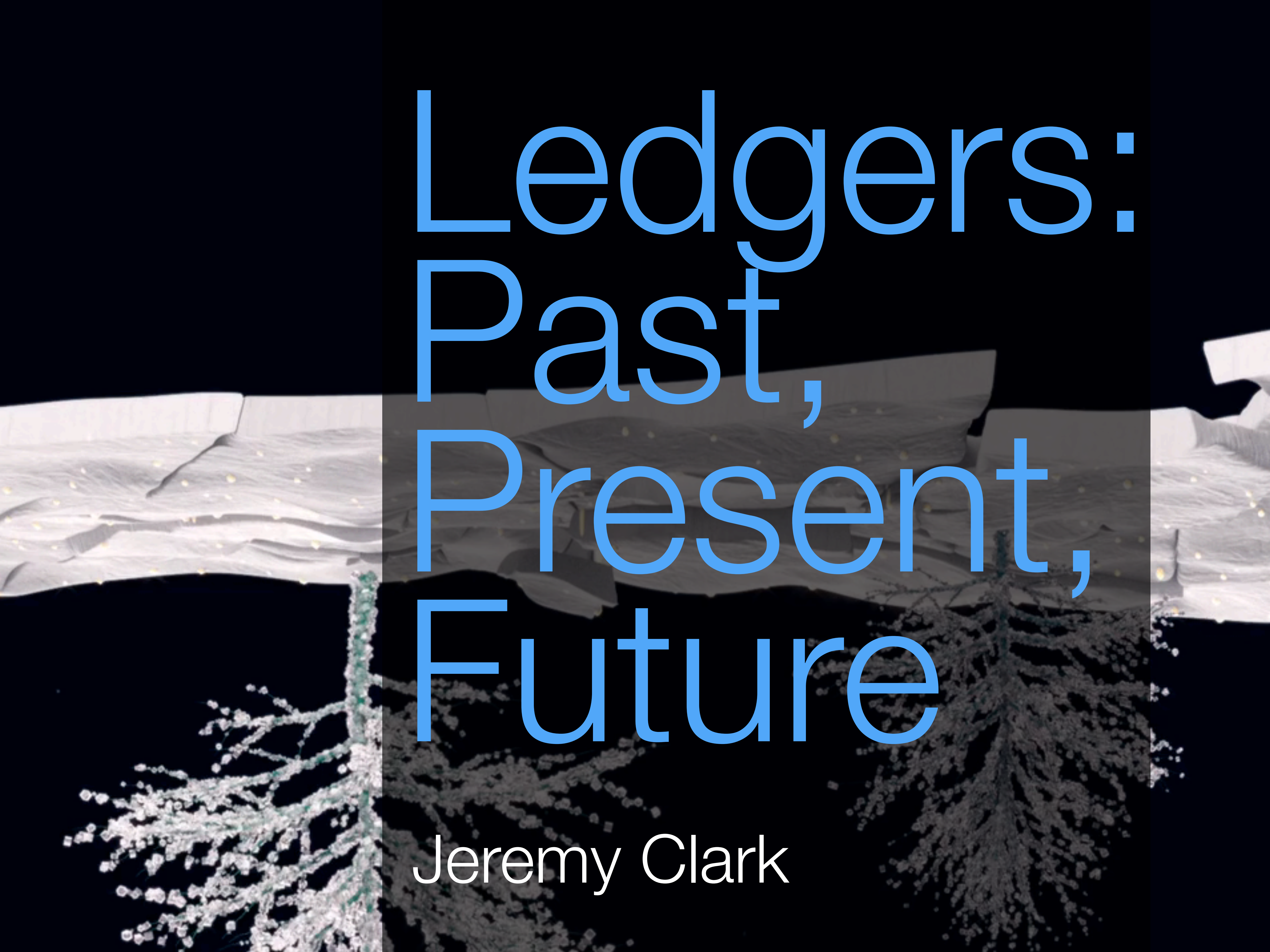
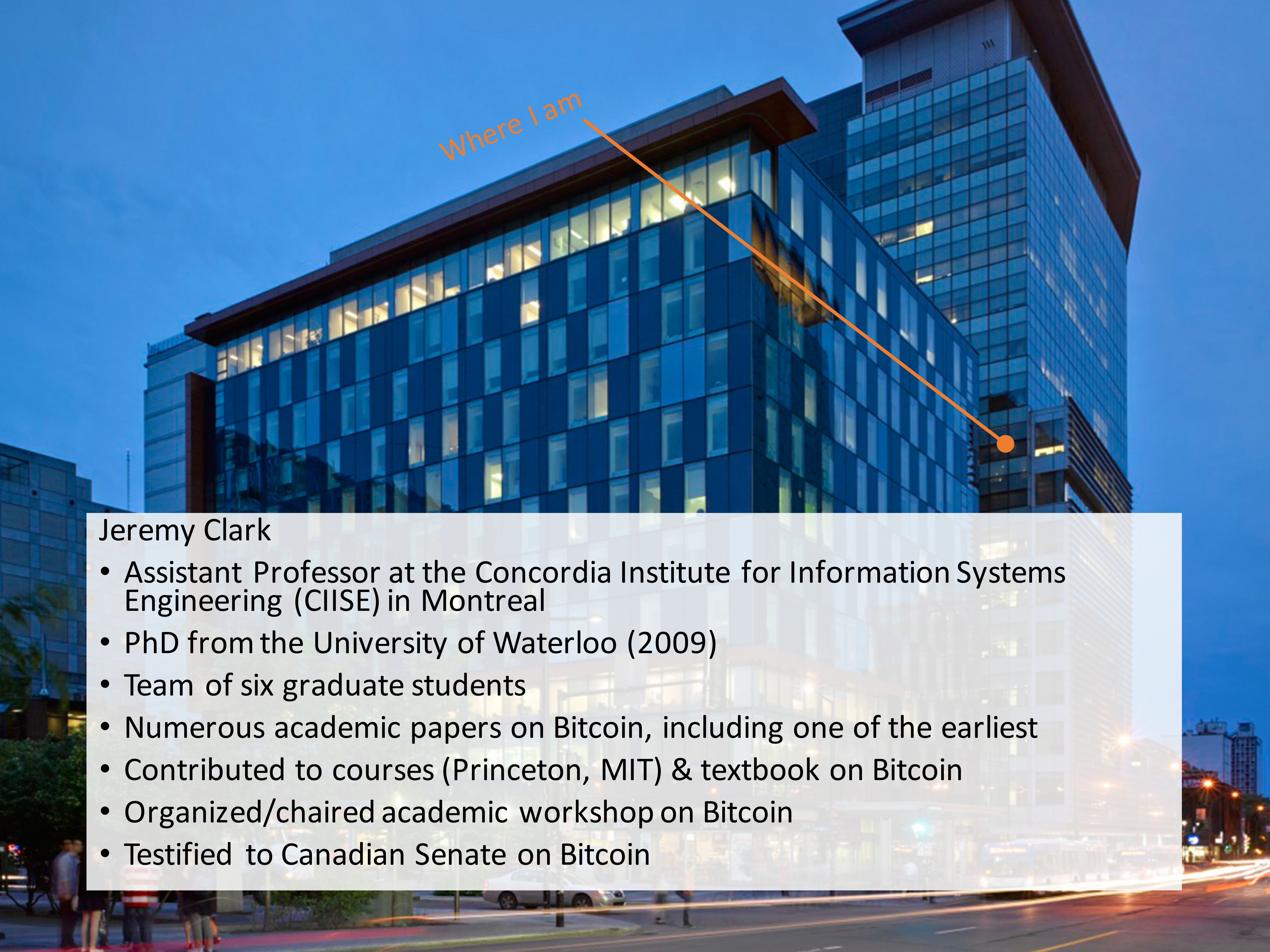


