

---

# WIDER ADOPTION OF BLOCKCHAIN TECH, CRYPTOCURRENCIES AND STABLECOINS: OBSTACLES AND INCENTIVES

**Dr Garrick Hileman**  
University of Cambridge

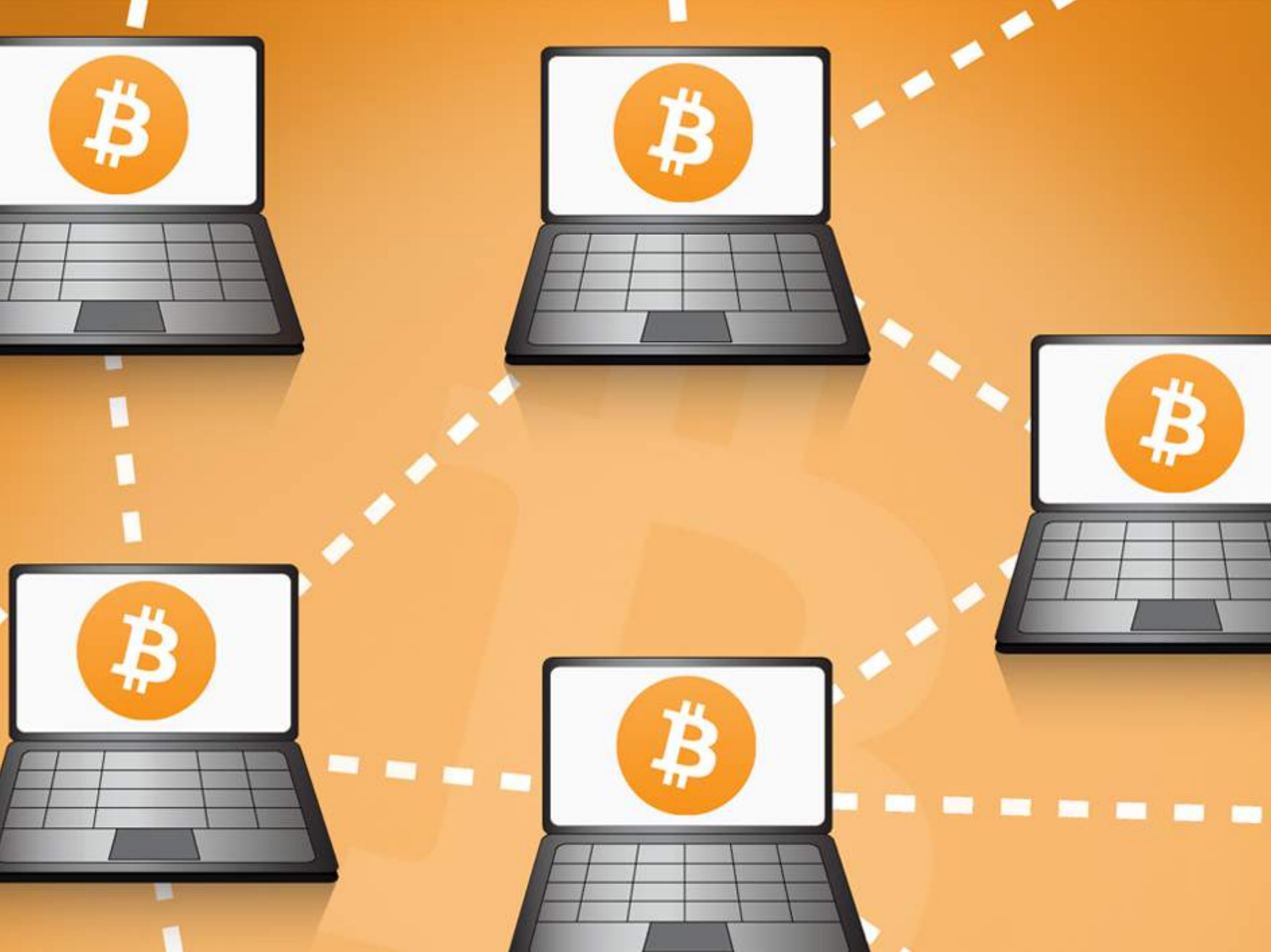
20 March 2018



Where does money come from?









Over 200 enterprise DLT start-ups, established corporations, central banks and other public sector institutions are included in the study sample\*



\*A number of survey respondents prefer not to have their participation disclosed. The names of participating central banks and other public sector institutions have been kept confidential. The survey data has been supplemented with secondary data sources.

