Blockchain's Promise for Cyber Security

Associate Professor Alex Sims

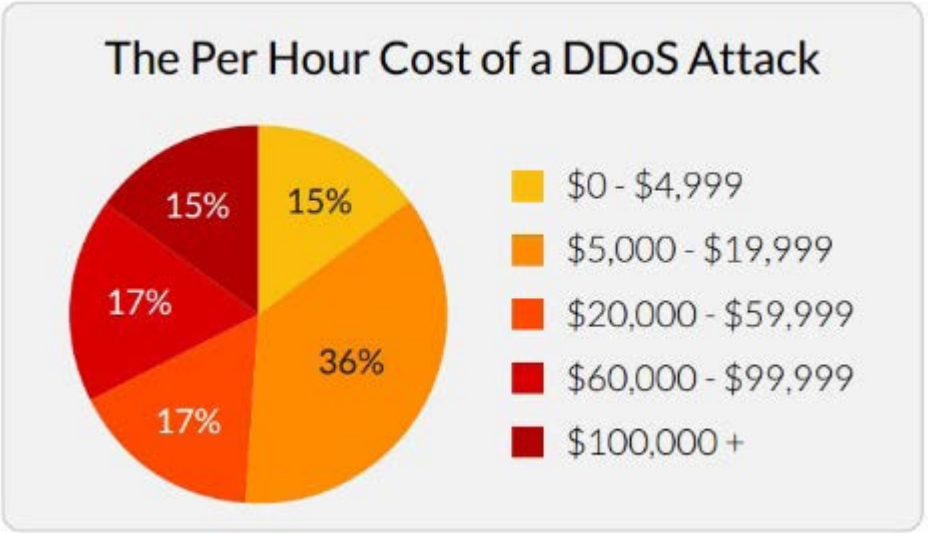
THE UNIVERSITY OF AUCKLAND
Te Whare Wānanga o Tāmaki Makaurau
NEW ZEALAND

Before looking at Blockchain

- Hackers will go for the weakest point, especially so with ICOs
- Eg, hacking into a website and changing Ether address, so Ether sent to a different account
  - Need much better security
- Websites cloned and a website with a slightly different URL including different domain used –
  - Patrol all forums where URLs are given and register in all domains
- DDoS attacks in particular can be crippling for organisations (see next slide)

DDoS attacks

- 45% of respondents reported a DDoS attack, 91% in last 12 months, 70% two or more DDoS attacks
- 49% last between 6-24 hours
- 87% experienced at least one non-financial consequence, such as loss of customer trust, loss of intellectual property, and virus/malware infection, 60% incurred two or more
- 33% had customers' data stolen



https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf

Blockchain

- Some people think blockchain is all about Bitcoin and other cryptocurrencies
- Blockchain as a technology is so much more than just cryptocurrency
- Cyber security is just one of blockchain's potential uses:
  - Note: blockchain is not a panacea, isn't the silver bullet, but does over some advantages
  - =
  - sticking to current systems because the alternative is not 100 fool proof is deluded thinking

What is a blockchain?