Ledgers: Past, Present, Future

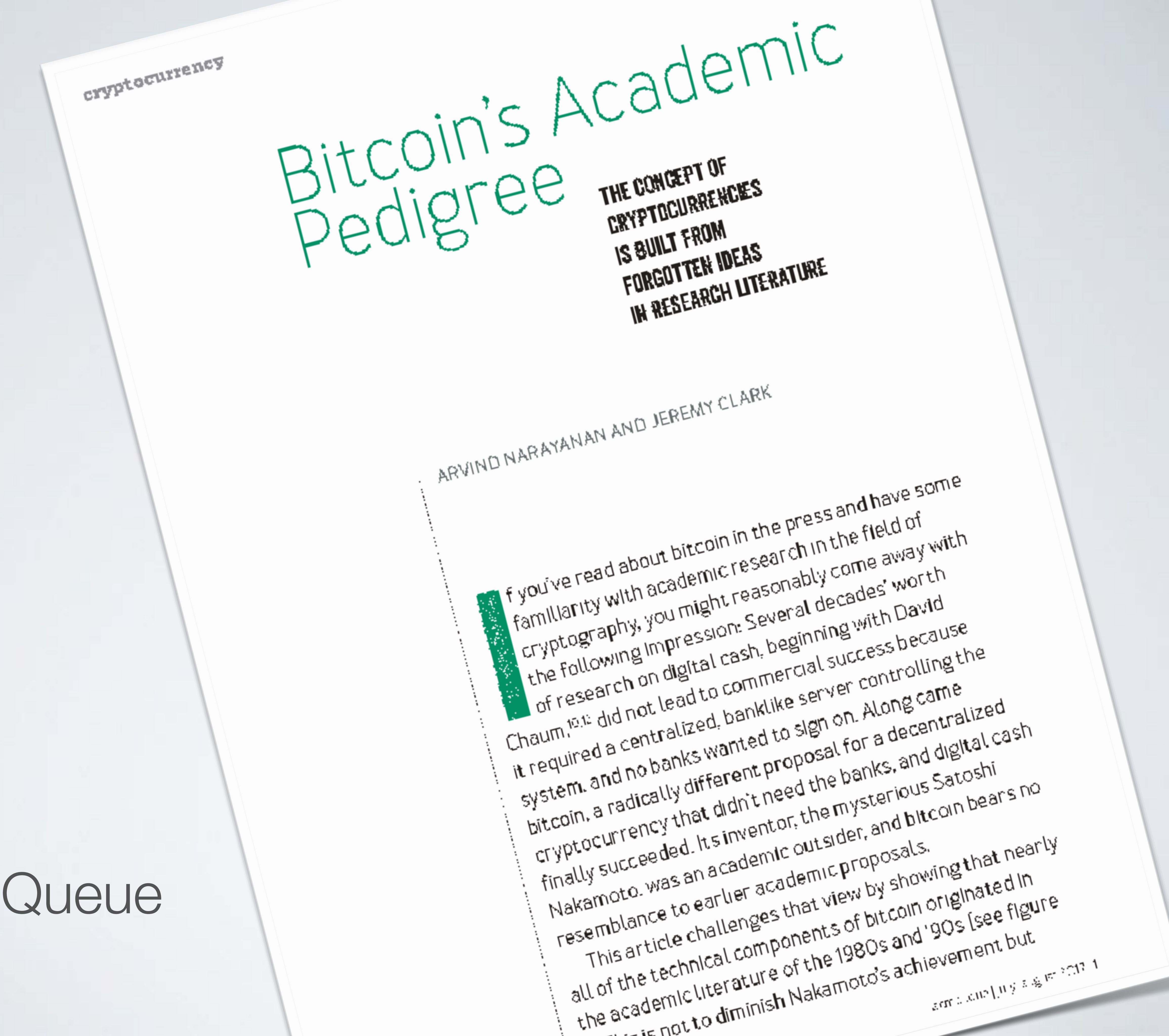
Jeremy Clark



Where I am

Jeremy Clark

- Assistant Professor at the Concordia Institute for Information Systems Engineering (CIISE) in Montreal
- PhD from the University of Waterloo (2009)
- Team of 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



cryptocurrency

Bitcoin's Academic Pedigree

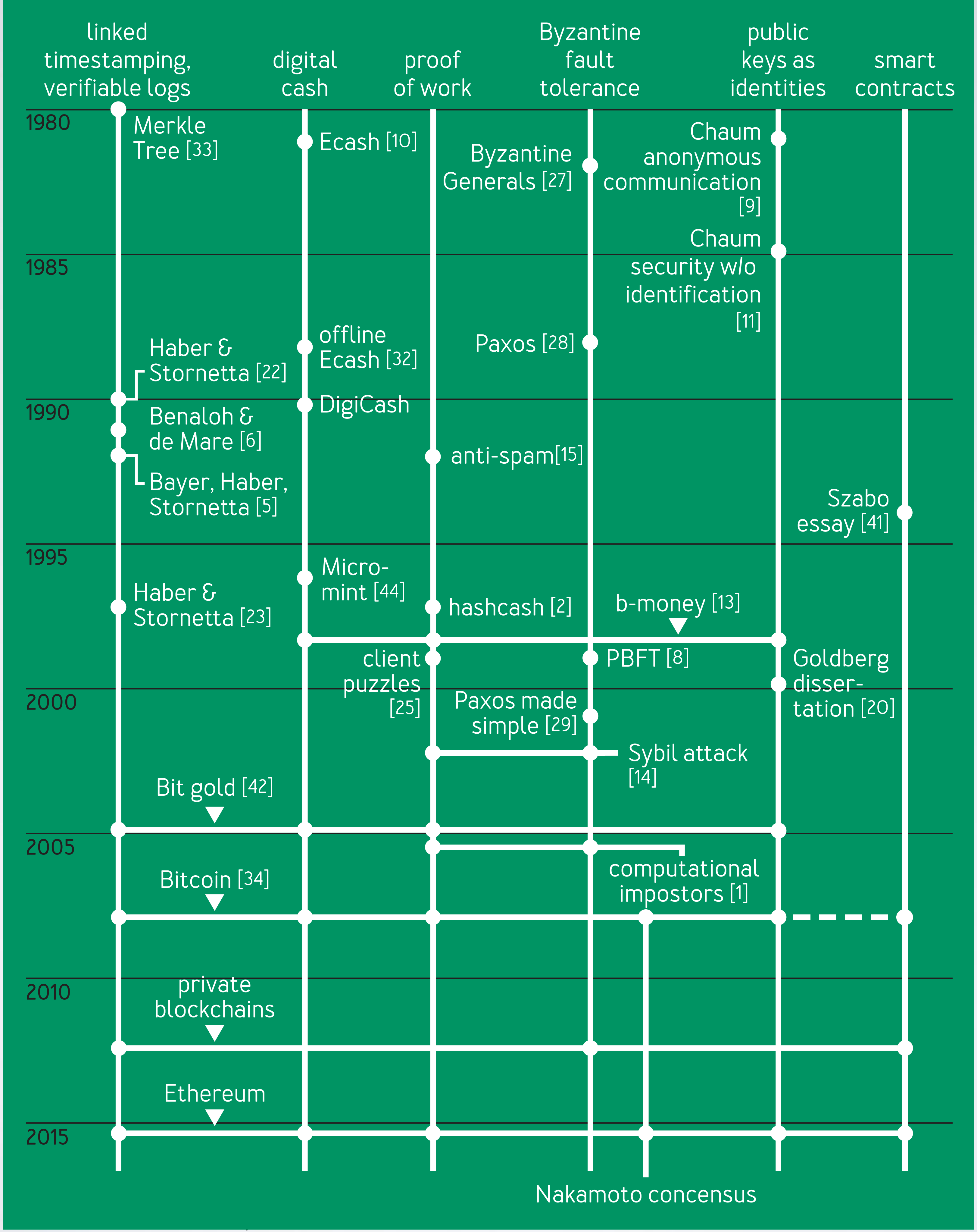
THE CONCEPT OF CRYPTOCURRENCIES IS BUILT FROM FORGOTTEN IDEAS IN RESEARCH LITERATURE

