



Blockchains & Voting An Assessment & Critique

Jeremy Clark, Concordia University

A photograph of a modern glass skyscraper at night. The building's windows are illuminated from within, reflecting the city lights. An orange arrow originates from the text 'Where I am' and points to a specific window on the building's facade. The sky is a deep blue, and the city street in the foreground is visible with some light trails from traffic.

Where I am

- 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
- Academic publications, textbooks, editorial positions on both verifiable voting & blockchain
- Part of team deploying verifiable voting (in-person/remote) for the first time in governmental elections
- Worked with various municipalities (Takoma Park, Toronto, Edmonton...) on secure voting
- Worked with government on Bitcoin/blockchain (Bank of Canada, RCMP, Fintrac, Industry Canada, ...)
- Contributed to courses (Princeton, MIT) on Bitcoin/blockchain

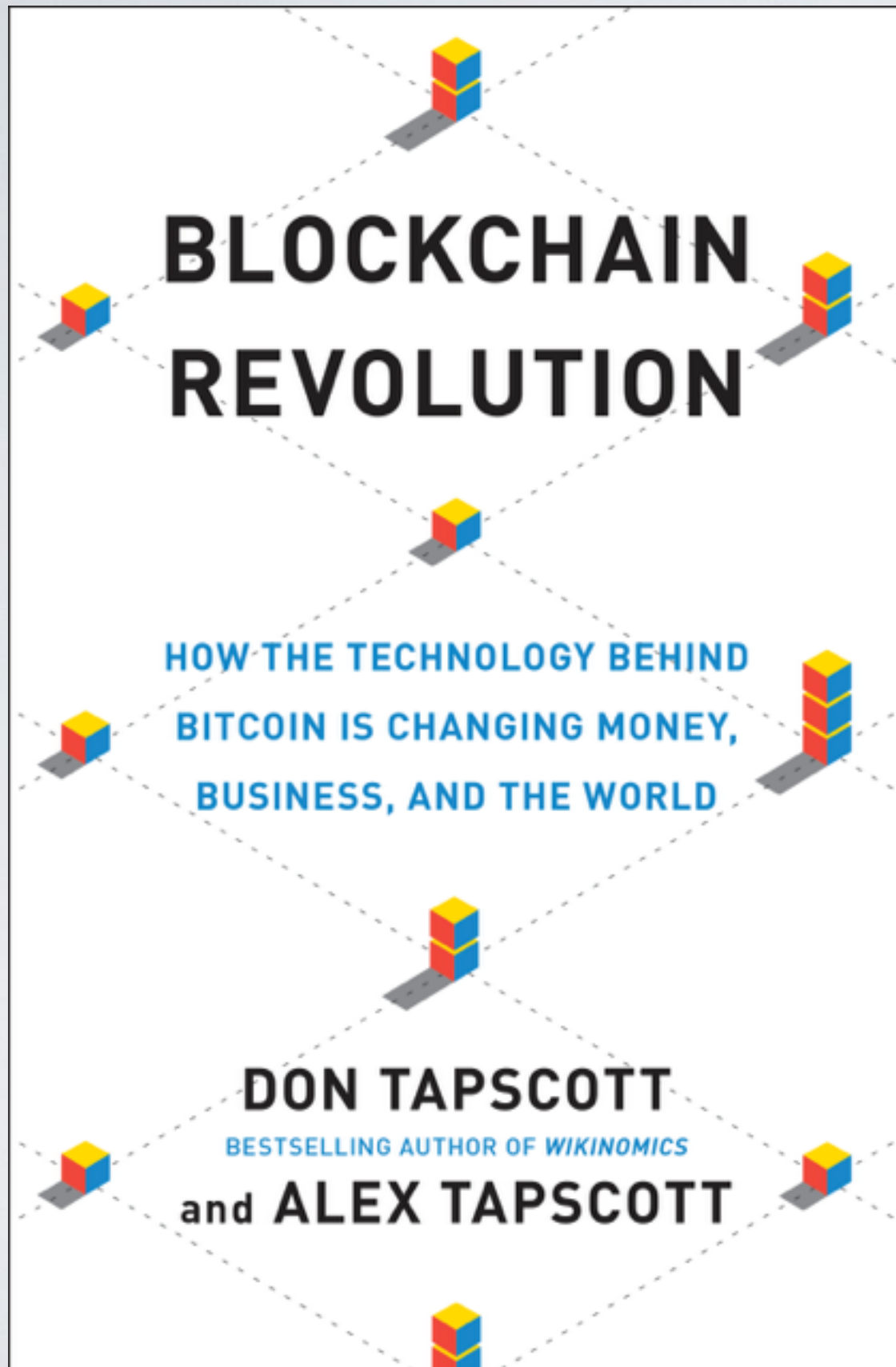
Blockchains: What are they?

What are they?