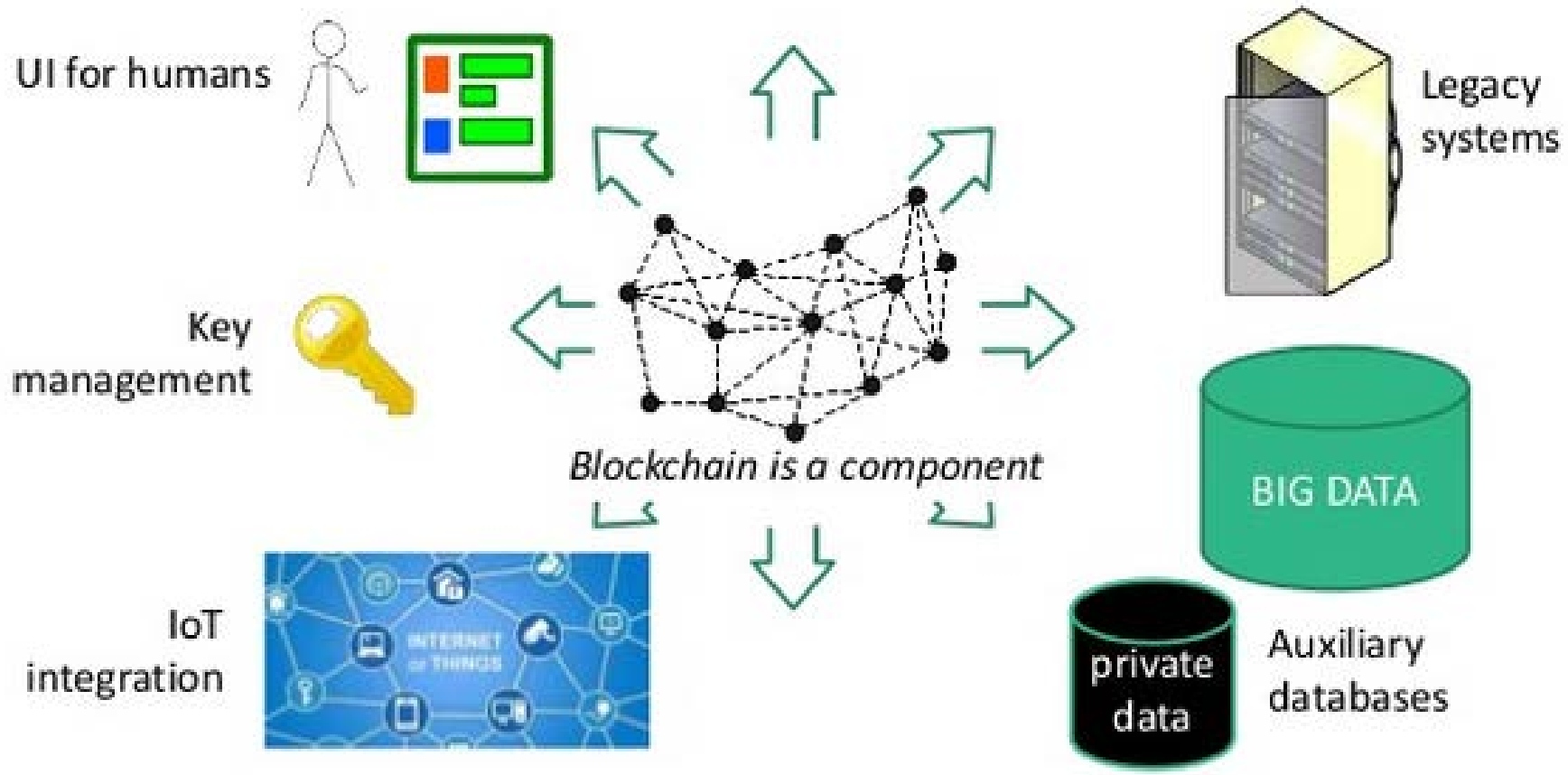
Definition of a blockchain

A database so **secure** it can be made **public**

Where **altering a copy** of the database **has no effect** & transactions can only be appended, **never deleted or updated**

Underpinned by a **Peer to Peer protocol that strictly enforces transaction validity prior to writing** to the database

Blockchains are not stand-alone systems



https://www.slideshare.net/IngoWeber2/blockchain-background-and-data61-research-overview

There is a bit too much hype about blockchain


I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.
S. Adams
E-mail: SCOTTADAMS@AOL.COM
© 1995 United Feature Syndicate, Inc.(NYC)

Why blockchain can be so powerful (generally)

- Once you put something on a blockchain for one purpose it opens up a whole range of other things
  - Eg if tokenise assets, ie record ownership of car, can also:
    - Have verified odometer readings
    - Copy of all work done to that car and the parts used (very useful if recall of parts)
    - Insurance
    - Car can have own wallet and pay for tolls etc and be paid
      - Estimates that information gained from cars, air temperature, rain, pollution levels etc could be worth $5,000 per year
    - If linked to IoT devices the average speed of the car and where it has been (obvious privacy issues)

Relevance of blockchain to cybersecurity?