ARVIND NARAYANAN AND JEREMY CLARK

If you've read about bitcoin in the press and have some familiarity with academic research in the field of cryptography, you might reasonably come away with the following impression: Several decades' worth of research on digital cash, beginning with David Chaum,[10,12] did not lead to commercial success because it required a centralized, banklike server controlling the system, and no banks wanted to sign on. Along came bitcoin, a radically different proposal for a decentralized cryptocurrency that didn't need the banks, and digital cash finally succeeded. Its inventor, the mysterious Satoshi Nakamoto, was an academic outsider, and bitcoin bears no resemblance to earlier academic proposals.

This article challenges that view by showing that nearly all of the technical components of bitcoin originated in the academic literature of the 1980s and '90s (see figure This is not to diminish Nakamoto's achievement but

ACM Queue



linked timestamping, verifiable logs

digital cash

proof of work

Byzantine fault tolerance

public keys as identities

smart contracts

1980

Merkle Tree [33]

Ecash [10]

Chaum anonymous communication [9]

Byzantine Generals [27]

Chaum security w/o identification [11]

1985

Haber & Stornetta [22]

offline Ecash [32]

Paxos [28]

DigiCash

1990

Benaloh & de Mare [6]

anti-spam[15]

Bayer, Haber, Stornetta [5]

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

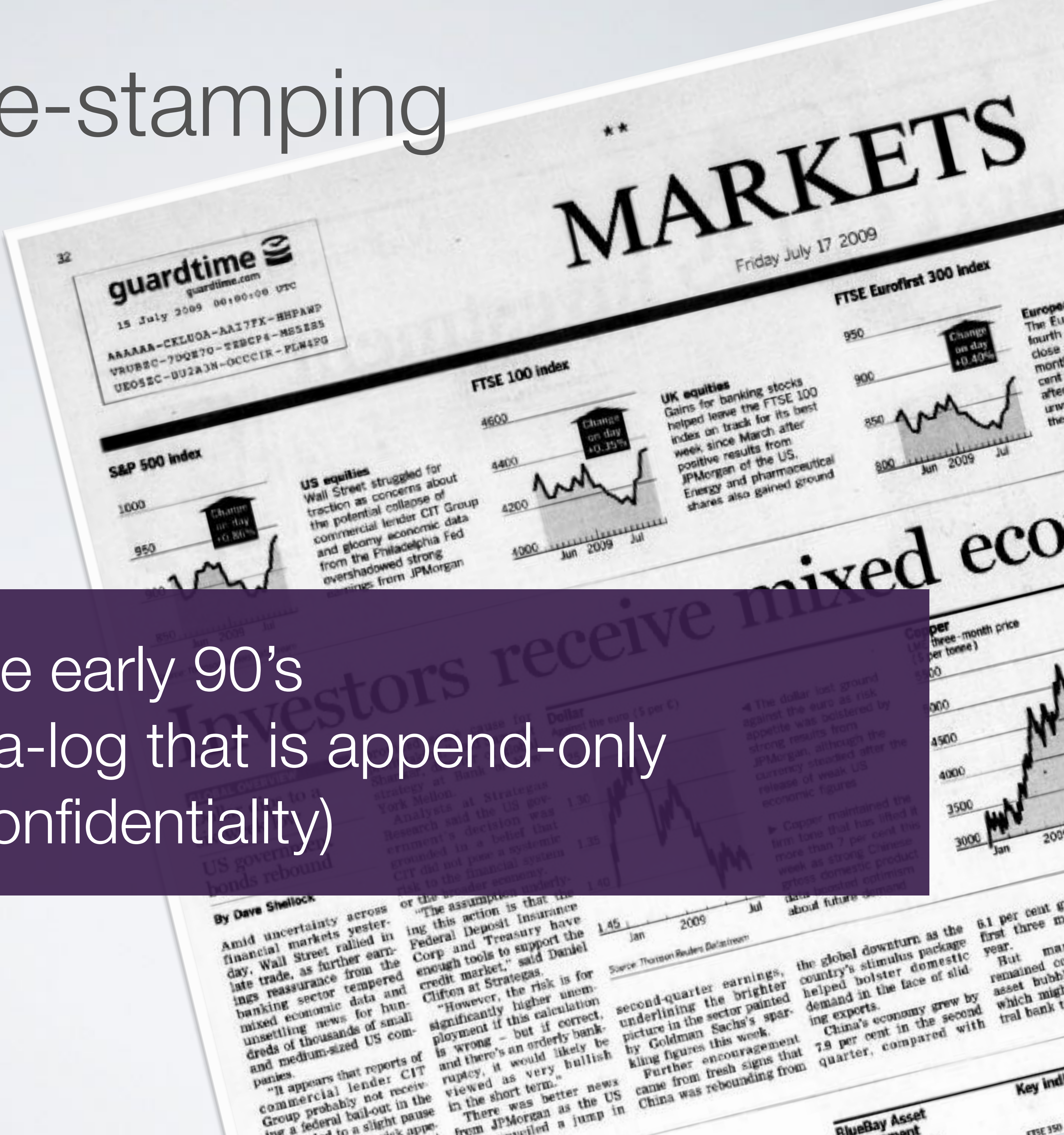
2015

Nakamoto concensus

Ledgers

Used historically to record credits
Eventually augmented with coins

Linked time-stamping



32

guardtime
guardtime.com
15 July 2009 00:00:00 UTC
AAAAAA-CKLUOA-AAI7FX-HHPAWP
VRUBZC-7DQE7O-TEBCP6-MB5EB5
UEOSZC-DU2A3N-OCCCIR-PLN4PG

**

MARKETS

Friday July 17 2009

S&P 500 index
1000
950
900
850
Change on day +0.86%
Jun 2009 Jul

US equities
Wall Street struggled for traction as concerns about the potential collapse of commercial lender CIT Group and gloomy economic data from the Philadelphia Fed overshadowed strong earnings from JPMorgan

UK equities
Gains for banking stocks helped leave the FTSE 100 index on track for its best week since March after positive results from JPMorgan of the US. Energy and pharmaceutical shares also gained ground

Europe
The Eu
fourth
close
mont
cent
after
unw
the

Investors receive mixed eco

US government bonds rebound

By Dave Shellock

Amid uncertainty across financial markets yesterday, Wall Street rallied in late trade, as further earnings reassurance from the banking sector tempered mixed economic data and unsettling news for hundreds of thousands of small and medium-sized US companies.

