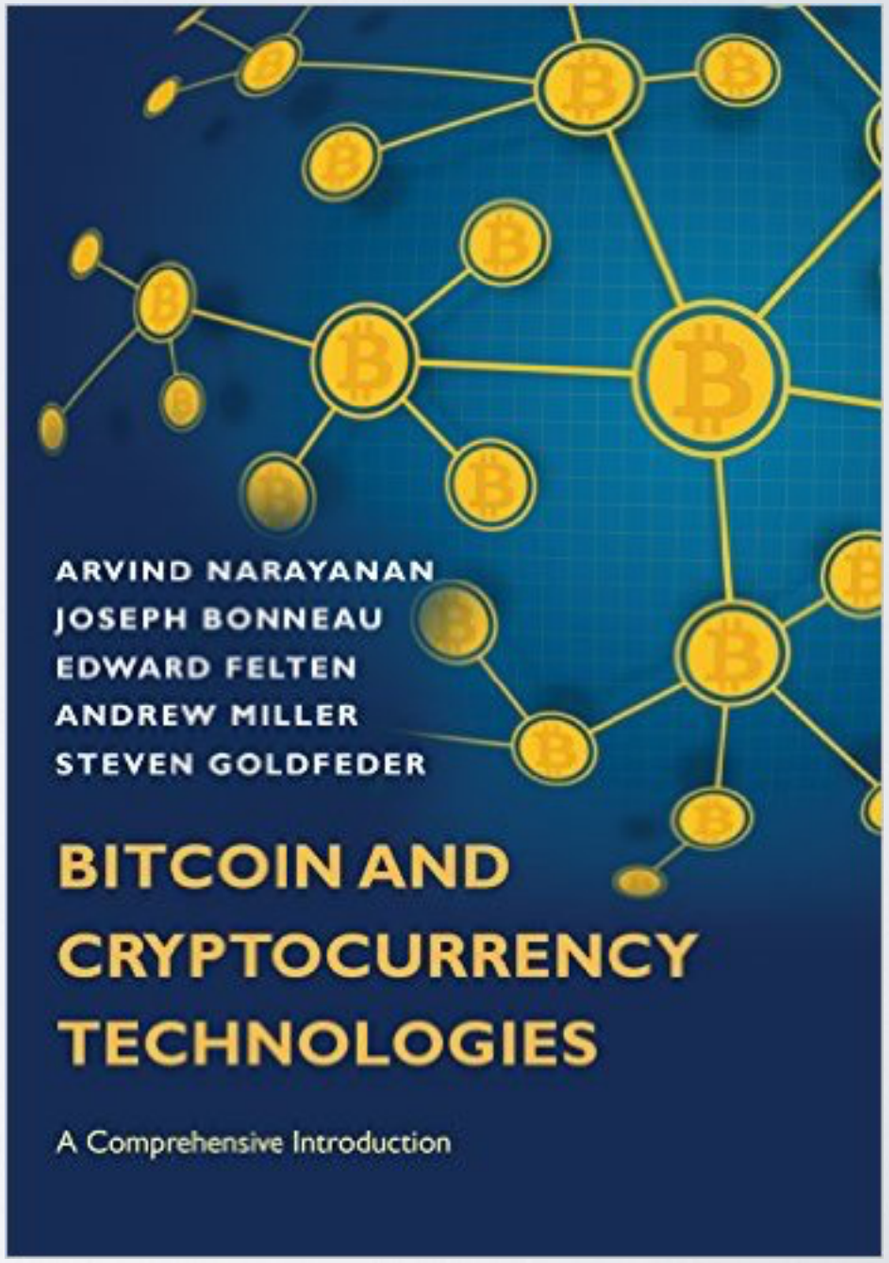
with a preface by Jeremy Clark

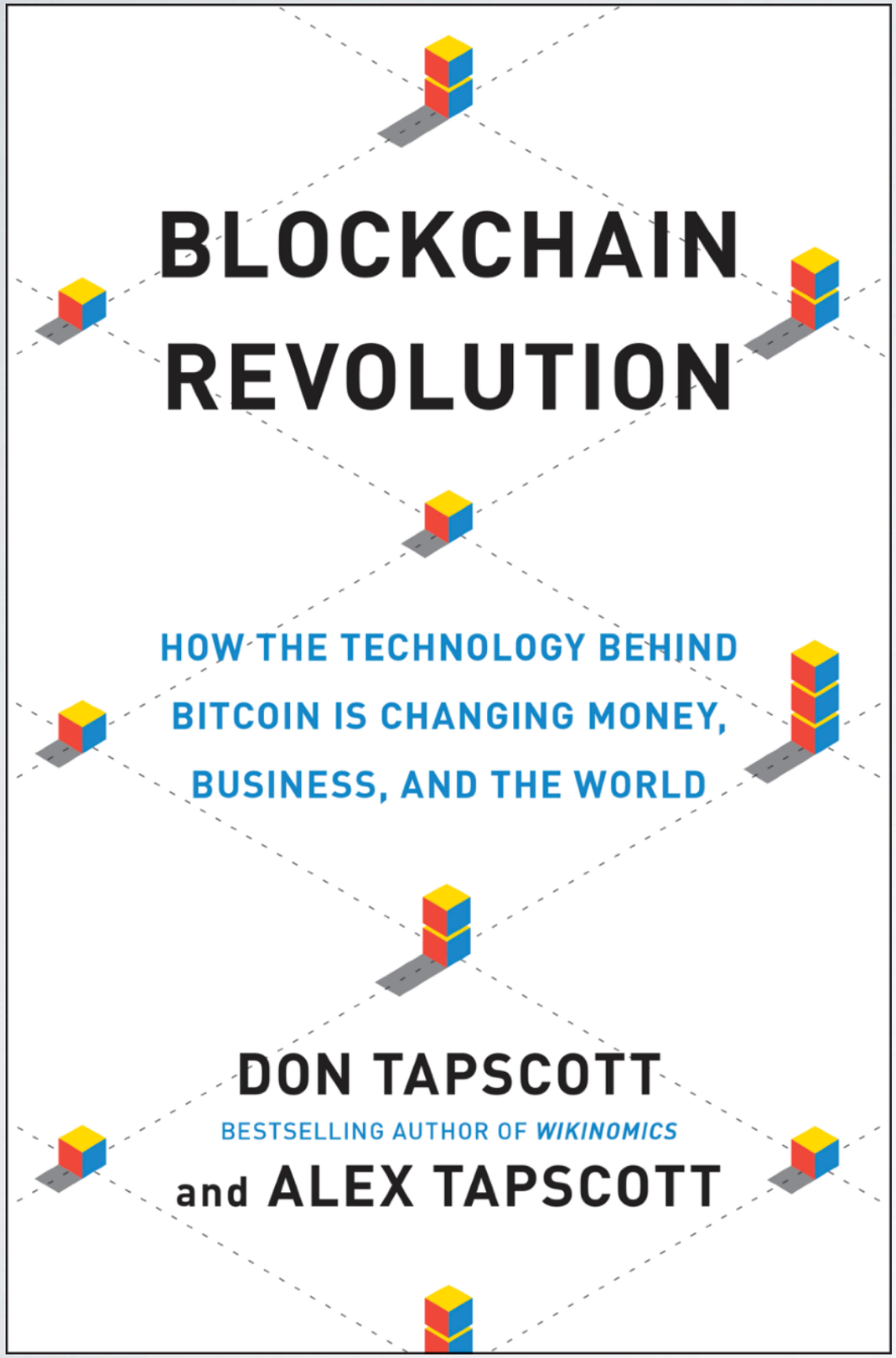
Draft — Feb 9, 2016

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

R3

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

Case Study:

Proof of Solvency

Joint Work

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

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

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.