"Imagine a computing platform that would have no single point of failure and would be resilient to … cyberattacks... This is the promise behind blockchain, the distributed ledger that underlies cryptocurrencies like Bitcoin and Ethereum and challenges the traditional server/client paradigm."

https://techcrunch.com/2016/12/05/how-blockchain-can-help-fight-cyberattacks/

Press Release

Lockheed Martin, 27 April 2017 **“Lockheed Martin Contracts Guardtime Federal for Innovative Cyber Technology”**

“Lockheed Martin becomes the first U.S. defense contractor to incorporate blockchain technology into its processes”

“How Emerging Blockchain Technology Will Revolutionize Cybersecurity” – Infosecurity Magazine, 13 September 2017

“Blockchain Takes Away a Cybercriminal's Greatest Edge”

PCMag 25 October 2017

Why could blockchain be useful for cyber security?

- Info on a blockchain is held in multiple places, so no one point of failure, ie decentralised storage
- Info on a blockchain can’t be changed – immutable:
  - If change required, ie new edition of document or change of ownership of asset – will be new entry in the blockchain so can always see the original document/owner of asset
  - Also means that a hacker (whether external or internal) can’t change records to hide evidence of its presence (thus hackers can be detected much quicker than currently)

Why could blockchain be useful for cyber security?

- Authentication of users
- Instead of passwords (very weak in the hands of a number of users!), could use a distributed public key infrastructure for authenticating devices and users
  - Devices use specific SSL certificate rather than a password
  - Management of certificate data carried out on blockchain – almost impossible for attackers to use fake certificates.

Encryption

- Contrary to (some) popular belief, information on a blockchain, even a public blockchain, can be encrypted so only the possessor of the private key can read it
- =
- Even if someone gets into the system, they can’t read the information (if it has been encrypted)
- (private keys are a problem, ie need to store a backup and risk of those being compromised)
- (Don’t actually need a blockchain for encryption)

How blockchain can help

- No one single source of information, same information replicated (and encrypted) amongst many computer systems – so can always retrieve information
- Use IPFS (Interplanetary File System) to replace DNS system and create a new secure internet:
  - “DNS is the weak link of the internet, exploited by rogue ISPs, censors, and hackers to create an unreliable web" –
  - Nebulis uses Ethereum blockchain and Interplanetary File System (IPFS), a distributed alternative to HTTP’s centralized structure, to make its DNS infrastructure immune to DDoS attacks

https://medium.com/@Physes/how-to-build-a-more-secure-domain-system-5efed811409e

But what about financial data, personal information including health records, intellectual property?

Don’t want unauthorised people accessing that information at all.

Personal information?

- Significant problem that personal info (ie valuable data and a target for hackers) is held by many organisations and hacks happen – Equifax, Uber etc, etc
- Blockchain can be used so each person stores and controls their info - Civic is an example (built on Bitcoin’s blockchain)
- No need for organisations to hold and protect customers’ personal data

https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

Benefits of not holding personal information

- When combined with blockchain providers offering digital identity solutions (ie Civic/Sovrin/Uport etc)
  - Radical reduction in KYC/AML costs
- Limited holding of any personal information, ie records of transactions linked only to anonymous decentralised identifiers (Sovrin)
  - Large reduction in costs because limited info needs to be held and secured
- Analogy with move in manufacturing from buying and storing large volumes of parts to just-in-time/lean manufacturing

IP and confidential information?

- Different considerations to basic information and personal information
- Slightly ironic that would want to use blockchain to secure IP given that public blockchains run on open source code and Hyperledger is open source…
- IP and confidential information can be protected by encryption and also can have just a few nodes that have access to that information rather than whole blockchain (useful especially if don’t/can’t send information off shore)