"It appears that reports of commercial lender CIT Group probably not receiving a federal bail-out in the

Analysts at Strategas Research said the US government's decision was grounded in a belief that CIT did not pose a systemic risk to the financial system or the broader economy.

"The assumption underlying this action is that the Federal Deposit Insurance Corp and Treasury have enough tools to support the credit market," said Daniel Clifton at Strategas.

"However, the risk is for significantly higher unemployment if this calculation is wrong – but if correct, and there's an orderly bankruptcy, it would likely be viewed as very bullish in the short term."

There was better news from JPMorgan as the US

second-quarter earnings, underlining the brighter picture in the sector painted by Goldman Sachs's sparkling figures this week.

Further encouragement came from fresh signs that China was rebounding from the global downturn as the country's stimulus package helped bolster domestic demand in the face of sliding exports.

China's economy grew by 7.9 per cent in the second quarter, compared with 6.1 per cent g first three m year.

But mar remained co asset bubb which migh tral bank t

Source: Thomson Reuters Datastream

◀ The dollar lost ground against the euro as risk appetite was bolstered by strong results from JPMorgan, although the currency steadied after the release of weak US economic figures

▶ Copper maintained the firm tone that has lifted it more than 7 per cent this week as strong Chinese gross domestic product data boosted optimism about future demand

Key ind

BlueBay Asset Management

Proposed in the early 90’s
Provides a data-log that is append-only
Integrity (not confidentiality)

Digital Cash

Proposed in the 1980s
Much interest in the 90s

ACC
Agora
AIMP
Allopass
b-money
BankNet
Bitbit
Bitgold
Bitpass
C-SET
CAFÉ
CheckFree
ClickandBuy
ClickShare
ComerceNet
CommercePOINT
CommerceSTAGE
Cybank
CyberCash
CyberCents
CyberCoin
CyberGold
DigiGold

Digigold
Digital Silk Road
e-Comm
E-Gold
Ecash
eCharge
eCoin
Edd
eVend
First Virtual
FSTC Electronic
Check
Geldkarte
Globe Left
Hashcash
HINDE
iBill
iKP
IMB-MP
InterCoin
Ipin
Javien
Karma

LotteryTickets
Lucre
MagicMoney
Mandate
MicroMint
Micromoney
MilliCent
Mini-Pay
Minitix
MobileMoney
Mojo
Mollie
Mondex
MPTP
Net900
NetBill
NetCard
NetCash
NetCheque
NetFare
No3rd
One Click Charge
PayMe

PayNet
PayPal
PaySafeCard
PayTrust
PayWord
Peppercoin
PhoneTicks
Playspan
Polling
Proton
Redi-Charge
S/PAY
Sandia Lab E-Cash
Secure Courier
Semopo
SET
SET2Go
SubScrip
Trivnet
TUB
Twitpay
VeriFone

VisaCash
Wallie
Way2Pay
WorldPay
X-Pay

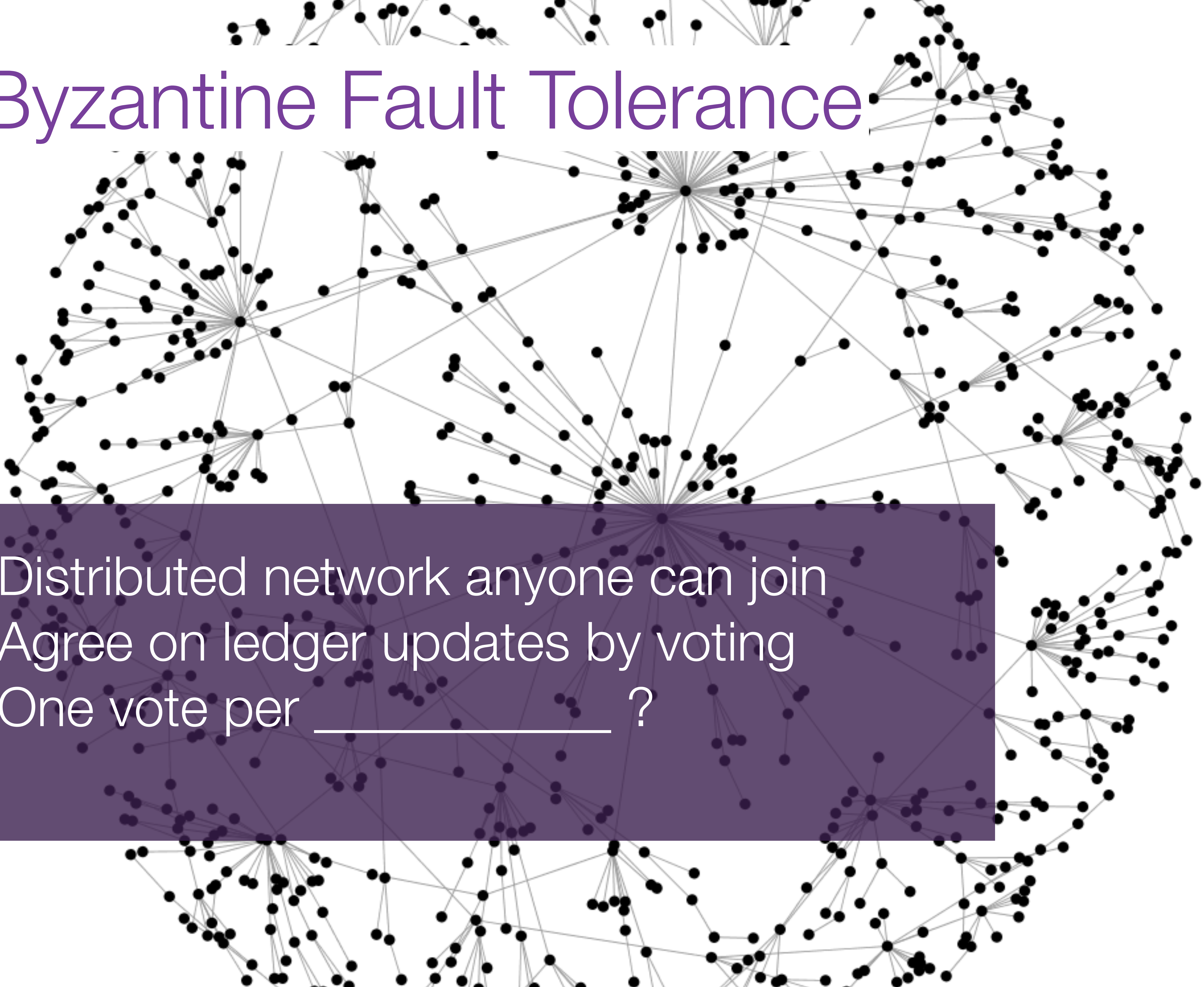
Digital Cash

0.30519173 BTC

Total Transactions	4
Total Received	0.50519173 BTC
Total Sent	0.20 BTC
Final Balance	0.30519173 BTC

Proposed in the 1980s
Much interest in the 90s
Traditionally focused on digital coins
Bitcoin: ledger-based money

