Privacy, Mimblewimble and BEAM

MUST READ: Android development: How to deliver a successful mobile app for business

Apple's Tim Cook: Silicon Valley has created privacy-violating 'chaos factory'

Time for tech companies to take responsibility for the digital privacy mess they're created, says Apple chief.

By Steve Ranger | June 17, 2019 -- 11:06 GMT (12:06 BST) | Topic: Security

7

MORE FROM STEVE RANGER

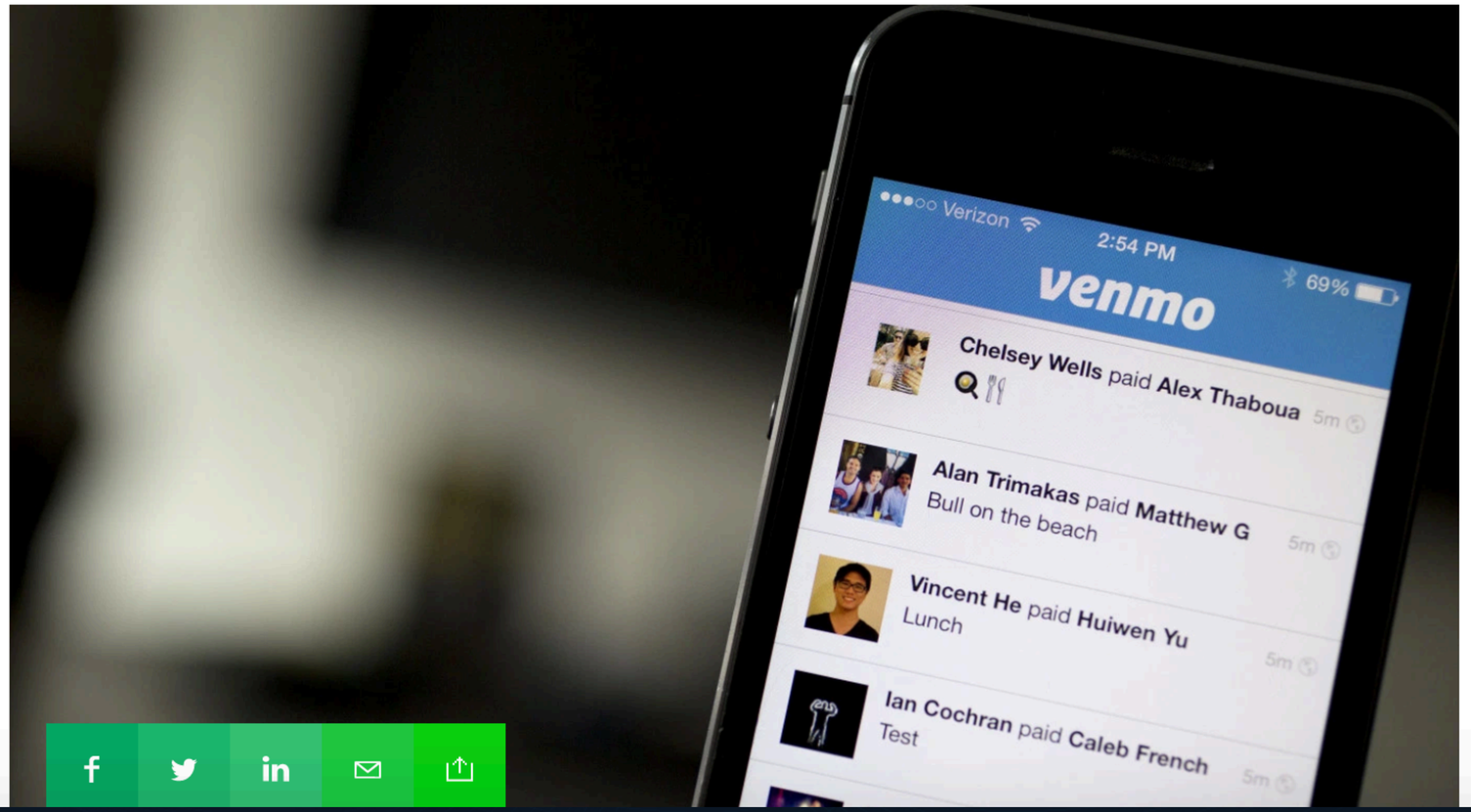
Security
Malicious Microsoft Word docs

source: https://www.zdnet.com/article/apples-tim-cook-silicon-valley-has-created-privacy-violating-chaos-factory/