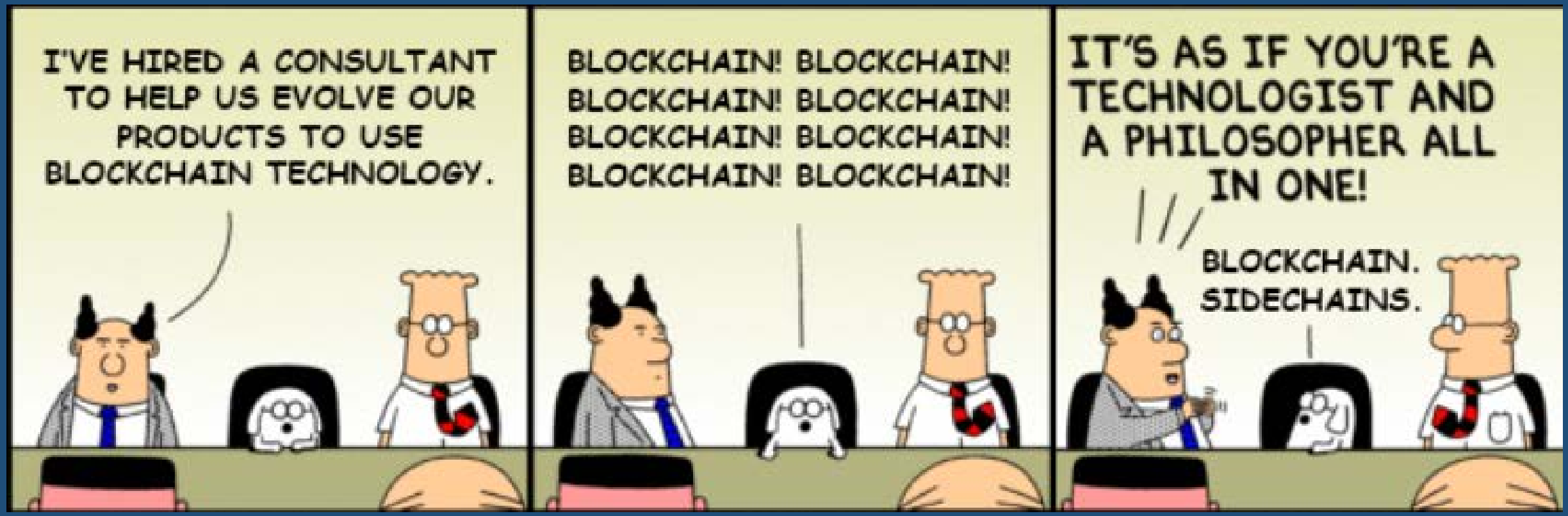
Limitations

- Cost, if using Ethereum, need to pay gas (ether) for each transaction – see Data 61's research
- Latency when using blockchain
  - don't and can't wait for even 20 seconds to access and change files is they are stored on blockchain
  - but superfast blockchains being worked on
  - could use distributed computing, and have blockchain for the time stamping so can see who has done what

https://www.slideshare.net/IngoWeber2/blockchain-background-and-data61-research-overview

Beyond blockchain…

- Blockchain was version 1.0, now various solutions being worked upon that make blockchain look outdated
- Blockchain not the best for IoT devices, security of IoT devices is a massive issue:
  - Tip – change the default password on IoT devices, most people do not change it
- But, IOTA and its “tangle” may potentially solve many issues (listen to podcast on “IOTA & the Post-Blockchian Era”)


I'VE HIRED A CONSULTANT TO HELP US EVOLVE OUR PRODUCTS TO USE BLOCKCHAIN TECHNOLOGY.
BLOCKCHAIN! BLOCKCHAIN!
BLOCKCHAIN! BLOCKCHAIN!
BLOCKCHAIN! BLOCKCHAIN!
BLOCKCHAIN! BLOCKCHAIN!
IT'S AS IF YOU'RE A TECHNOLOGIST AND A PHILOSOPHER ALL IN ONE!
BLOCKCHAIN.
SIDECHAINS.

Questions

- https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf
- http://www.blockarmour.com/
- https://www.forbes.com/sites/julianmitchell/2017/12/31/this-startup-uses-blockchain-tech-to-rethink-cyber-security-in-the-bitcoin-era/#7f824e8f2b39
- https://gladius.io/#about-us - https://coinjoker.com/blockchain-ethereum-can-prevent-ddos-attacks/
- https://www.infosecurity-magazine.com/next-gen-infosec/blockchain-cybersecurity/
- https://www.slideshare.net/IngoWeber2/blockchain-background-and-data61-research-overview
- https://georgianpartners.com/podcast-how-a-cyber-attack-inspired-a-new-era-of-blockchain-powered-digital-security/
- https://medium.com/@S.protocol/so-what-is-the-solution-to-nem-hack-and-its-kind-3cf7cadb0239
- https://etherreview.info/ether-review-69-iota-the-post-blockchain-era-591f00e2ea5d