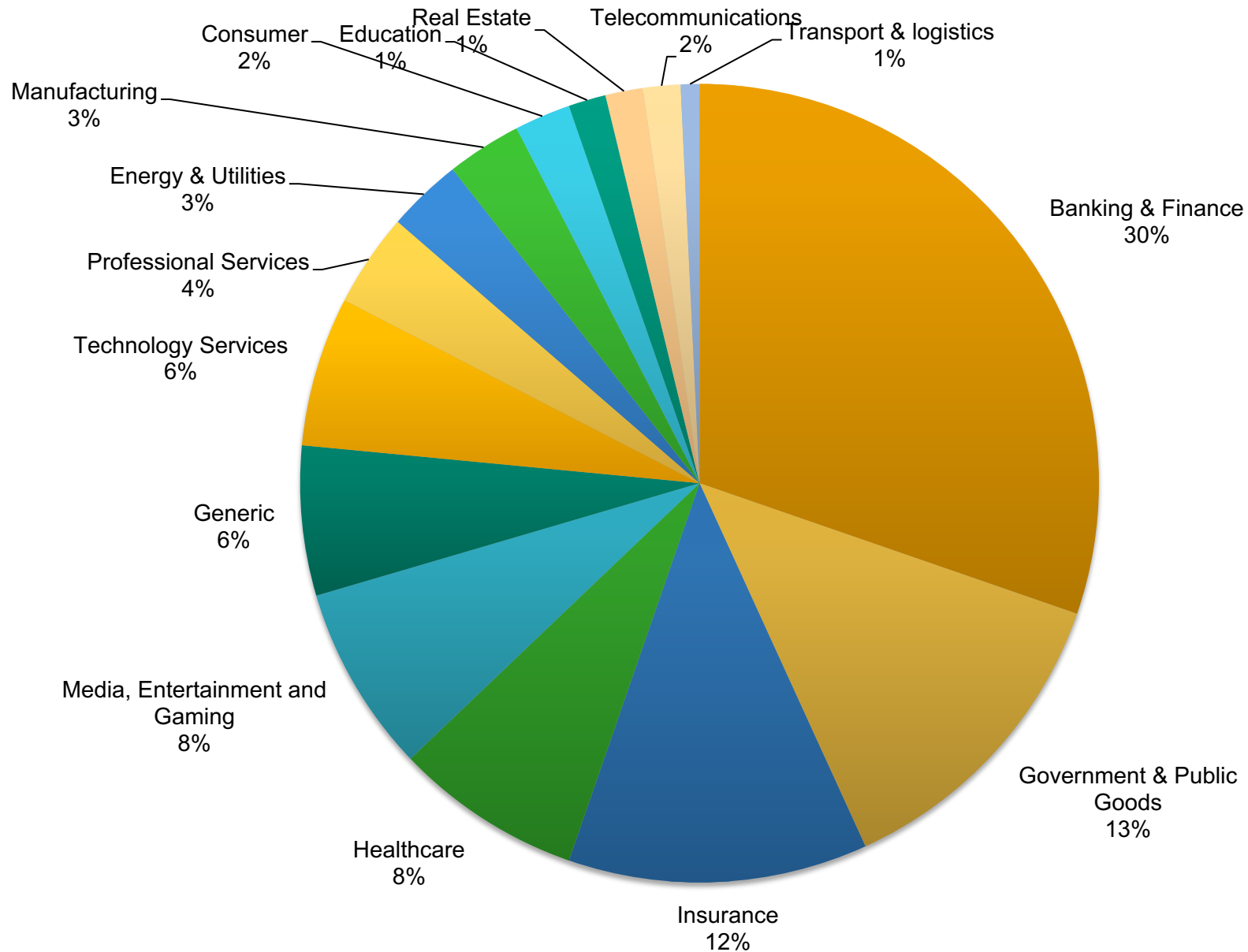
# **Use Cases and Business Models**

## 133 identified DLT/blockchain use cases by industry sector

Industry	Use Cases
Technology Services	Supply chain management
Banking & Finance	Netting and clearing
Government	Central Bank digital currency
Insurance	Claims management
Healthcare	Electronic medical records
Media	Copyright database

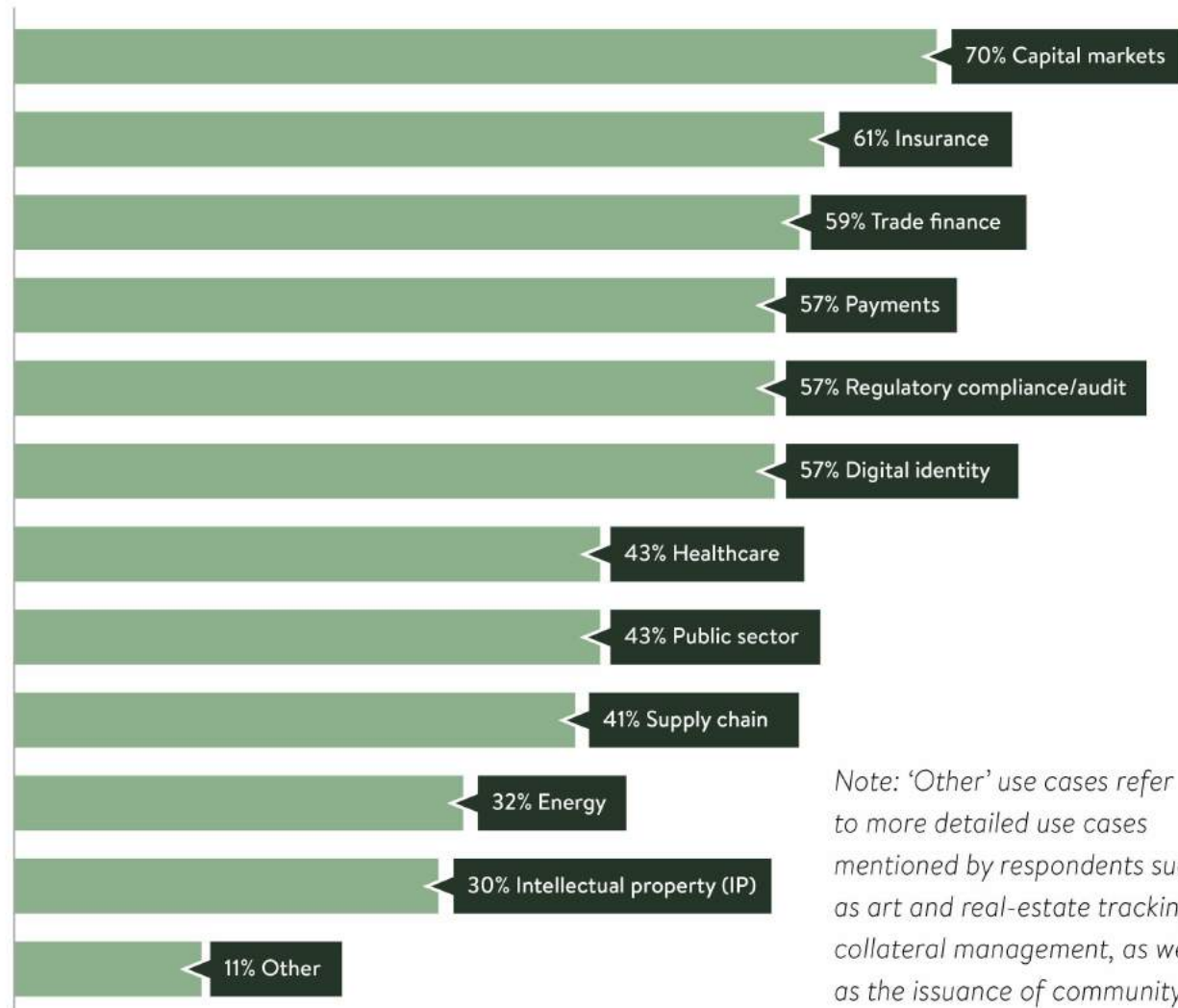


# Banking and finance has the most publicly identified use cases, followed by insurance and government



# Financial services and banking are the most frequently targeted sectors for DLT; increasing attention is given to non-monetary use cases

