RSA Conference2016

Singapore | 20-22 July | Marina Bay Sands

Connect to Protect

SESSION ID: **FLE1-F01**

Security Implications of Using Blockchain Technology for More than Money

Dr. Thomas P. Keenan
FCIPS, I.S.P., ITCP
Professor, University of Calgary
Research Fellow, Canadian Global Affairs Institute (Ottawa)
keenan@ucalgary.ca
@drfuture

#RSAC

Who hasn't heard of Bitcoin?

- "The currency of the future"
- "A major disruptive force"
- "An underground currency to allow people to buy drugs and worse"

Source: Sean MacEntee via Flickr under CC 2.0 license

Today we're not going to worry about

- Who created Bitcoin?
- Is it a good investment?
- How do you get some?
  - Though a hospital in California, and a wine store in Calgary, both needed to go buy Bitcoin to get rid of ransomware!
- Will it replace money someday?

We are going to think about

- What makes Bitcoin work? (The blockchain)
- What makes these things special?
- Why do they have a bad reputation?
- What non-financial uses can they have?
- Which uses are here already, or coming soon?
- What are some security lessons and pitfalls to avoid!

Bitcoin and blockchain 101

- The blockchain is the underlying system behind Bitcoin
- It is a distributed database that contains transactional data which can represent anything (e.g., with Bitcoin it represents monetary value)
- Each block contains a hash of the previous one, providing linkage
- Unlike your accountant's spreadsheet, there are many copies, widely distributed, and a mechanism that allows verification and reduces the chance of tampering

Bitcoin and blockchain 101

- It's peer-to-peer and permissionless (anybody can write to it)
- Order is maintained by "miners" who do computational work (often on specialized computers) to ensure the integrity of the blockchain, and receive a small compensation for their work
- Transactions (such as Bitcoins) are not "backed" by anyone and have no intrinsic value

Why drug buyers and sellers love it

- Some degree of anonymity
  - While all the transactions are public (unlike say, credit card purchases) they are not linked to personally identifiable info
- There is no upper limit to the number of bitcoin addresses a user can control. (They are often expressed as QR codes)
- Leftover “change” can be moved to a new address
- Subdividable: 1mBTC = 0.001 BTC; 1 Satoshi = 0.00000001 BTC

Why businesspeople love it

- **Disintermediation**: Enables direct ownership and transfer of digital assets without the need for an intermediary
- **Speed & Efficiency**: Faster settlement on a relatively cost effective and efficient network
- **Automation**: Programmability enables automation of capabilities on the ledger (e.g. smart contracts)
- **Certainty**: Provides irrefutable proof of existence, proof of process and proof of provenance

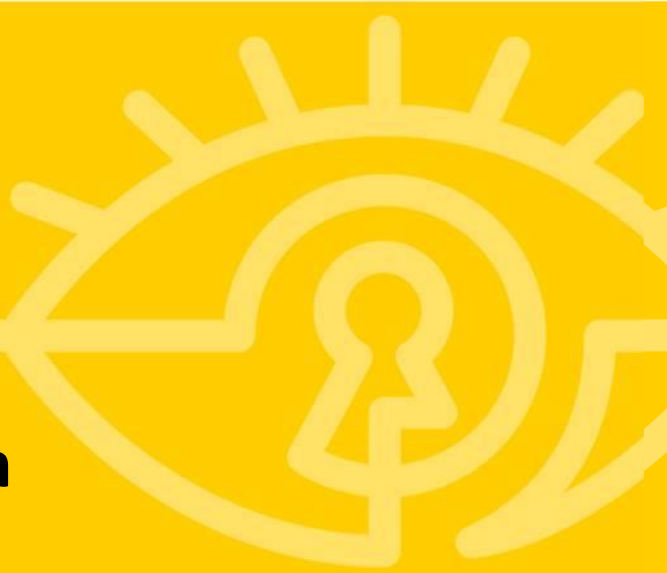
Source: Citi Research, *Digital Disruption* report, available at www.citi.com/citigps

Why I love that last point – a War Story

- Years ago, I was an expert witness in a multi-million dollar insurance claim dispute
- It was a fascinating case involving a basement full of expensive computers that were flooded by a careless contractor
- Much of the claim hinged on proving that certain things had happened on certain days.
- The claimant won, big $, largely because he had a “magic time stamper” machine

If they're so good, why do Bitcoin and the blockchain have such shady reputations?