Millions of Venmo transactions scraped in warning over privacy settings

Zack Whittaker @zackwhittaker / 1 week ago

Comment



source: https://techcrunch.com/2019/06/16/millions-venmo-transactions-scraped

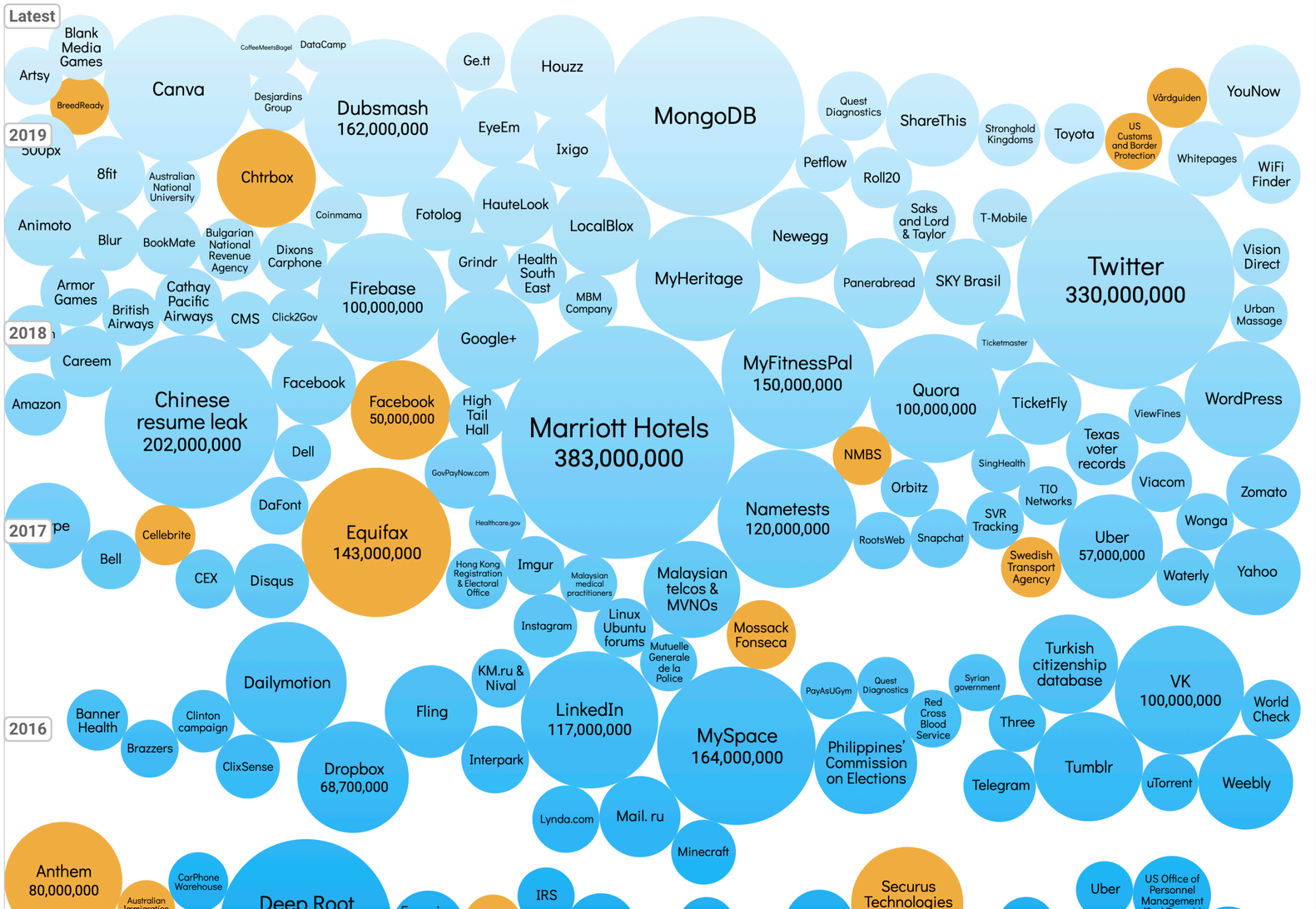
World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

Last updated: 1 April 2019

interesting story

Filter Colour YEAR DATA SENSITIVITY 2009 2019 Search...