% of DLT service providers targeting different sectors/use cases



*Note: 'Other' use cases refer to more detailed use cases mentioned by respondents such as art and real-estate tracking, collateral management, as well as the issuance of community currencies and loyalty points.*

# Banking and finance-related tokens command the majority of value amongst cryptocurrencies

## Market value of tokens by sector

Industries	Combined Market Value (\$)	Market Value Share %
Banking and Finance	\$92,050,673,900	70.4%
Technology Services	\$36,672,438,026	28.0%
Media and Entertainment	\$1,513,689,080	1.2%
Consumer Goods and Retail	\$209,897,687	0.2%
Government and Public Goods	\$183,621,933	0.1%
Professional Services	\$86,894,719	0.1%
Manufacturing	\$45,215,838	0.0%
Healthcare	\$32,039,770	0.0%
Telecommunications	\$0	0.0%
Insurance	\$0	0.0%
Energy	\$0	0.0%
Transportation	\$0	0.0%
<b>TOTAL</b>	<b>\$130,794,470,953</b>	<b>100%</b>

## Number of tokens by sector

Industries	Number of Tokens	Token Number Share (%)
Banking and Finance	50	48.5%
Technology Services	30	29.1%
Media and Entertainment	14	13.6%
Consumer Goods and Retail	3	2.9%
Government and Public Goods	2	1.9%
Professional Services	2	1.9%
Manufacturing	1	1.0%
Healthcare	1	1.0%
Telecommunications	0	0.0%
Insurance	0	0.0%
Energy	0	0.0%
Transportation	0	0.0%
<b>TOTAL</b>	<b>103</b>	<b>100%</b>

# **Challenges and Interoperability**

# Legal risks and an unclear regulatory environment are key inhibitors of broader DLT adoption

Lowest average score  Highest average score

1: Strongly agree    2: Somewhat agree    3: Neither agree nor disagree    4: Somewhat disagree    5: Strongly disagree

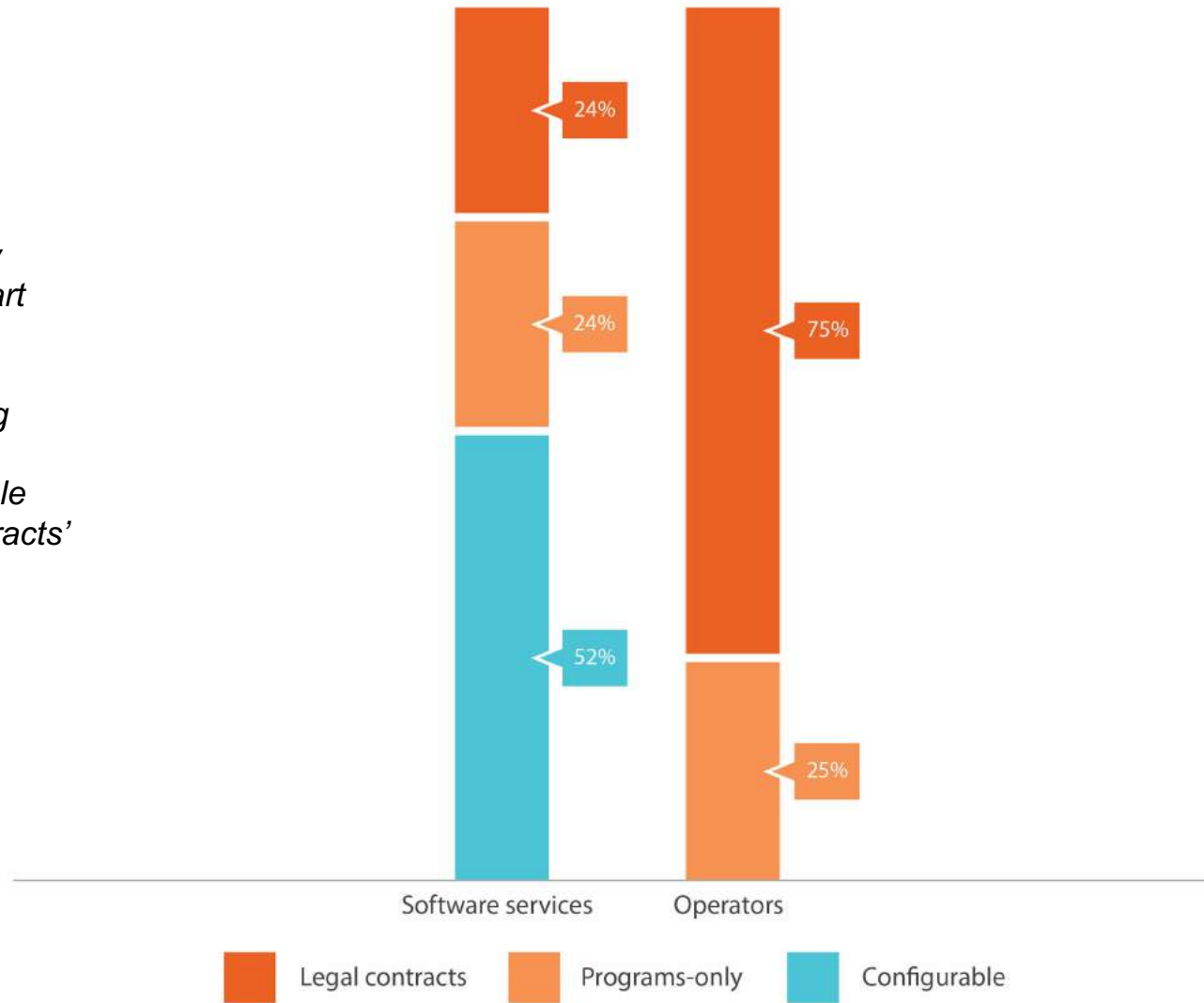
CHALLENGES TO BROAD DLT ADOPTION	WEIGHTED AVERAGE	INFRASTRUCTURE PROVIDERS	APPLICATION DEVELOPERS	OPERATORS
Legal risks/regulatory framework	<b>1.97</b>	2.25	1.60	1.64
Confidentiality issues	<b>2.09</b>	2.05	2.20	2.10
Reluctance to change established business processes	<b>2.17</b>	2.47	2.00	1.73
Immature technology	<b>2.28</b>	1.85	3.20	2.64
Difficulty of building business network	<b>2.44</b>	2.45	2.20	2.55
Potential issues with data protection laws	<b>2.60</b>	2.85	2.80	2.00
Scalability/performance concerns	<b>2.81</b>	2.70	2.80	3.00
Reluctance to give up some control	<b>2.88</b>	3.05	2.60	2.70
Security concerns	<b>2.91</b>	2.95	2.80	2.89
Unknown costs/benefits	<b>3.08</b>	3.14	3.60	2.70
Lack of suitable use/business case	<b>4.00</b>	4.10	4.00	3.82

