Guest Lecture – COMP6452 @ UNSW

Blockchain,
Key Management,
& Self-Sovereign Identity

Adnene Guabtni

Senior Research Engineer
Data61, CSIRO

adnene.guabtni@data61.csiro.au

Hugo O'Connor

Senior Engineer
Data61, CSIRO

hugo.o'connor@data61.csiro.au

New tech is … old tech

- Blockchain technology relies on

Public Key Cryptography, also known as Asymmetric Cryptography

Invented in 1970 by James H. Ellis, a British cryptographer

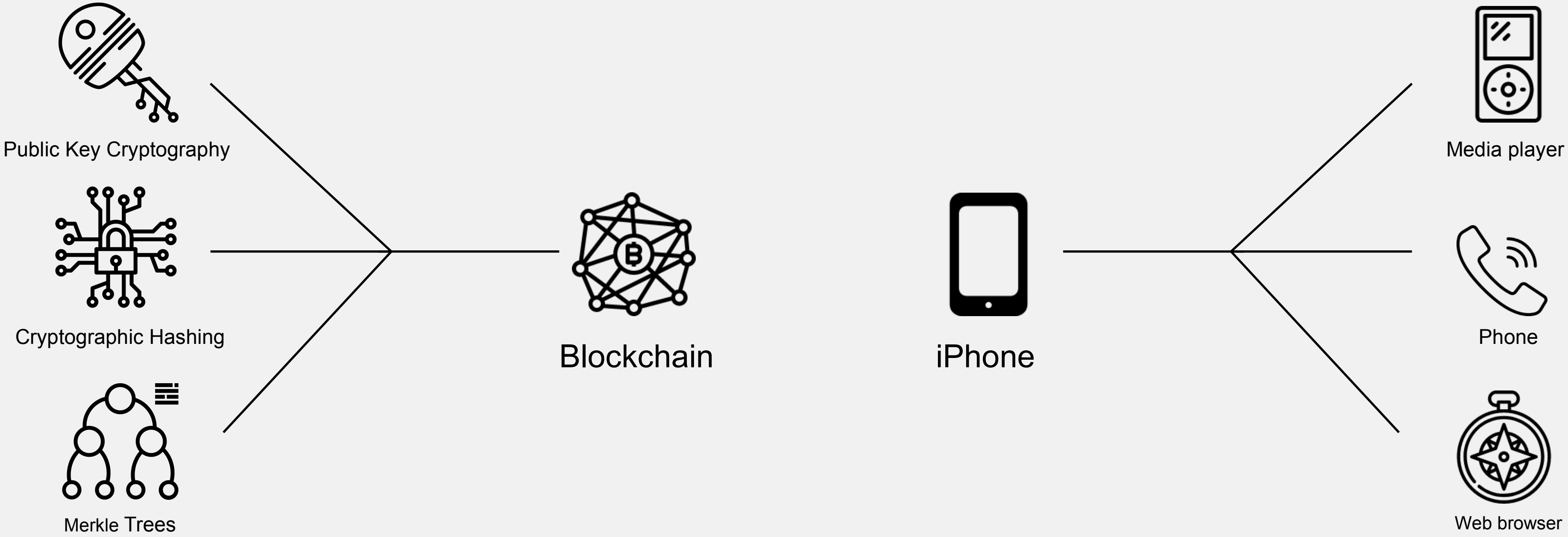
Cryptographic Hashing

Invented in 1953 by Hans Peter Luhn at IBM

Merkle Trees, or Hash Trees

Patented by Ralph Merkle in 1979

Innovation is often a smart combination of existing tech



Public Key Cryptography

Cryptographic Hashing

Merkle Trees

Blockchain

iPhone

Media player

Phone

Web browser

The building blocks for innovation are readily available

Public Key Cryptography

Web technologies

Biometrics

Wireless networks

On-Chip Capabilities

Cryptographic Hashing

Mobile computing

Sensors

P2P networks

Traceability

Merkle Trees

Cloud computing

Internet of Things

Short-range networks

Geo-localisation

Cryptography

Public Key Cryptography

Cryptographic Hashing

- Public Key Cryptography & Cryptographic Hashing are key enablers of the modern Internet
  - **Public Key Encryption**: Transport-Layer Security (TLS) – Securing Internet communications
  - **Digital Signatures**: To verify that a message was provided from a trusted party.
  - Public keys are distributed on a public ledger / certificate issuer
  - Private keys are kept secret somehow
  - Key Management still poses a challenge

Where to store your Cryptographic Private Key?

File System on your own machine?

High risk of theft if your machine is compromised

Within your browser (using an add-on)

High risk of theft if your machine or your browser is compromised

Paper wallet

Offline = more secure; Paper-based = fragile → risk of loss or damage

Hardware wallet

Offline = more secure; Needs to be plugged into a computer

Sofware wallet (on mobile or desktop)

Available anywhere anytime; Better access control; Limited to blockchain transactions

Where to store your Cryptographic Private Key?