Byzantine Fault Tolerance



Distributed network anyone can join

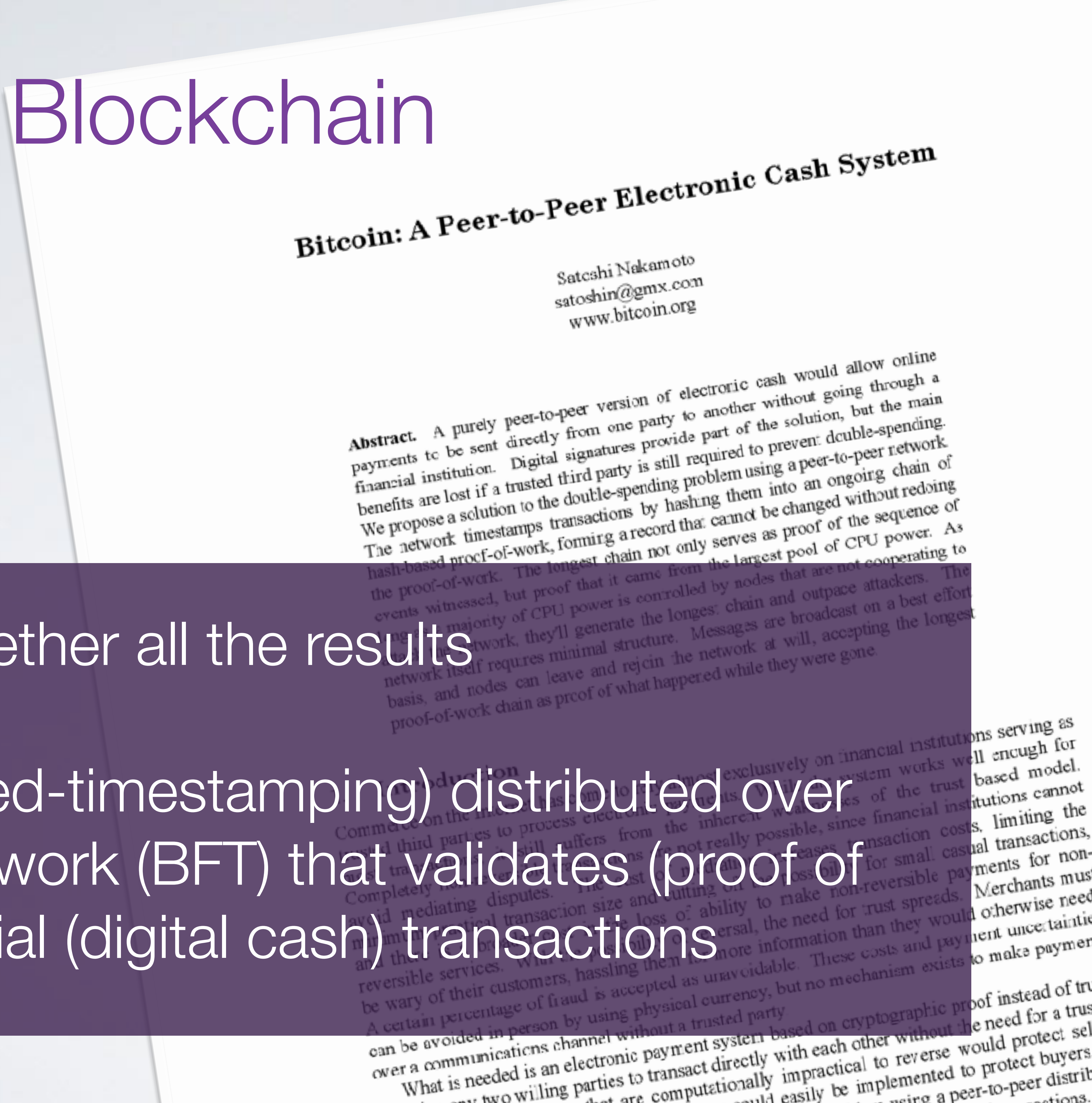
Agree on ledger updates by voting

One vote per _____________ ?

Proof of work

An amount of computational effort
Postage stamp for email
Voting in an open network

Bitcoin’s Blockchain



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants mus be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertaintie can be avoided in person by using physical currency, but no mechanism exists to make paymen over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of tru any two willing parties to transact directly with each other without the need for a trus that are computationally impractical to reverse would protect sel could easily be implemented to protect buyers using a peer-to-peer distrib

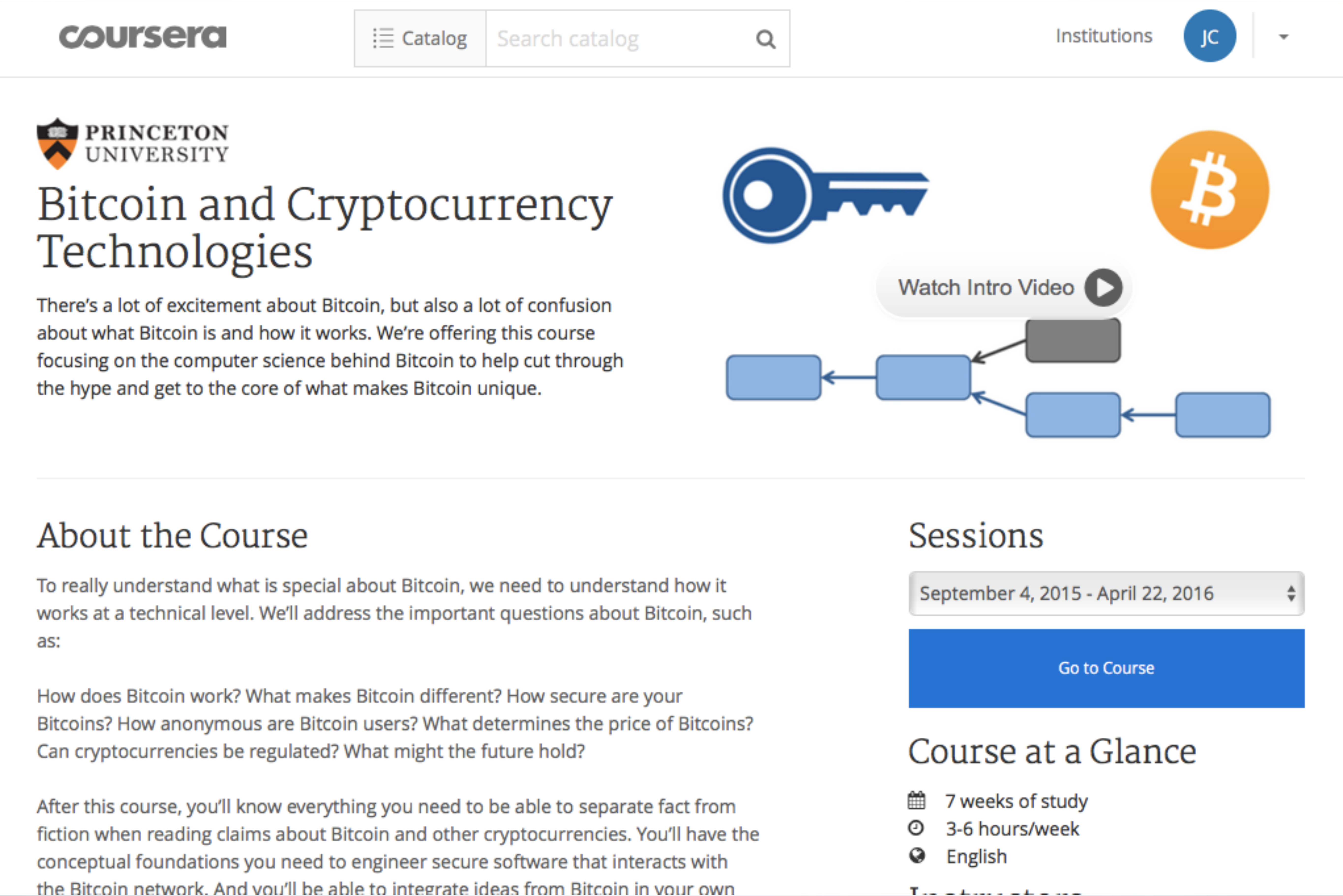
Weaves together all the results

Ledger (linked-timestamping) distributed over an open network (BFT) that validates (proof of work) financial (digital cash) transactions

Future Distributed Ledgers

Ledgers for running code (smart contracts)
Remove the proof of work (permissioned)
Layering on confidentiality

More resources



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?