Note: The lower the score, the more important the challenge is considered (1: very significant challenge; 5: no challenge at all).

# The majority of industry actors integrate smart contracts with the legal system

Level of support for smart contract code vs. smart legal contracts

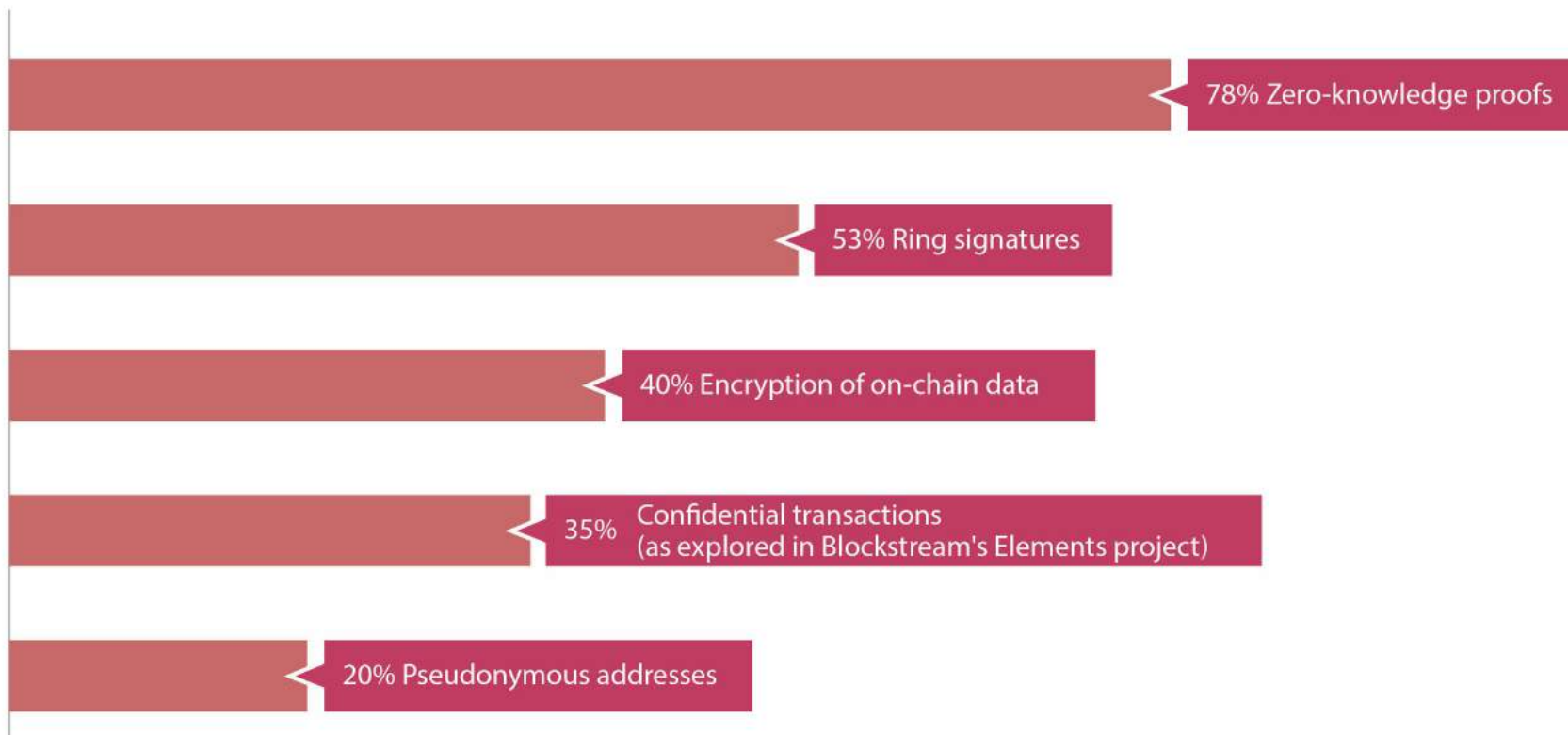
*In practice, many operators tie smart contract code to existing legal contracts, making them effectively legally enforceable 'smart legal contracts'*