- They are new, bleeding edge, and threaten some powerful entities (banks, governments, etc.)
- Guilt by association with things like The Silk Road
- Scandals!
  - Mt Gox – bankrupt after losing $450M USD in Bitcoins
  - Bitstamp (3rd largest bitcoin exchange) hacked, lost 19000 BTC
  - Mycoin (Hong Kong) shut down by police, as a Ponzi scheme
  - Ethereum: DAO Attack in June 2016 (3.6m Ether valued @ $20/ETH)



Non-financial uses of the blockchain

Remember that…

- A transaction in a blockchain doesn't have to represent a Bitcoin, or even money -- it can be anything!
- The parties simply need to agree how to interpret it
- So, blockchain could be used to secure something like a land title in a way that counteracts bribery and corruption
- That's exactly what they're trying to do in Honduras

Factom's Honduras land titles project

- "The country's database was basically hacked. So bureaucrats could get in there and they could get themselves beachfront properties." – Factom CEO Peter Kirby
- Project intended by Factom to be completed in 2015, but now it is "stalled"
- Kirby says delays were "political in nature"

Take away: people can get in the way of projects like this

Digital Rights Management application

- Dr. H. Engelbrecht of Custos Media Technologies (S. Africa):
- “I recalled an experience I had several years before, where I purchased an ebook that had my credit card details embedded as a visible footnote in each page, and wondered aloud whether we can’t use bitcoin to impose a similar ‘owner responsibility’ on digital media recipients.”
- ascribe GmbH taking a similar approach to limited edition art

Take away: Blockchain is value-neutral and widely applicable

Internet of Things, and more Things

- IBM rigged a Samsung W9000 washer to automatically order supplies like detergent when it runs low
- Proof of concept for their blockchain-based ADEPT platform
- Lawyers say you are on the hook for purchases made by your things, if you set them in motion, e.g. as self-executing contracts
- However Swiss police gave “Random Darknet Shopper”, a robot that bought ecstasy online, a free pass in the name of art

Take Away: Give your appliances a monthly budget!

Ethereum: A platform for blockchain apps

- Open source
- Crowd-funded
- “Enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middle man or counterparty risk” – Ethereum Foundation

Health records

- A thorny problem. We want our health privacy but we also want the ER doctor to “know all about us” immediately
- Multiple players: doctors, hospitals, insurance companies, lenders, and even patients – cries out for a blockchain approach
- Factom and HealthNautica encrypting health records onto the blockchain with timestamp

Take Away: The technology will follow the money

Blockchain will follow you to the grave

- Coroner (e-) certifies you death
- Your bank accounts are automatically frozen
- All your other financial accounts are flagged as “deceased”
- Your life insurance is paid out to your beneficiaries
- Your taxes are paid

Take Away: No escaping death and taxes, but this is efficient

Blockchain Security Issues

The fundamental concept may have flaws

- "51% attack": When more than half the computing power on a blockchain mining network is controlled by an entity, it can effectively collude to certify false transactions.
- This sounded far-fetched with "Mom and Pop miners" -- but the mining landscape has completely changed!
- In April 2016, "over 70 percent of the transactions on the Bitcoin network were going through just four Chinese companies, known as Bitcoin mining pools — and most flowed through just two of those companies." – New York Times, June 29, 2016