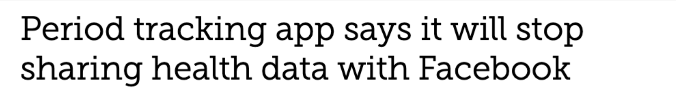
Cloud-based / Server-based Key Management Systems

Ease of use; High risk of hacking of the hosting servers

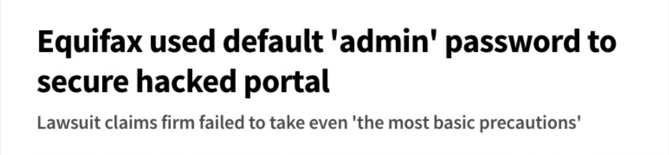
Facebook Is Still Leaking Data More Than One Year After Cambridge Analytica

Michael Nuñez Forbes Staff
Social Media
I'm an associate editor covering Facebook and social media.

Australian National University hit by huge data breach

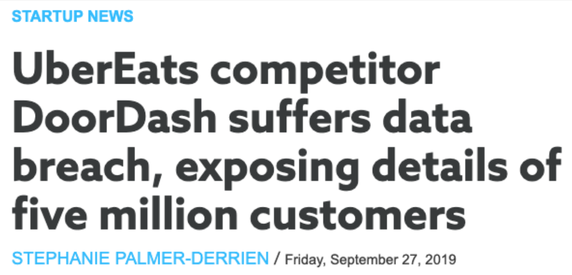


Period tracking app says it will stop sharing health data with Facebook



Equifax used default 'admin' password to secure hacked portal

Lawsuit claims firm failed to take even 'the most basic precautions'



STARTUP NEWS

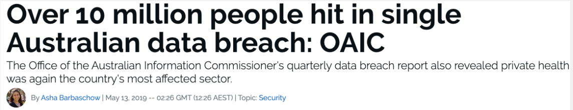
UberEats competitor DoorDash suffers data breach, exposing details of five million customers

STEPHANIE PALMER-DERRIEN / Friday, September 27, 2019

TECH INSIDER

Hackers have become so sophisticated that nearly 4 billion records have been stolen from people in the last decade alone. Here are the 10 biggest data breaches of the 2010s.

AARON HOLMES
OCT 19, 2019, 1:24 AM



Over 10 million people hit in single Australian data breach: OAIC

The Office of the Australian Information Commissioner's quarterly data breach report also revealed private health was again the country's most affected sector.

By Asha Barbaschow | May 13, 2019 -- 02:26 GMT (12:26 AEST) | Topic: Security

TECH

Google workers are eavesdropping on your private conversations via its smart speakers

Joshua Bote USA TODAY

Published 11:43 a.m. ET Jul. 11, 2019 | **Updated 8:20 p.m. ET Jul. 11, 2019**

Sensitive personal data of hundreds of visa applicants accidentally leaked in email mishap

TECH INSIDER

Canva under cyber-attack, with reportedly as many as 139 million users affected

ALEKS VICKOVICH
MAY 27, 2019, 10:57 AM

YAHOO'S HUGE BREACH —

Yahoo tries to settle 3-billion-account data breach with $118 million payout

Verizon-owned Yahoo boosted offer after judge rejected first settlement.

Unlocking the full potential of Public Key Cryptography

Full cryptographic operations (encrypt, decrypt, sign, verify, hash) on any data (not just cryptocurrencies)

Decentralized digital identity on- or off-blockchain

Proof of claims on- or off- blockchain

Building trust in P2P networks with or without blockchain

Building trust on the World Wide Web with or without blockchain

What is our vision?

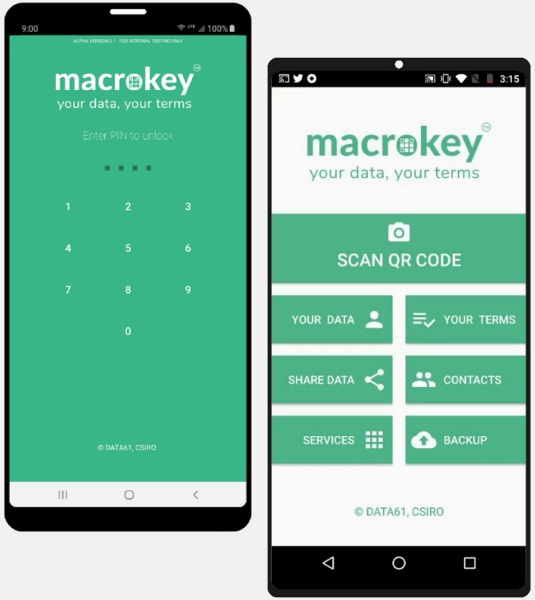
Our vision is for individuals to be empowered with digital dignity through trust forming technologies that lower barriers to trade and cooperation, leading to freer and more prosperous societies.

***

“Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently political tool, and it confers on the field an intrinsically moral dimension”

Rogaway, P. (2015). The Moral Character of Cryptographic Work. IACR Cryptology ePrint Archive, 2015, 1162.

What is macrokey?



- A mobile application
- A self-sovereign identity
- A cryptographic service
- A simpler, more secure way to authenticate
- An access control engine
- An encrypted personal data vault
- Extensible
- A communication tool
- A query-able data graph
- An enabler of trust

LIVE DEMO

Thank you for your attention

Learn more at macrokey.io

Follow us on Twitter @macrokeyio

Credits: This presentation has been designed using graphics from Flaticon.com