# The majority of roadmaps include the implementation of zero-knowledge proofs and ring signatures

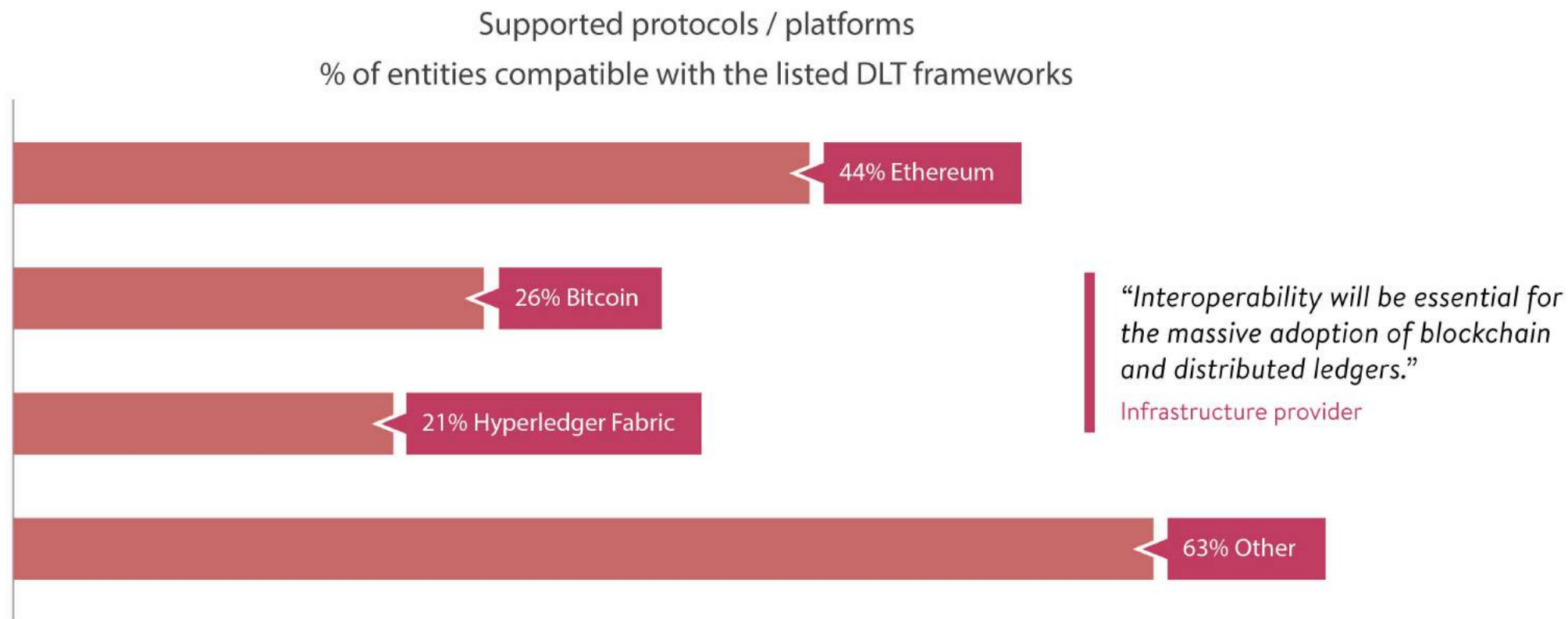
## Privacy-enhancing techniques on current roadmap

% of entities not having implemented the listed techniques yet planning to do so



*57% of roadmaps include support for more privacy-enhancing techniques*

# DLT interoperability is most common with Ethereum, Bitcoin and Hyperledger Fabric



*Note: In this context, supporting a DLT framework means that the service is compatible with the listed frameworks, but does not necessarily mean that a particular framework is used in practice.*



# **Public Sector Blockchain Data**

We conservatively estimate that more than 500 public sector staff are working full-time on various DLT-related activities

## ESTIMATED NUMBER OF PUBLIC SECTOR STAFF WORKING ON DLT



**500+**

STAFF WORKING  
FULL-TIME ON DLT

# Central banks have in general more staff working on DLT-related activities than OPSIs

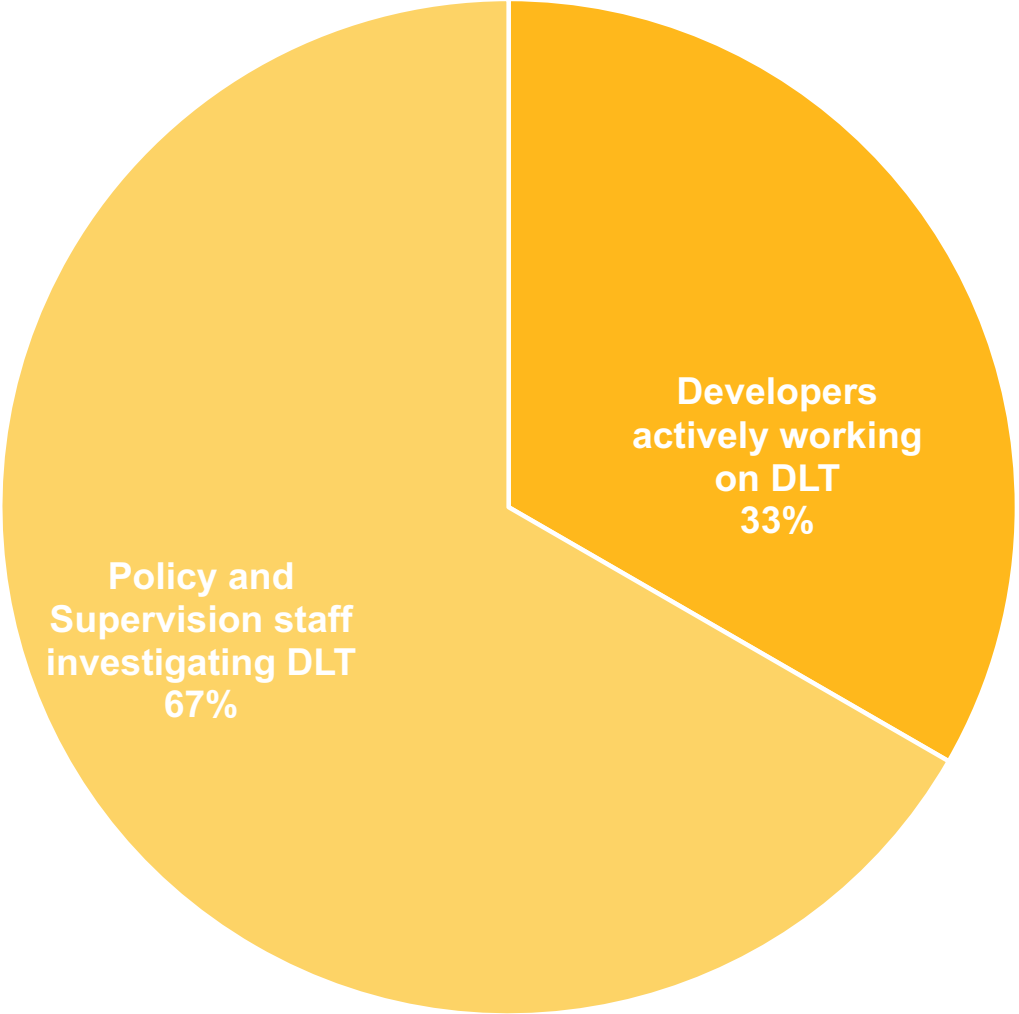
*Distribution ranges from a single staff member to up to 30 (central banks) and 50 members (OPSIs)*