A place for storing data that is maintained by a network of nodes without anyone in charge

Rules can be written to describe what is eligible for storage and what should be dropped, and the network is incentivized to execute these rules

Once written to, data stored in a blockchain cannot be modified (e.g., it is append only)



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

f t e



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

Blockchain Tech

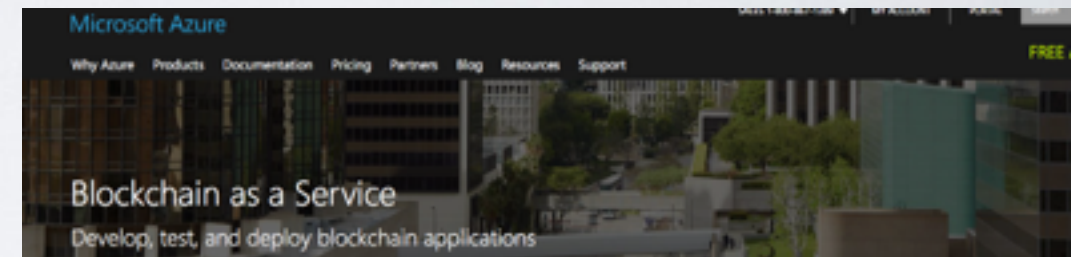
Large Value Transfers (Payments Canada)

RBC, TD, BMO, Scotiabank, CIBC



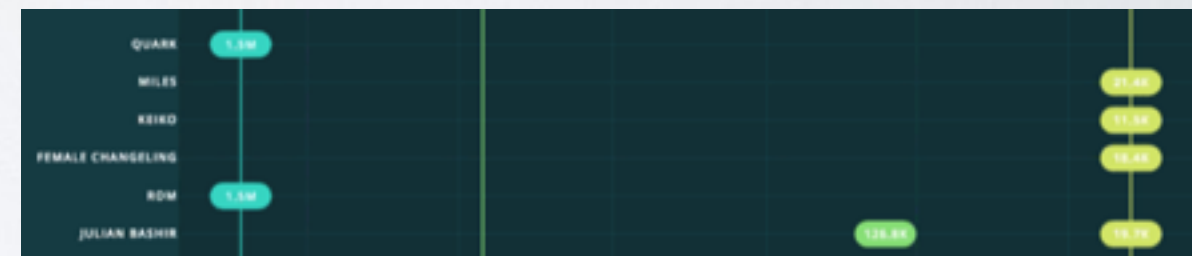
Blockchain as a Service

IBM, Microsoft, Linux, InfoSys



Securities

NASDAQ, ICAP, DTCC, JPX, ASX



Miscellaneous

Voting, Consumption, Health Data



Three Definitions

Blockchain

The data structure from Bitcoin, a decentralized digital currency

Distributed Ledgers

Variations on Bitcoin's blockchain that are used to disintermediate systems

Applied Cryptography

Use cryptographic tools to “digitize” in a secure way things that traditionally are not digital and/or secure

Online Voting vs. Online Banking

- Online bank is not secure—fraud is tolerated
- Any amount of voting fraud should not be tolerated
- Users have zero liability for online banking
- Voters are responsible for their own security
- Banking transactions are visible, traceable and reversible
- Votes are secret, modifications cannot be noticed

Blockchain vs Databases for Voting

Transparency

Voters can trace their ballots in the system and ensure they count for the correct candidate

Immutability

A ballot written into an established blockchain cannot be easily modified (edits will be appended & visible)

Non-Equivocation

A blockchain cannot show different information to different people; there is a single “golden record”

Challenges

The Secret Ballot

Blockchains are visible by default, and provide no way to cast a secret ballot. Layering secrecy on top is non-trivial.

A Running Tally

Blockchains, by default, will display a running a tally which advocates promote as a feature, but is generally illegal

Web & Malware

Writing to a blockchain requires a website, or obtaining a client from a website, and a compromise of either allows privacy violations and/or vote stealing before it reaches

Challenges

Usability

Passwords are not secure enough to protect blockchain transactions. Humans are bad at managing keys.

Vote Selling

Any online system (even with re-voting) is susceptible to selling voting credentials for money or to pressure tactics

Mixed Results on Denial of Service

A large decentralized network should be difficult to take down with traffic but seen DoS attacks on Bitcoin/Ethereum

Conclusions

Blockchains are not a silver bullet

They might play a role as a component in a voting system but blockchains themselves aren't a game changer

Crypto + Voting = Necessary

Adding an “end-to-end verifiable” (E2E) digital audit trail to any voting system, using cryptography, is a game changer

E2E Doesn't Solve Internet Voting (Yet...)

Still have no control over voter devices, voter credentials, or interactions between voters and others

A vibrant purple ink splash or smoke-like pattern against a white background, creating a dynamic and artistic visual. The ink forms swirling, organic shapes that fill the frame.

Questions?

@PulpSpy

<http://vaddr.space>