Bitcoin Savings & Trust (1834303 $)
MyBitcoin Theft (1110544 $)
Allinvain Theft (502750.20 $)
July 2012 Bitcoinica Theft (305200 $)
Bitfloor Theft (248088 $)
Linode Hacks (230468 $)
Bitomat.pl Loss (236000 $)
Tony Silk Road Scam (150000 $)
Stefan Thomas Loss (128000 $)
Just-Dice.com Incident (121000 $)
Cdecker Theft (113894 $)
May 2012 Bitcoinica Hack (91306.46 $)
XBTGuild Incident (58737 $)
Bit LC Theft (51000 $)
Bitcoin7 Hack (50000 $)
June 2011 Mt. Gox Incident (46970.91 $)
BTC-E Hack (42000 $)
2012 Trojan (38000 $)
Mooncoin Theft (24000 $)
Betcoin Theft (15509 $)

Proof of Solvency

We *cannot* stop thefts

We *can* require exchanges' solvency to be proven

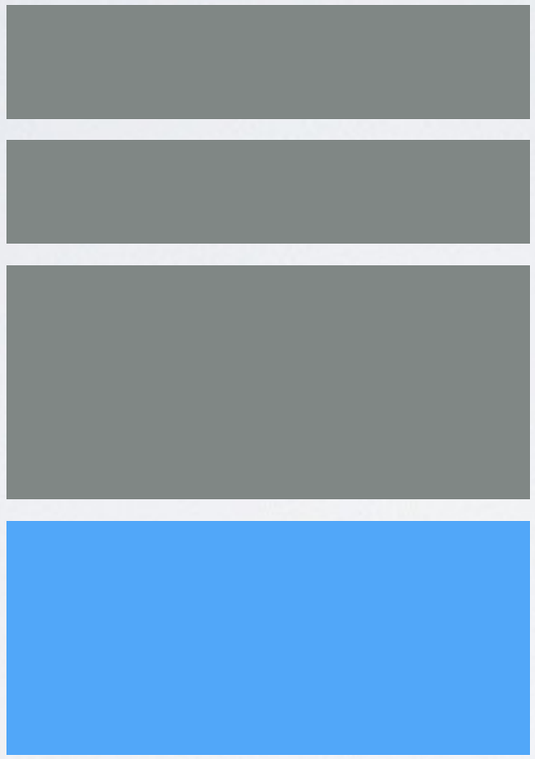
With some crypto, we can even prove solvency without revealing:

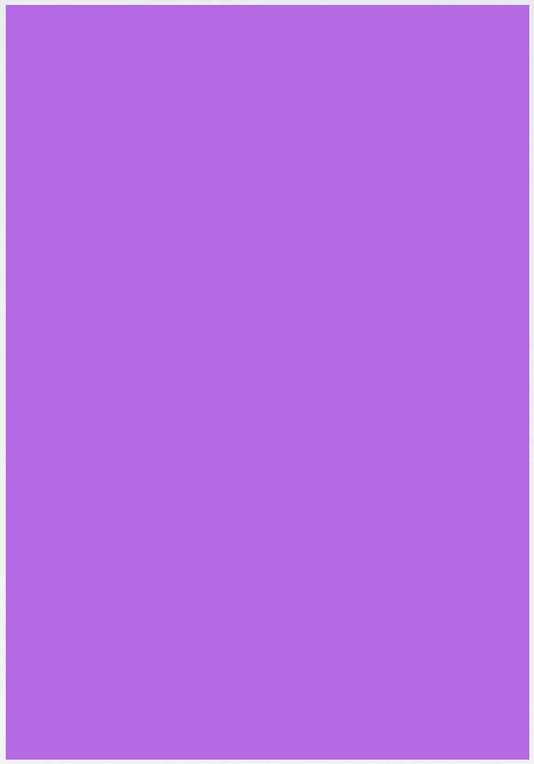
- Customer information
- Exchanges' total holdings
- Exchanges' addresses

Balance Sheet

Liabilities

Equity





Assets
(on blockchain)

Balance Sheet

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

Primitives

Special “encryption”:

- Given [[x]], [[y]] : compute [[x + y]]

Zero knowledge proofs:

- Given [[x]], prove it decrypts to x
- Given [[x]], prove x is a positive number
- Given [[x]], where x is a public key, prove knowledge of the signing private key

Precisely: Pedersen commitments w/ basic non-interactive sigma protocols

Sketch

[[Assets]]

Sketch

[[Assets]] [[Liabilities]]