*One central bank reported that one-third of DLT staff are working on technical development*

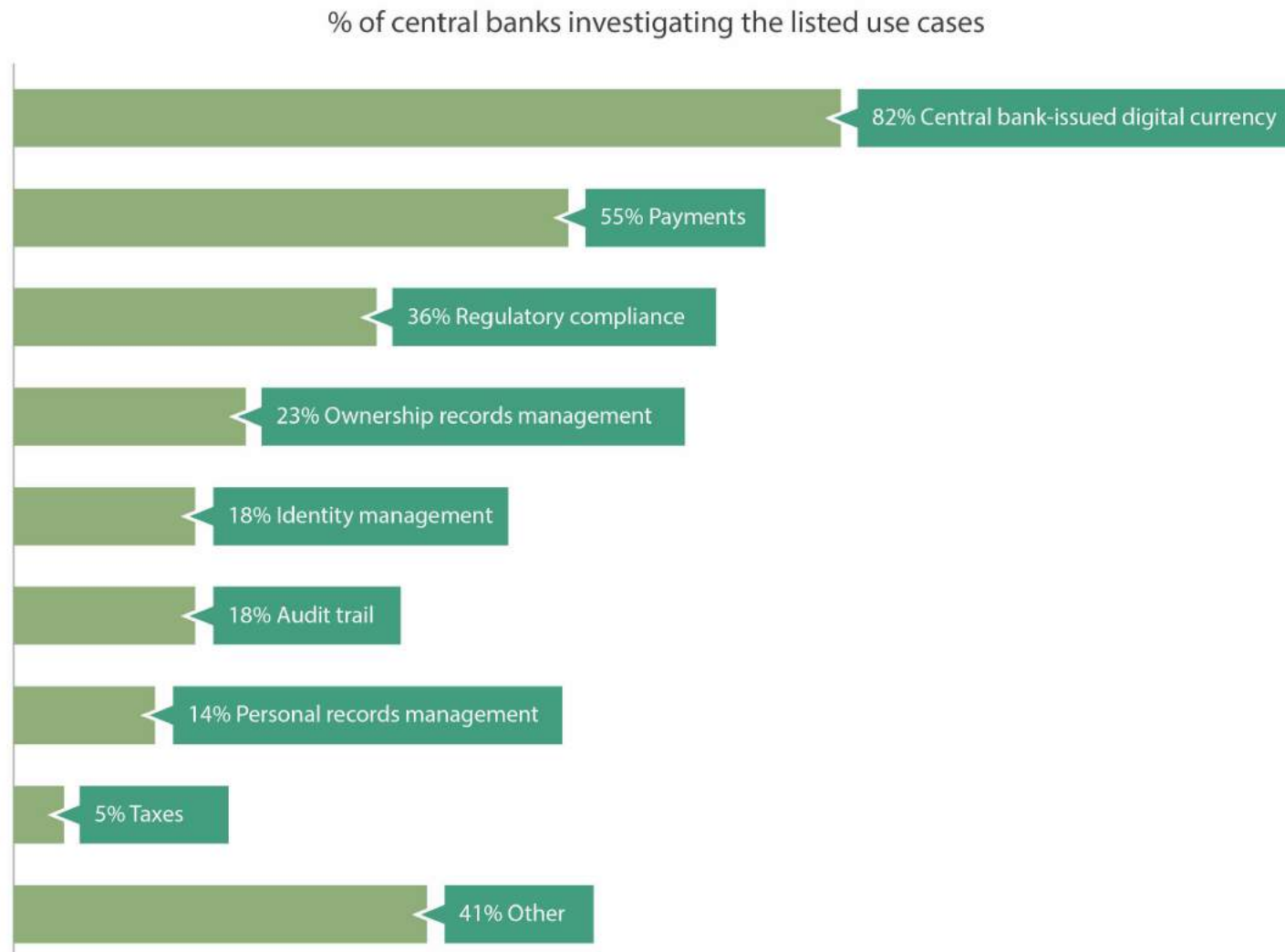
Staff working full-time on DLT



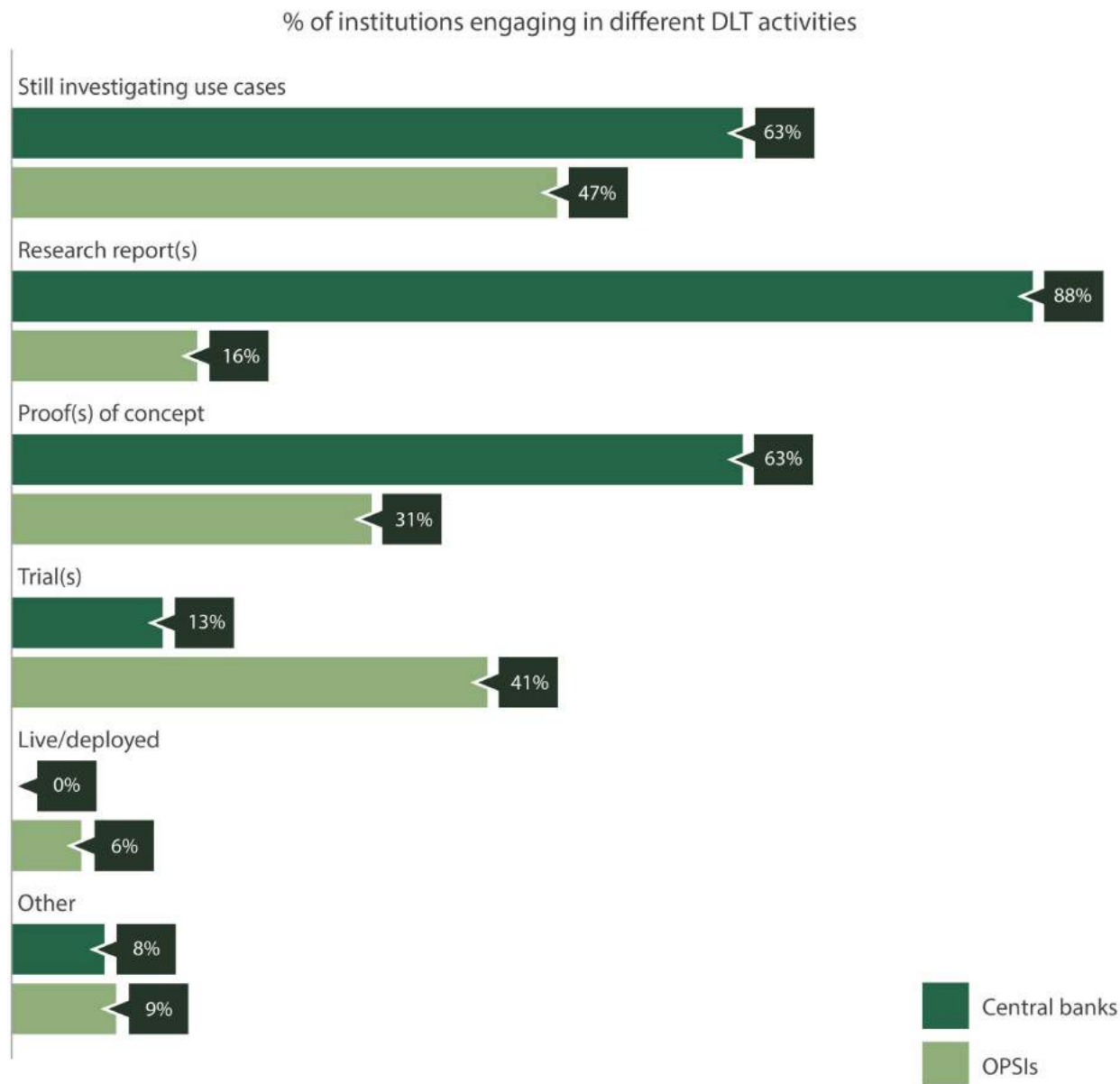
# Staffing Mix: at central banks twice as many staff working on DLT policy/supervision as tech