The fundamental concept may have flaws

- Bitcoin “miners” are compensated in BTC; how to incentivize people to maintain the integrity of non-financial blockchains?
- Speculation has been an issue with Bitcoin and can certainly spill over into other applications (“data speculation”)
- Questions about scalability – “it’s never been load-tested”
- Much-touted anonymity is not mathematically guaranteed
  - To understand why, let’s look another ‘anonymous’ service - TOR

De-anonymizing TOR traffic – a War Story

- In 2008, at a computer security "Summer School" in Europe, working with a graduate student, I produced working code that could partially de-anonymize some messages in test data set transmitted with TOR
- By analyzing traffic patterns, we made good "educated guesses" linking the sender and the receiver of a particular transaction
- Similar work reported in *IEEE Symposium on Security and Privacy* by Murdoch and Danezis 2005: http://sec.cs.ucl.ac.uk/users/smurdoch/papers/oakland05torta.pdf
- Kwon, et.al. had 88% success "in telling which sites the (TOR) user was accessing" if positioned as Guard node of Tor Network (which is chosen at random): http://people.csail.mit.edu/devadas/pubs/circuit_finger.pdf
- These are passive attacks, but active ones have also been described, using e.g., a DDOS attack (e.g. Evans and Grothoff at DEF CON 2008) and measuring the load

What does this all mean?

- TOR is constantly being improved and all these attacks were against the then-latest version
- The Tor Project welcomes attempts to break its anonymity, e.g., Torproject.org reported “traffic confirmation attacks” in July 2014
- So TOR’s decoupling of sender and receiver is “probable” but not “guaranteed”
- There were also specific vulnerabilities (e.g. one the NSA code-named “EgotisticalGiraffe” – versus a previous version of Firefox) *in the ecosystem*

Holes in Bitcoin/blockchain anonymity

- Transaction Graph Analysis takes a similar approach -- analyzing traffic and trying to link blockchain transactions to certain wallets
- Good practice says to never re-use an address, but instead to move any leftover BTC (for example) to a new address, however…
  - Unintended consequence is that an address that has never been seen before is probably a “change address” which yields some info
  - Also things can be deduced from amounts, e.g. with two BTC outputs of 3.0 and 2.712791, the first is likely purchase, the second the change
- There are additional anonymization tools like “mixers” and “tumblers”

Reference: http://www.coindesk.com/anonymous-bitcoin-backgrounder-policymakers/

As for getting real word identity…

- You have to go outside the blockchain
- Some entities divulge their Bitcoin address, e.g. on blockchain.info

1LjBQSHrtY5pXaNp4WWJ2MSZHZduc2yF9z	Dan Carlin Donation	http://www.dancarlin.com/dc-donate/
16YhFXjpQhpbGRzhntJhFJaB36gY3bnm7Q	BitRevenues - Free BTC Lottery	http://bitrevenues.com
1MPYyfoWK8CkAzhLzLLtZGa9dwEGT5dm2T	neocities.org	https://neocities.org/donate

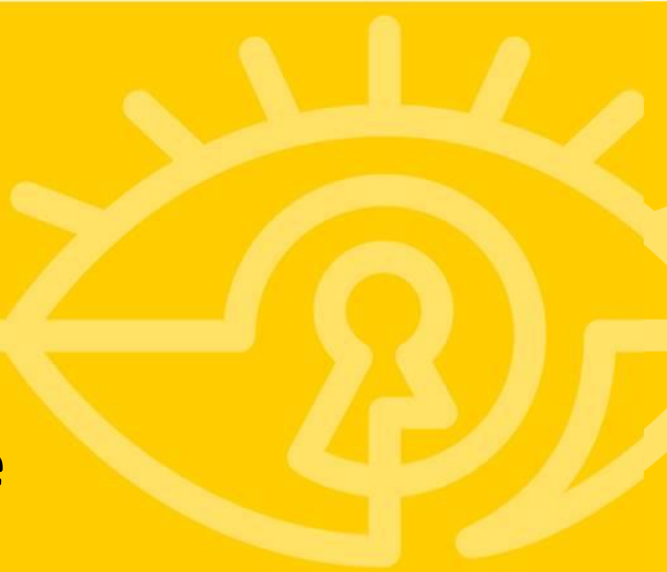
- Conclusion: Bitcoin is not as anonymous as cash, but more anonymous than most other payment methods
- “Beware of time travelling robots from the future”