source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Privacy

is a basic human right

Public Blockchains

- Transparent
- History of all transactions can be seen
- Good for compliance but bad for privacy

Privacy Focused Blockchains

- Private
- Not scalable
- Good for privacy but bad for compliance

A Bitcoin Transaction

- Spills 3 pieces of information:
  - Sending address
  - Receiving address
  - The amount sent

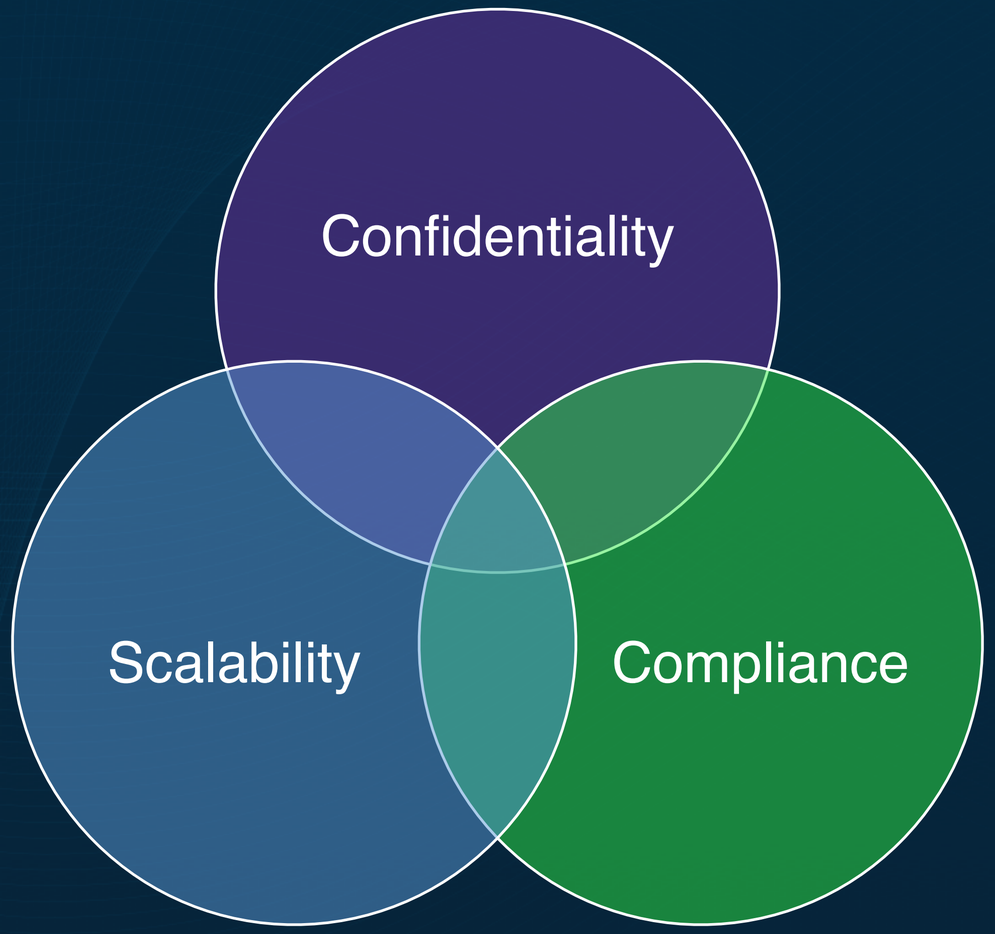
Blockchain Analytics Companies

BEAM

What the real world needs

- Permissionless Digital Cash
- Sovereign Digital Cash
- Stable coins
- Tokenized Securities
- Debt, financial derivatives
- Supply chain management
- Moving Personal Data

All Require



Why and What

We want a world where crypto **coexists** with legacy financial systems

We enable decentralized transfer of value that is confidential, scalable and **optionally** compliant