Sketch

[[Assets]] - [[Liabilities]]

[[Assets - Liabilities]]

Sketch

[[Assets]] - [[Liabilities]]

[[Assets - Liabilities]]

[[0]]

Sketch

[[Assets]] - [[Liabilities]]

[[Assets - Liabilities]]

[[0]]

[[Liabilities]]

Alice	50
Bob	100
Carol	25

Private

[[Liabilities]]

Alice	50
Bob	100
Carol	25

Private

[[Alice]]	[[50]]	
[[Bob]]	[[100]]	
[[Carol]]	[[25]]	

Public

[[Liabilities]]

Alice	50
Bob	100
Carol	25

Private

[[Alice]]	[[50]]	
[[Bob]]	[[100]]	
[[Carol]]	[[25]]	
	[[Liabil]]	Total

Public

[[Liabilities]]

Alice	50
Bob	100
Carol	25

Private

[[Alice]]	[[50]]	
[[Bob]]	[[100]]	
[[Carol]]	[[25]]	
	[[Liabil]]	Total

Public

Bob only:

$rand_{[[Bob]]}$	$rand_{[[100]]}$

[[Liabilities]]

Alice	50
Bob	100
Carol	25

Private

[[Alice]]	[[50]]	
~~[[Bob]]~~	~~[[100]]~~	
[[Carol]]	[[25]]	

Public

Bob only:

$rand_{[[Bob]]}$	$rand_{[[100]]}$

[[Liabilities]]

Alice	50
Bob	100
Carol	25

Private

[[Alice]]	[[50]]	
[[Bob]]	[[0]]	
[[Carol]]	[[25]]	

Public

Bob only:

$rand_{[[Bob]]}$	$rand_{[[100]]}$

[[Liabilities]]

Alice	50
Bob	100
Carol	25

Private

[[Alice]]	[[50]]	
[[Bob]]	[[100]]	
[[Carol]]	[[25]]	
[[Eve]]	[[100]]	

Public

Bob only:

$rand_{[[Bob]]}$	$rand_{[[100]]}$

[[Liabilities]]

Alice	50
Bob	100
Carol	25

Private

[[Alice]]	[[50]]	
[[Bob]]	[[100]]	
[[Carol]]	[[25]]	
[[Eve]]	[[-100]]	

Public

Bob only:

$rand_{[[Bob]]}$	$rand_{[[100]]}$

[[Liabilities]]

Alice	50
Bob	100
Carol	25

Private

[[Alice]]	[[50]]	ZKP+
[[Bob]]	[[100]]	ZKP+
[[Carol]]	[[25]]	ZKP+
[[Eve]]	~~[[-100]]~~	

Public

Bob only:

$rand_{[[Bob]]}$	$rand_{[[100]]}$

[[Assets]]

PK_1	50
PK_2	75
PK_3	25
PK_4	100

Public
(Blockchain)

[[Assets]]

PK_1	50
PK_2	75
PK_3	25
PK_4	100

Public
(Blockchain)

$[[PK_2]]$	[[75]]
$[[PK_3]]$	[[25]]
$[[PK_4]]$	[[100]]
$[[PK_1]]$	[[50]]

Public

[[Assets]]

PK_1	50
PK_2	75
PK_3	25
PK_4	100

Public
(Blockchain)

$[[PK_2]]$	$[[75]]$
$[[PK_3]]$	$[[25]]$
$[[PK_4]]$	$[[100]]$
$[[PK_1]]$	$[[50]]$

Public

[[Assets]]

PK_1	50
PK_2	75
PK_3	25
PK_4	100

Public
(Blockchain)

$[[PK_2]]$	$[[75]]$
$[[PK_3]]$	$[[25]]$
$[[PK_4]]$	$[[100]]$
$[[PK_1]]$	$[[50]]$

Public

☜ ZKP: know SK_2 that corresponds to PK_2 inside of $[[PK_2]]$

☜ ZKP: know SK_4 that corresponds to PK_4 inside of $[[PK_4]]$

[[Assets]]

PK_1	50
PK_2	75
PK_3	25
PK_4	100

Public
(Blockchain)