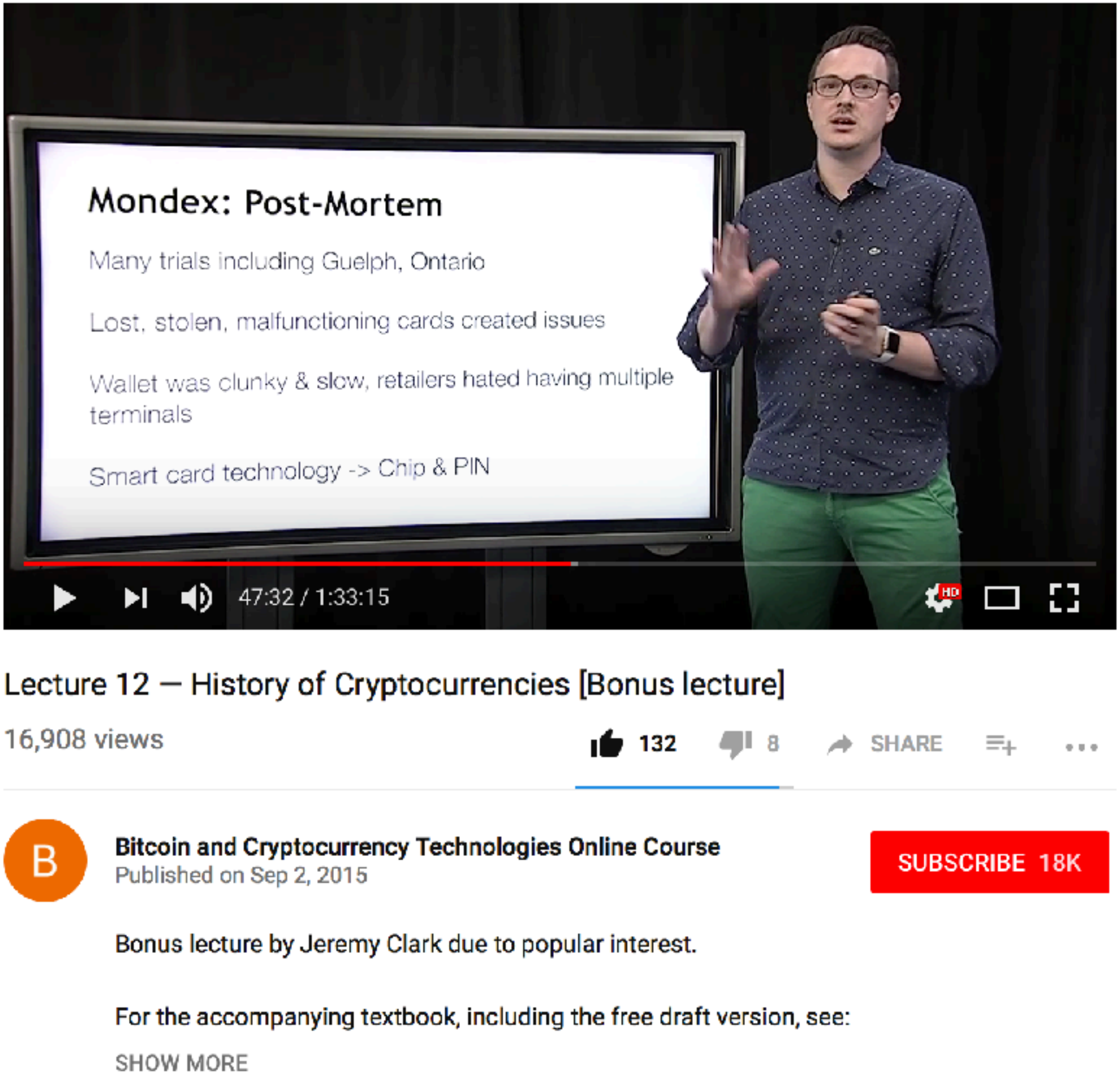
After this course, you'll know everything you need to be able to separate fact from fiction when reading claims about Bitcoin and other cryptocurrencies. You'll have the conceptual foundations you need to engineer secure software that interacts with the Bitcoin network. And you'll be able to integrate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



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]