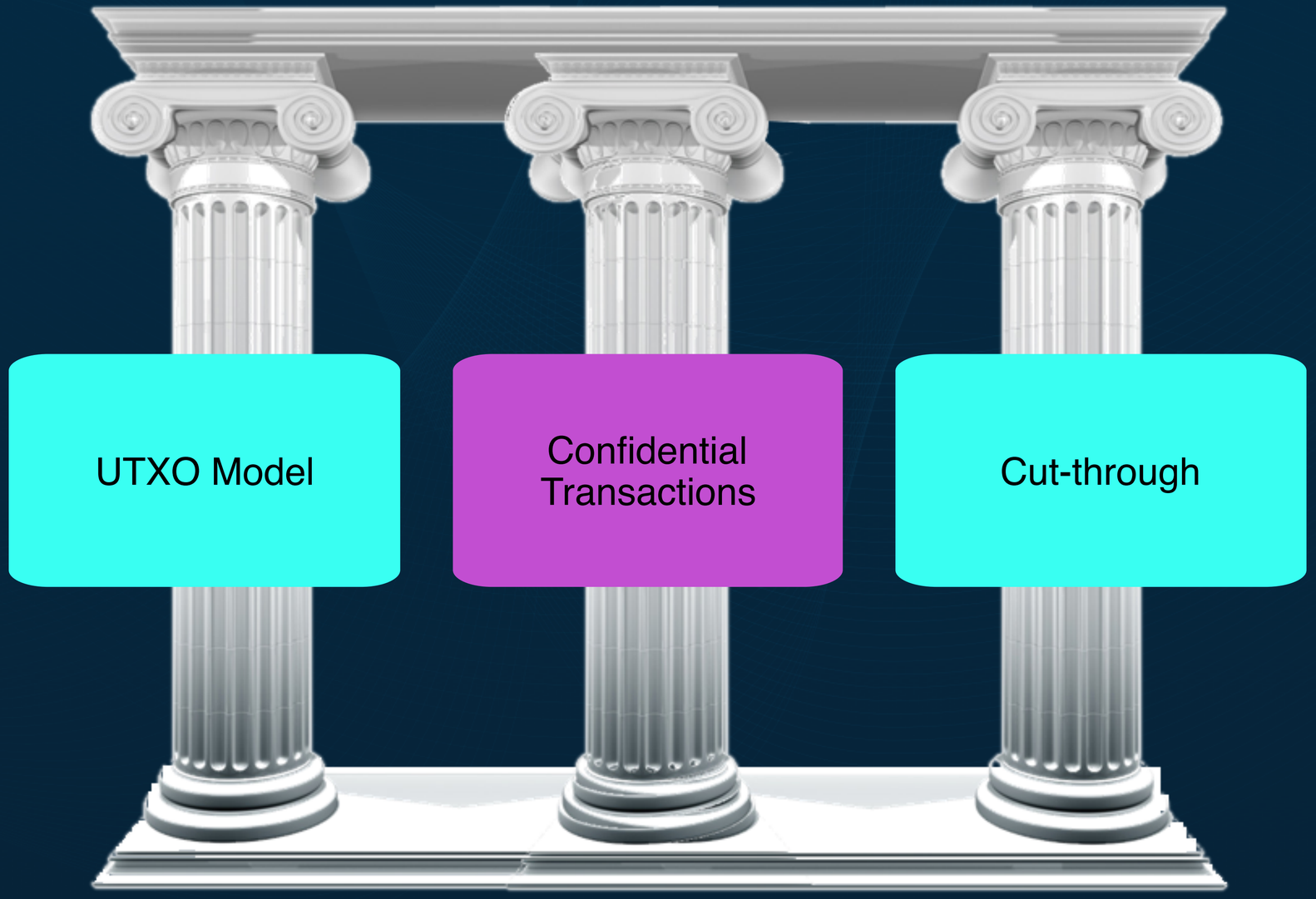
Mimble what?

Mimblewimble.

An elegant protocol offering full privacy without sacrificing scalability.

Developed by an anonymous author -> Tom Elvis Jedusor
(French for lord Voldemort)

How Mimblewimble works



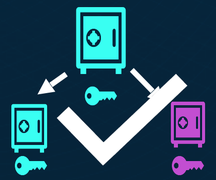
UTXO Model

Each user holds keys to their own Safe Deposit Boxes

Secure bulletin board system (SBBS)

Both sender and receiver have to be online or connect to the SBBS

Confidential Transactions



✔ Is the sum Zero?
✔ Are the values positive?