$[[PK_2]]$	$[[75]]$
$[[PK_3]]$	$[[25]]$
$[[PK_4]]$	$[[100]]$
$[[PK_1]]$	$[[50]]$

Public

☜ ZKP: know SK_2 that corresponds to PK_2 inside of $[[PK_2]]$

☜ ZKP: know SK_4 that corresponds to PK_4 inside of $[[PK_4]]$

[[Assets]]

PK_1	50
PK_2	75
PK_3	25
PK_4	100

Public
(Blockchain)

[[PK_2]]	[[75]]
[[PK_3]]	[[25]]
[[PK_4]]	[[100]]
[[PK_1]]	[[50]]

Public

[[Assets]]

PK_1	50
PK_2	75
PK_3	25
PK_4	100

Public
(Blockchain)

[[PK_2]]	[[75]]
[[PK_4]]	[[100]]

Public

[[Assets]]
=[[75]]+[[100]]

[[Assets]] (Method 2)

PK_1	50
PK_2	75
PK_3	25
PK_4	100

Public
(Blockchain)

[[Assets]] (Method 2)

PK_1	50
PK_2	75
PK_3	25
PK_4	100

Public
(Blockchain)

$[[SK_1]]$	[[50]]
$[[SK_2]]$	[[75]]
$[[SK_3]]$	[[25]]
$[[SK_4]]$	[[100]]

Public

[[Assets]] (Method 2)

[[SK_1]]	[[50]]
[[SK_2]]	[[75]]
[[SK_3]]	[[25]]
[[SK_4]]	[[100]]

Public

[[Assets]] (Method 2)

[[SK_1]]	[[50]]
[[SK_2]]	[[75]]
[[SK_3]]	[[25]]
[[SK_4]]	[[100]]

Public

[[0]]
[[1]]
[[0]]
[[1]]

Selection

[[0]]	[[0]]
[[SK_2]]	[[75]]
[[0]]	[[0]]
[[SK_4]]	[[100]]

[[Assets]] (Method 2)

[[SK_1]]	[[50]]
[[SK_2]]	[[75]]
[[SK_3]]	[[25]]
[[SK_4]]	[[100]]

Public

[[0]]
[[1]]
[[0]]
[[1]]

Selection

[[0]]	[[0]]
[[SK_2]]	[[75]]
[[0]]	[[0]]
[[SK_4]]	[[100]]

ZKP: Each is 0 or 1

[[Assets]] (Method 2)

[[SK_1]]	[[50]]
[[SK_2]]	[[75]]
[[SK_3]]	[[25]]
[[SK_4]]	[[100]]

Public

[[0]]
[[1]]
[[0]]
[[1]]

Selection

[[0]]	[[0]]
[[SK_2]]	[[75]]
[[0]]	[[0]]
[[SK_4]]	[[100]]

Commitment
Consistent

ZKP: [[X]],[[bit]] → $[[X]]^{bit} = [[X*bit]]$

[[Assets]] (Method 2)

[[SK_1]]	[[50]]
[[SK_2]]	[[75]]
[[SK_3]]	[[25]]
[[SK_4]]	[[100]]

Public

[[0]]
[[1]]
[[0]]
[[1]]

Selection

[[0]]	[[0]]
[[SK_2]]	[[75]]
[[0]]	[[0]]
[[SK_4]]	[[100]]

Proof of Knowledge

ZKP: know SKi for all [[SKi]] and [[0]]

[[Assets]] (Method 2)

[[SK_1]]	[[50]]
[[SK_2]]	[[75]]
[[SK_3]]	[[25]]
[[SK_4]]	[[100]]

Public

[[0]]
[[1]]
[[0]]
[[1]]

Selection

[[0]]	[[0]]
[[SK_2]]	[[75]]
[[0]]	[[0]]
[[SK_4]]	[[100]]

[[Assets]]
=[[75]]+[[100]]

Recall

[[Assets]] - [[Liabilities]]

[[Assets - Liabilities]]

[[0]]

Verifiably decrypt

0

Recall

[[Assets]] - [[Liabilities]] - [[Equity]]