The ecosystem around the blockchain can be problematic

- Many of Bitcoin's woes were related to thefts from "hot wallets"
- While the blockchain is resistant to tampering, systems to implement and use it are just as vulnerable as any others to hacking, programming errors, corrupt staff, malware
- The kind of data being considered for blockchain systems, from highly personal health information, to control of important physical facilities, may have consequences that far exceed the loss of money (breach of privacy, hijacking of infrastructure, etc.)

In summary

- You will be hearing more and more about the blockchain, even from its traditional enemies like financial institutions
- The only limit to blockchain applications will be human creativity, and perceived creepiness
- Security risks of the core technology are manageable
- Danger awaits in the ecosystem around the blockchain
- As always, people are the biggest threat!



Applying What You've Learned Here

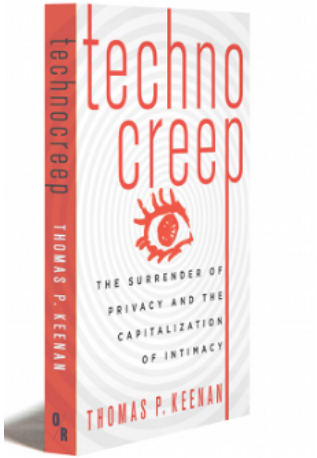
Things to do right away

- Next week you should:
  - Go buy a small amount of Bitcoin so you understand the process
- In the first three months following this presentation you should:
  - List business processes relevant to your work that could be affected by the factors (e.g. disintermediation) made possible by blockchain technology
  - Brainstorm whole new processes and applications that might be made possible by the blockchain
  - List some risks involved in moving to the blockchain

Longer Term Application

- Within six months you should:
  - Sell that Bitcoin if its value has gone up
  - Subscribe to online newsletters such as CoinDesk to keep abreast of this technology
  - Monitor what your peer organizations are doing with the blockchain
  - If it makes business sense, move some non-critical process to the blockchain, possibly in parallel with other technologies

So, for example…OR Books takes Bitcoin



Technocreep

THE SURRENDER OF PRIVACY AND THE CAPITALIZATION OF INTIMACY

THOMAS P. KEENAN

"In *Technocreep*, Dr. Keenan explores some of the most troublesome privacy-invasive scenarios encountered on the web and offers users a number of excellent, practical ideas on how best to protect their privacy and identity online." —Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario

"Keenan's vivid explanation of the perils of creepy technologies is both hilarious and terrifying. A great read for those who build systems and an entertaining excursion for anyone who wants to peek under the covers of technology." —Dr. Cullen Jennings, Cisco Fellow

"Thomas P. Keenan has done a wonderful job in threading seemingly disparate ideas into the single notion of 'creep.' This book gives numerous pithy examples of how we arrived at where we are, and where we might be headed." —Dr. Peter G. Neumann, Senior Principal Scientist in the Computer Science Laboratory at SRI International, ACM Risks Forum moderator

Tweet Like 98

MORE OR TITLES

Cypherpunks
Freedom and the Future of the Internet
Julian Assange
Paperback ($16), E-book ($10), Print + E-book ($20)

BUY THIS BOOK

Paperback: $18/£12 ADD | E-book: $10/£7 ADD | Print + E-book: $24/£15 ADD

FAQs and shipping information

BUY WITH BITCOIN

ABOUT THE BOOK

Let's stay in touch!

- keenan@ucalgary.ca
- +1 (403) 220-7437 at The University of Calgary
- @drfuture on Twitter
- www.technocreep.com