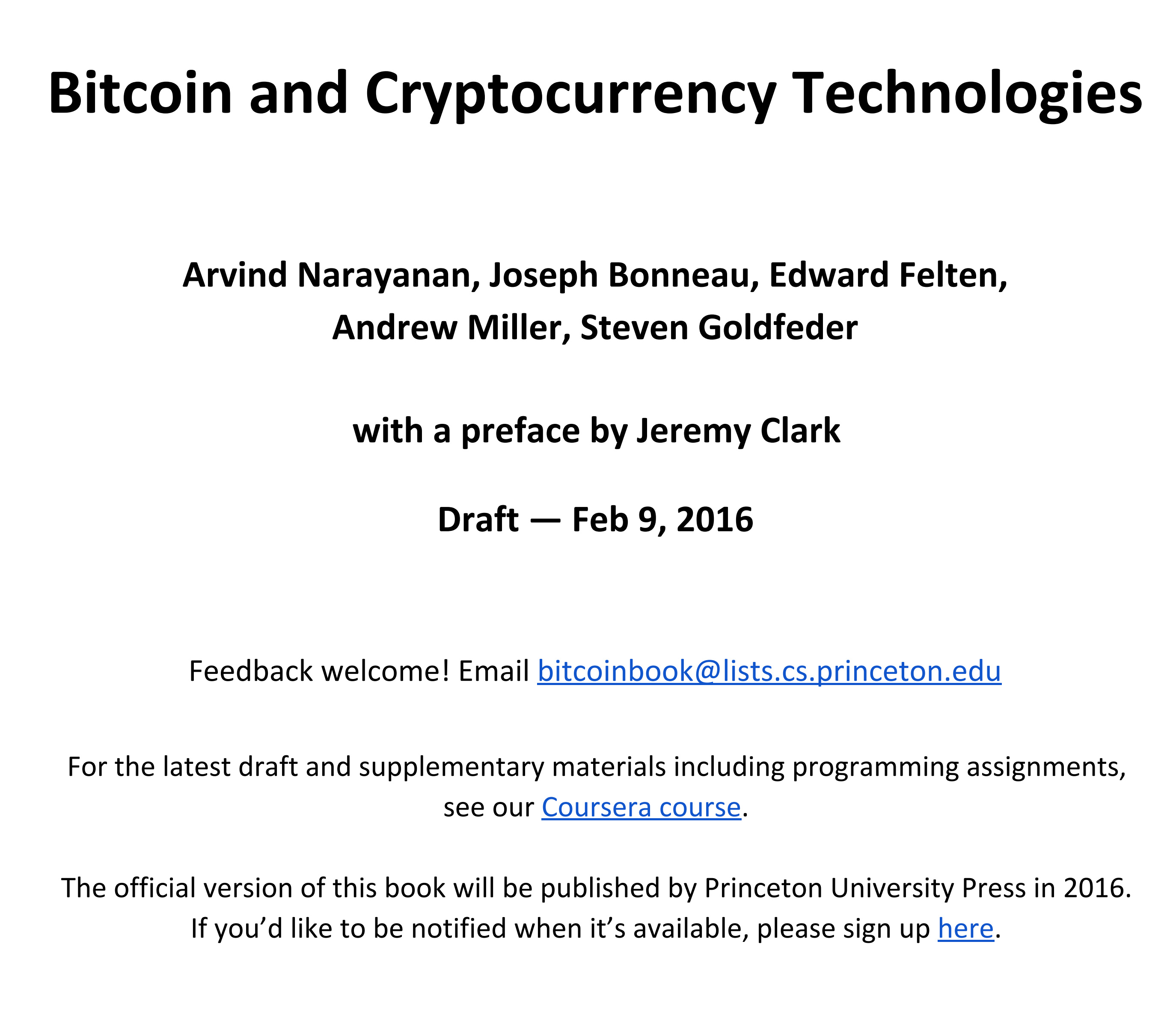
16,908 views

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

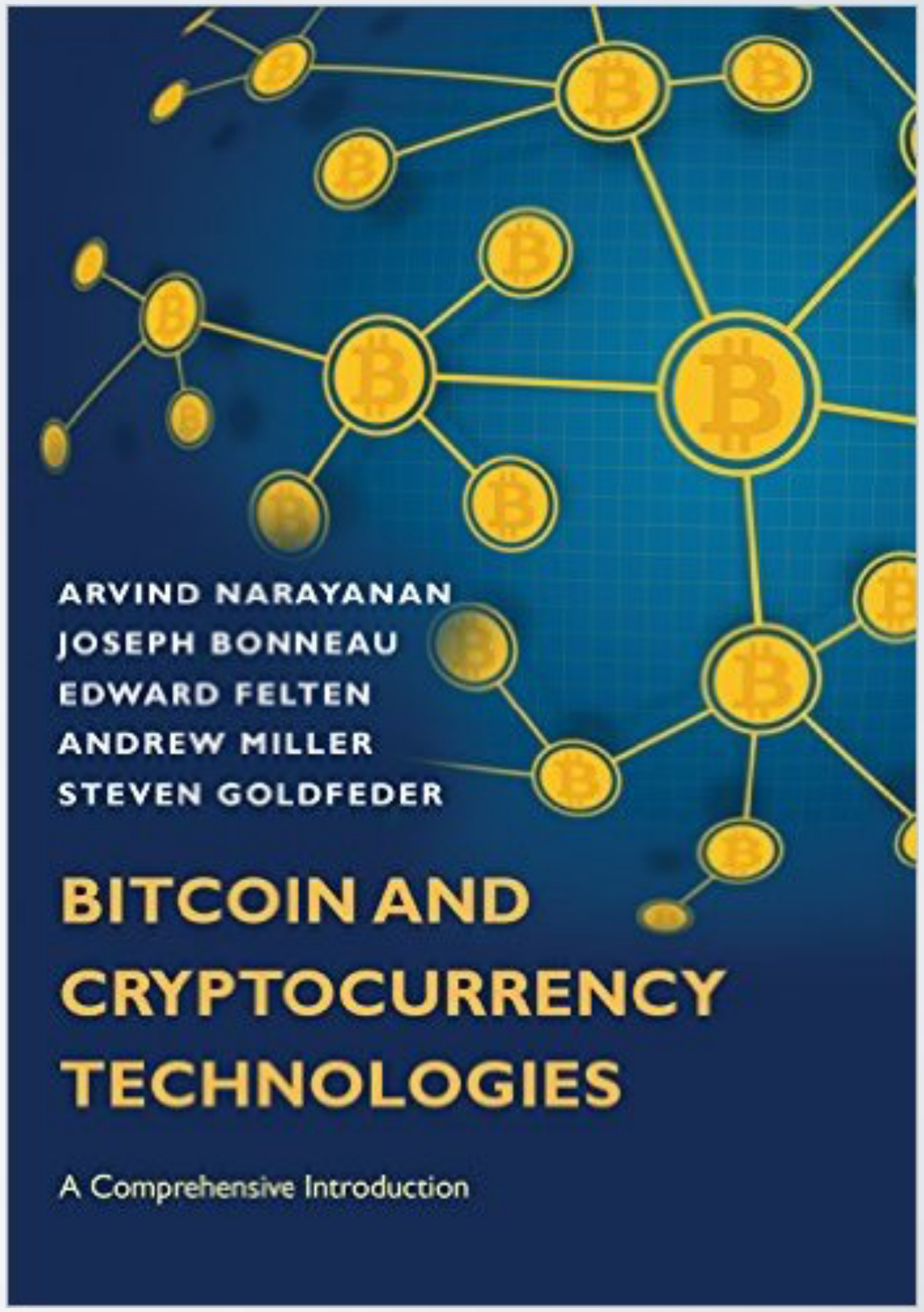
with a preface by Jeremy Clark

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.