UTXO Model

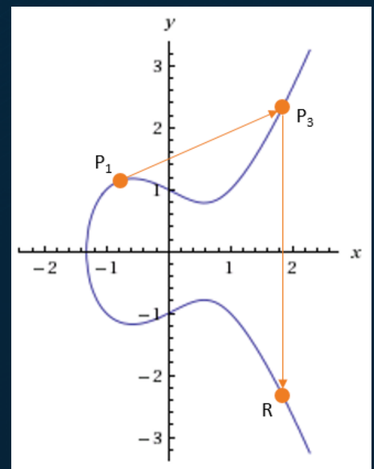
- Well, there aren’t really any safe deposit boxes…
- Meet Pedersen Commitment (Torben Pryds Pedersen)

blinding factor
=
secret key

Value

$$P = r \cdot G + v \cdot H$$

Elliptic Curve Generator Points



Multiplying is easy but factorizing is hard

213 x 28 = ?

? x ? = 5964

? x ? = 596439873239

$$213 \times \mathbf{G} + 345 \times \mathbf{H} = 596439873239$$

Transaction Cut-through

Alice

Bob

$P_i = r_1 \cdot G + v \cdot H$

$P_O = r_2 \cdot G + v \cdot H$

$(r_2 - r_1) \cdot G$

$P_I = r_2 \cdot G + v \cdot H$

$P_O = r_3 \cdot G + v \cdot H$

$(r_3 - r_2) \cdot G$

Bob

Carol

Transaction Cut-through

Alice

$P_i = r_1 \cdot G + v \cdot H$

$(r_2 - r_1) \cdot G$

$P_O = r_3 \cdot G + v \cdot H$

$(r_3 - r_2) \cdot G$

Carol

- Intermediary states removed –keep just current state of UTXOs
- Same repeated for all the blockchain

Block 303258

FEE:	50 Groth
HASH:	a62ecc25075a49704e0ce78f13be0eb2a1028fbceec0f900a8ecf34cf915758e
DIFFICULTY:	305,475,840
SUBSIDY:	8,000,000,000 Groth
CHAINWORK:	0x3231b33148d2e00000
AGE:	August 3, 2019, 5:50:46 AM

INPUTS: 2

Commitment:	Maturity:
0x3dcf7c602d76c4df23ffe39e4cb1245ae15c2f9a77fd244aeab67ee2ca81a832	303205
0xf3a89ab011ed8429024cb311a050f17f96ab3c3b722e365ef2a62f6aa02ea219	303205

OUTPUTS: 4

Commitment:	Maturity:	Coinbase:
0x8ca6e28ea2c0679d56ca3fbb468ca4ac9f46d8571f9e5798758ce71e31484ef3	303258	false
0xa8e1ef93efcbd4478018c9b2adbd6c7e13e95f9c1aab1d194cbcbc13c3d1cbf1	303258	false
0xd1012838b4e75020d0c299a6ca0ddd83895d56c885cd32069f3511264893e567	303258	false
0x1afd3d21445d5506d7b30e694ad8f404e223ed5ac48871deac9d512f8d79d310	303498	true

KERNELS: 2

Fee:	Excess:	ID:
0	0x18c1ac18e1d8790e09081589a9cee5dfa9bac6cd40ca717007ab540483f04e78	859227e8c173d01c59b4b9bc6a818729d94e1b6c4a5e01e1a8dd84cdfcb24bda
50	0x8aafbf8f6512815eb04984006ed61c2ac63f2fe6a2c413038ec7568e284f0184	16a8f6a2e9f4c32377d62e60d4c81f93cc8d1e4e65c1dafbd1537acb99f9b346

Comparison (8.2019)

Currency	# of Transactions	Blockchain Size (GB)	Avg KB Per Transaction	Blockchain Size Assuming	Monetary Policy
BTC	439,017,363	232.434	0.53	:)	Deflationary
MONERO	13,153,493	54.587	4.15	1.8 TB	“Trail Emission"
ZCASH	5,040,118	23.55	4.67	2.05 TB	Deflationary
GRIN	**861,055**	**0.25**	**0.3**	**131GB**	**Inflationary**
BEAM	**1,463,424**	**1.039**	**0.575 - 0.77**	**252-338 GB**	**Deflationary**

What is BEAM

A new blockchain based on Mimblewimble protocol

- PoW consensus
- Decentralized
- Permissionless
- Deflationary
- Implemented from scratch in C++
- Development started in March 2018
- Launched on Jan 3 2019

Some Exciting Developments

- Asset layer (Confidential Assets)
- Compliance component
- Atomic swaps with BTC & LTC
- Hardware wallet support
- Lighting network POC

@innovationMaze

oe@coin-ix.com

Thank You All

BEAM

Privacy is a basic human right