[[Assets - Liabilities - Equity]]

ZKP+

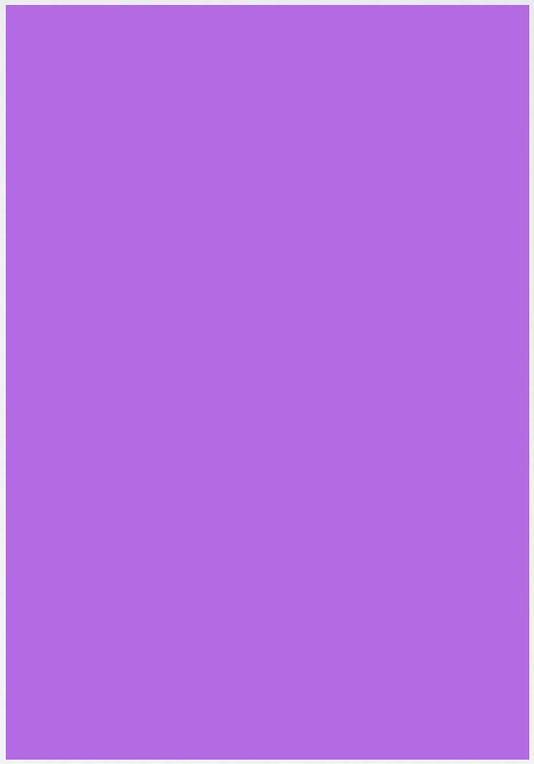
[[0]]

Verifiably decrypt

0

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

Equity: encrypted amount that is zero or positive 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]] - [[Equity]] = 0

Remarks

Proof of liability is a bit more complicated to hide the number addresses held by the exchange:

1. Exchange commits to bit vector of owned addresses
2. ZKP it is a bit vector
3. Multiplies it in to vector of public keys and proves knowledge of each
4. Multiplies *the same* vector into a vector of balances, adds them

Implementation

- I take zero credit for this :)

- Proof of Assets: Anonymity set of 500K
  - 10s of minutes to construct proof
  - 1 hour to verify
  - 1 GB proof size

- Proof of Liabilities: 1M users
  - 2 hours to construct
  - 5 GB

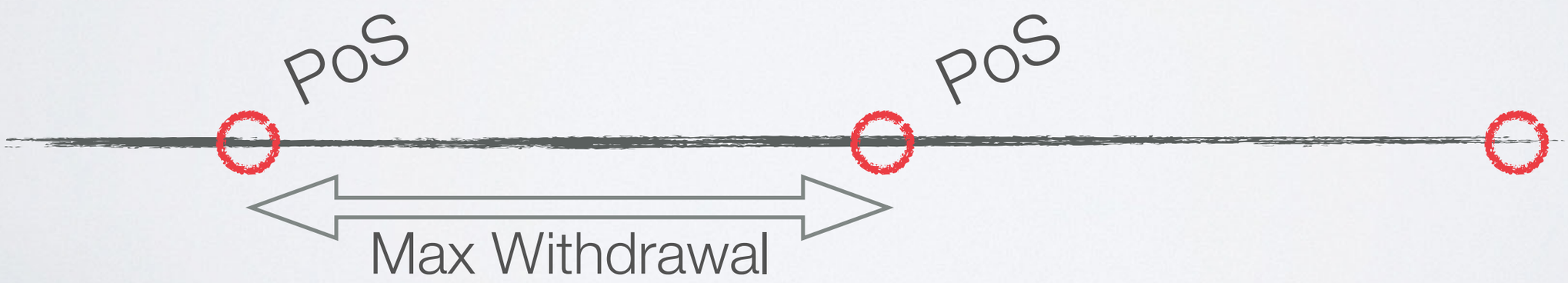
Limitations

- Proof of solvency is “detection” not “prevention”
- Multiple insolvent exchanges might collude to pool their resources together -> see paper
- Proof of Assets can only include transactions that a redeemable by a known public key

Idea: Limited Liability

1) Proof of Solvencies — snapshot in time

2) Bitcoin covenants — slow theft down



Questions?

@PulpSpy