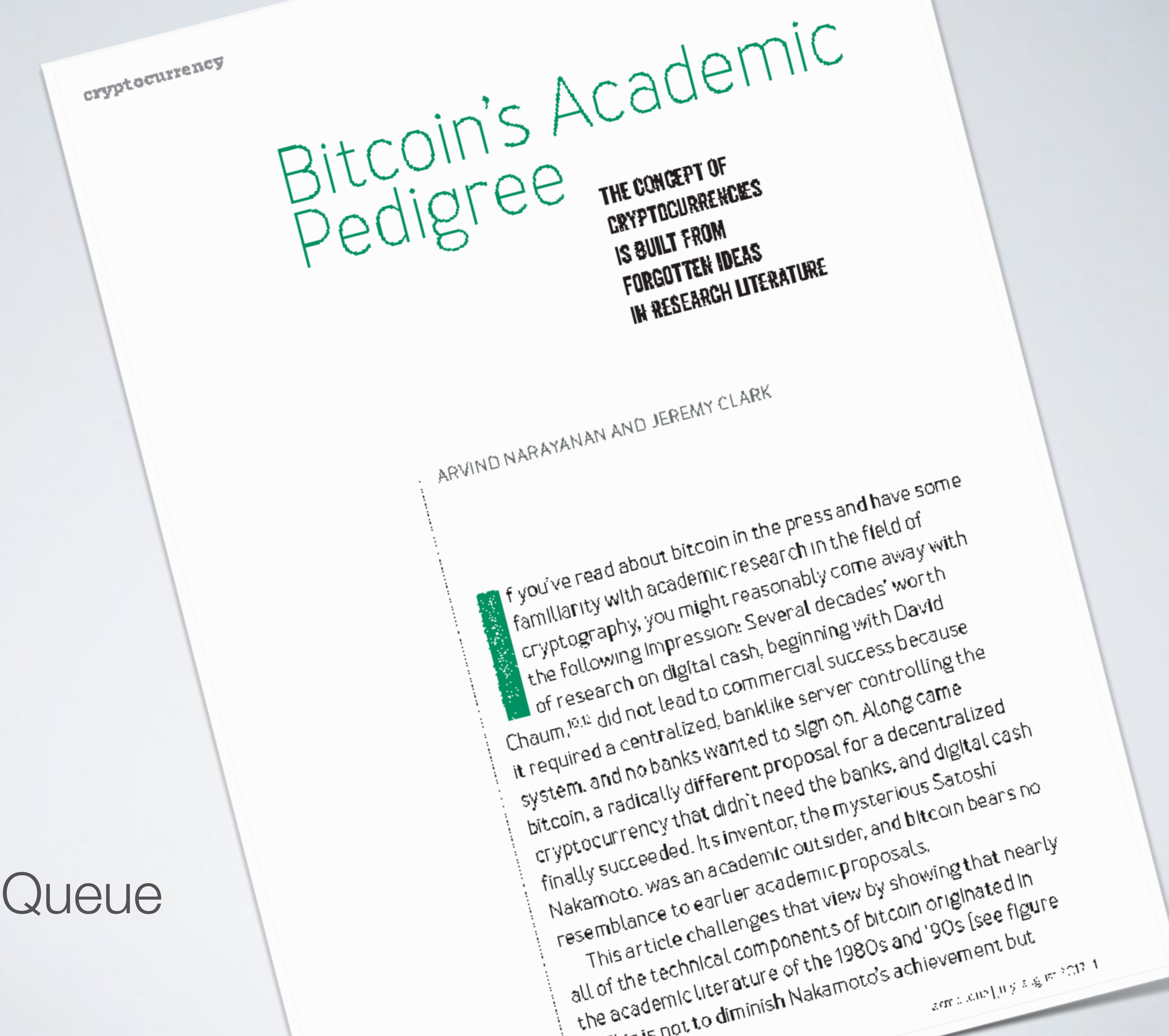
The official version of this book will be published by Princeton University Press in 2016. If you'd like to be notified when it's available, please sign up here.



ARVIND NARAYANAN
JOSEPH BONNEAU
EDWARD FELTEN
ANDREW MILLER
STEVEN GOLDFEDER

BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES

A Comprehensive Introduction



cryptocurrency

Bitcoin's Academic Pedigree

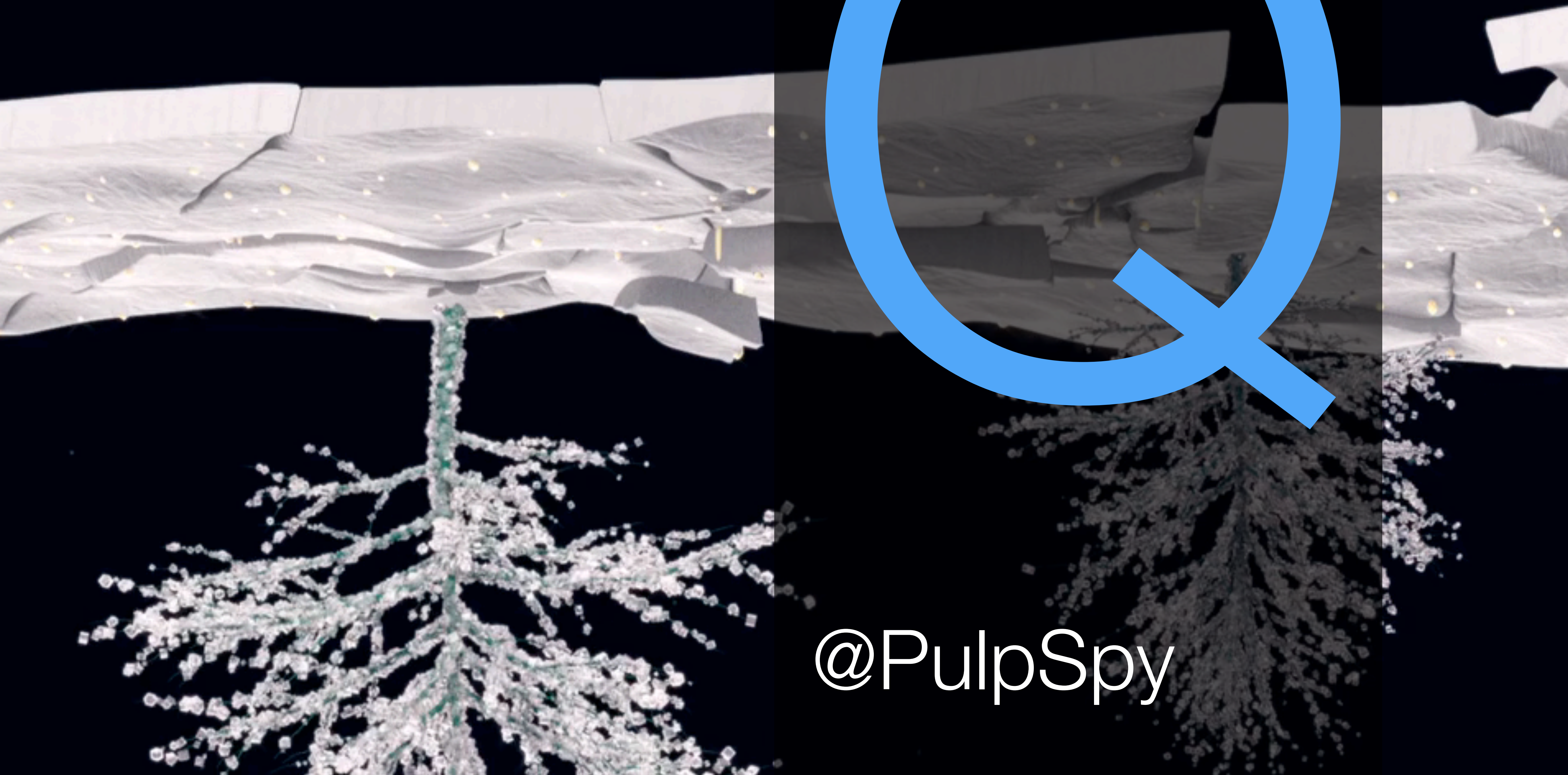
THE CONCEPT OF CRYPTOCURRENCIES IS BUILT FROM FORGOTTEN IDEAS IN RESEARCH LITERATURE

ARVIND NARAYANAN AND JEREMY CLARK

If you've read about bitcoin in the press and have some familiarity with academic research in the field of cryptography, you might reasonably come away with the following impression: Several decades' worth of research on digital cash, beginning with David Chaum,[10,12] did not lead to commercial success because it required a centralized, banklike server controlling the system, and no banks wanted to sign on. Along came bitcoin, a radically different proposal for a decentralized cryptocurrency that didn't need the banks, and digital cash finally succeeded. Its inventor, the mysterious Satoshi Nakamoto, was an academic outsider, and bitcoin bears no resemblance to earlier academic proposals.

This article challenges that view by showing that nearly all of the technical components of bitcoin originated in the academic literature of the 1980s and '90s (see figure 1). This is not to diminish Nakamoto's achievement but

ACM Queue



Q

@PulpSpy