# Central banks are investigating a wide range of DLT uses beyond digital currency and payments

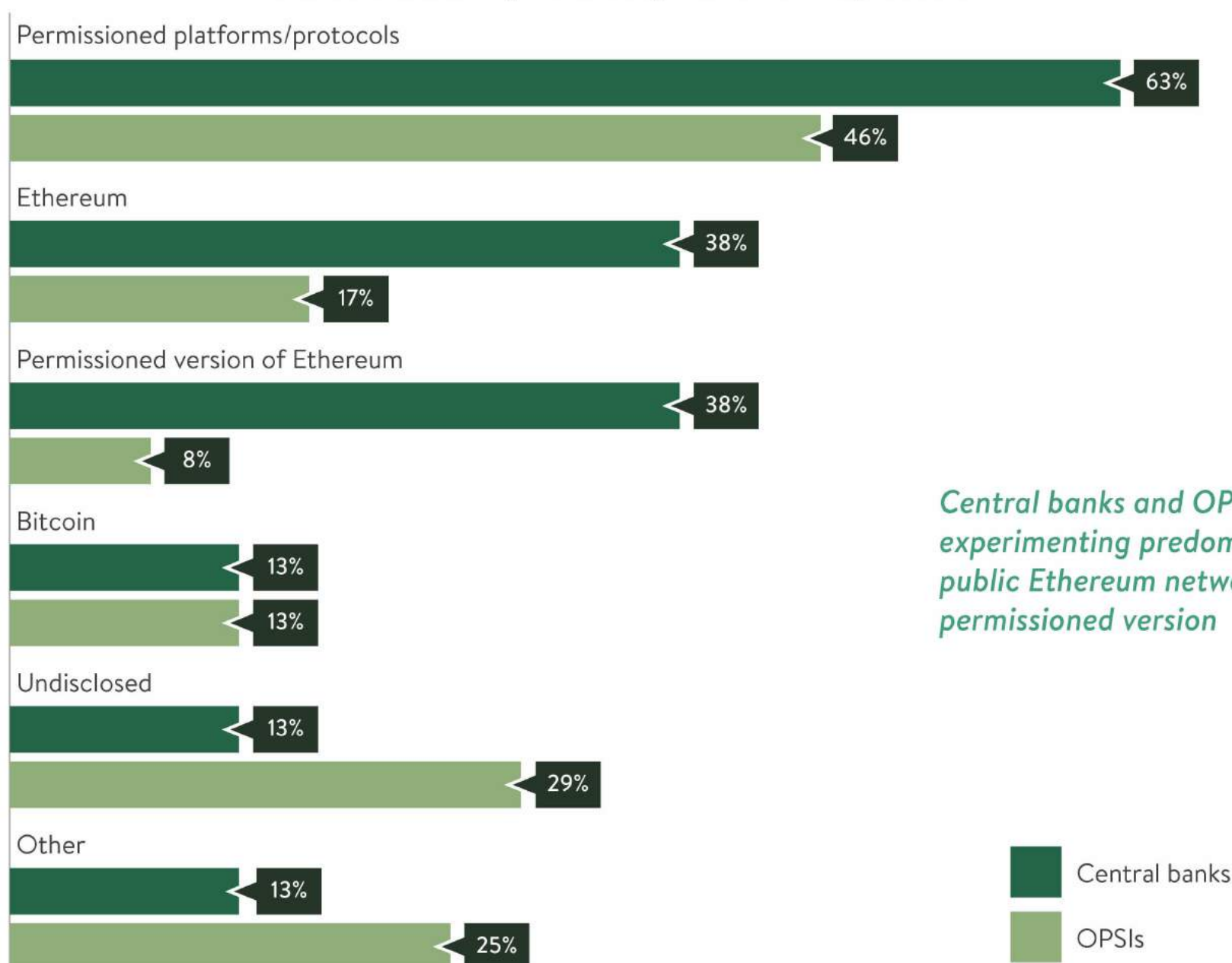


# Central banks are engaged in more activities, but OPSI activities are more advanced in terms of deployment



# Ethereum is more frequently used by central banks than by OPSIs

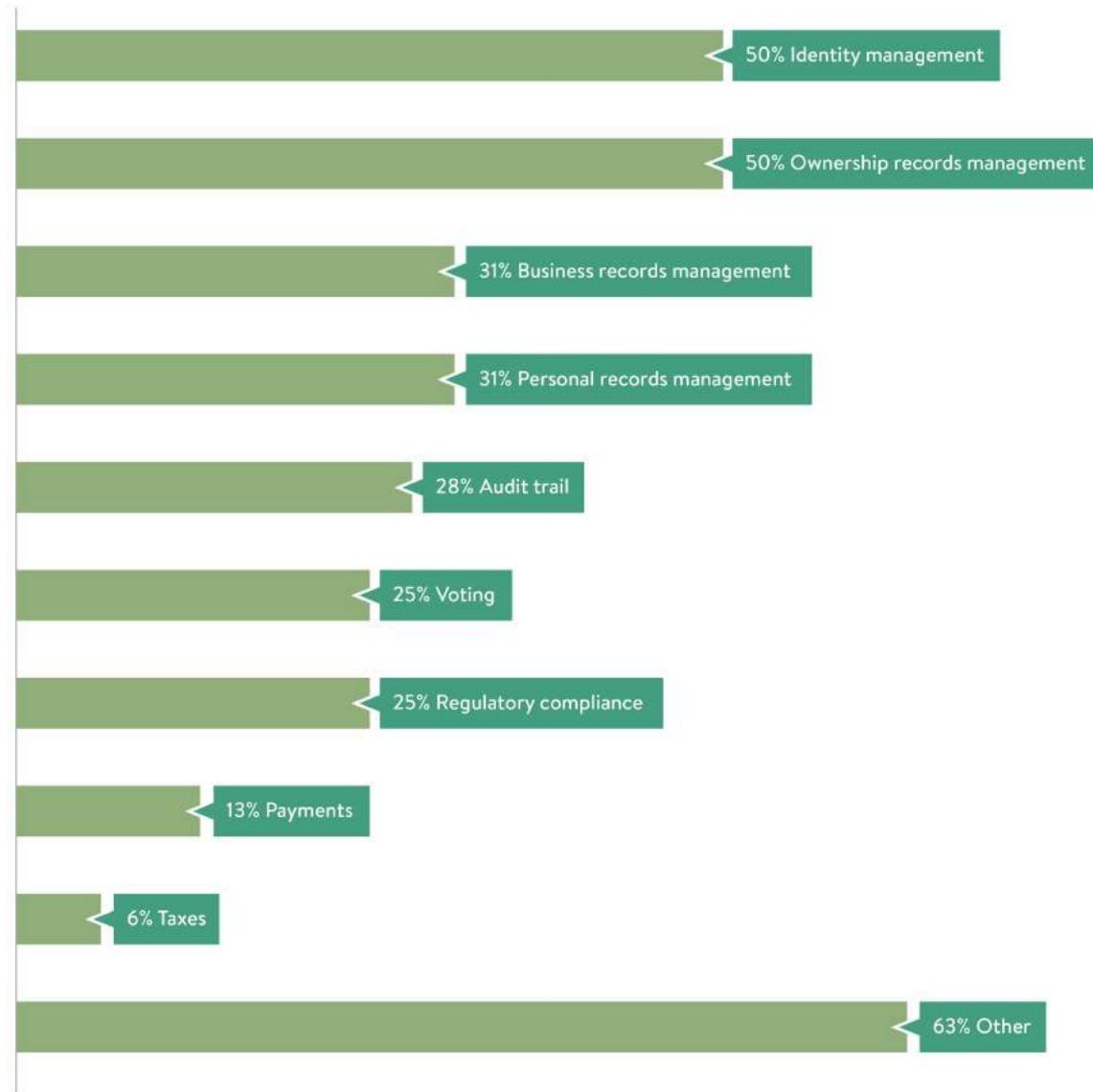
% of institutions experimenting with the listed protocols



*Central banks and OPSIs are experimenting predominantly with the public Ethereum network rather than a permissioned version*

# OPSI are exploring a wide variety of DLT use cases, with managing identities and ownership records most common

% of OPSIs investigating the listed use cases



*72% of OPSIs are exploring two or more different use cases, compared to 53% of central banks*



# GLOBAL CRYPTOCURRENCY BENCHMARKING STUDY

Dr Garrick Hileman & Michel Rauchs  
2017



Cambridge  
Centre  
for Alternative  
Finance



With the support of:

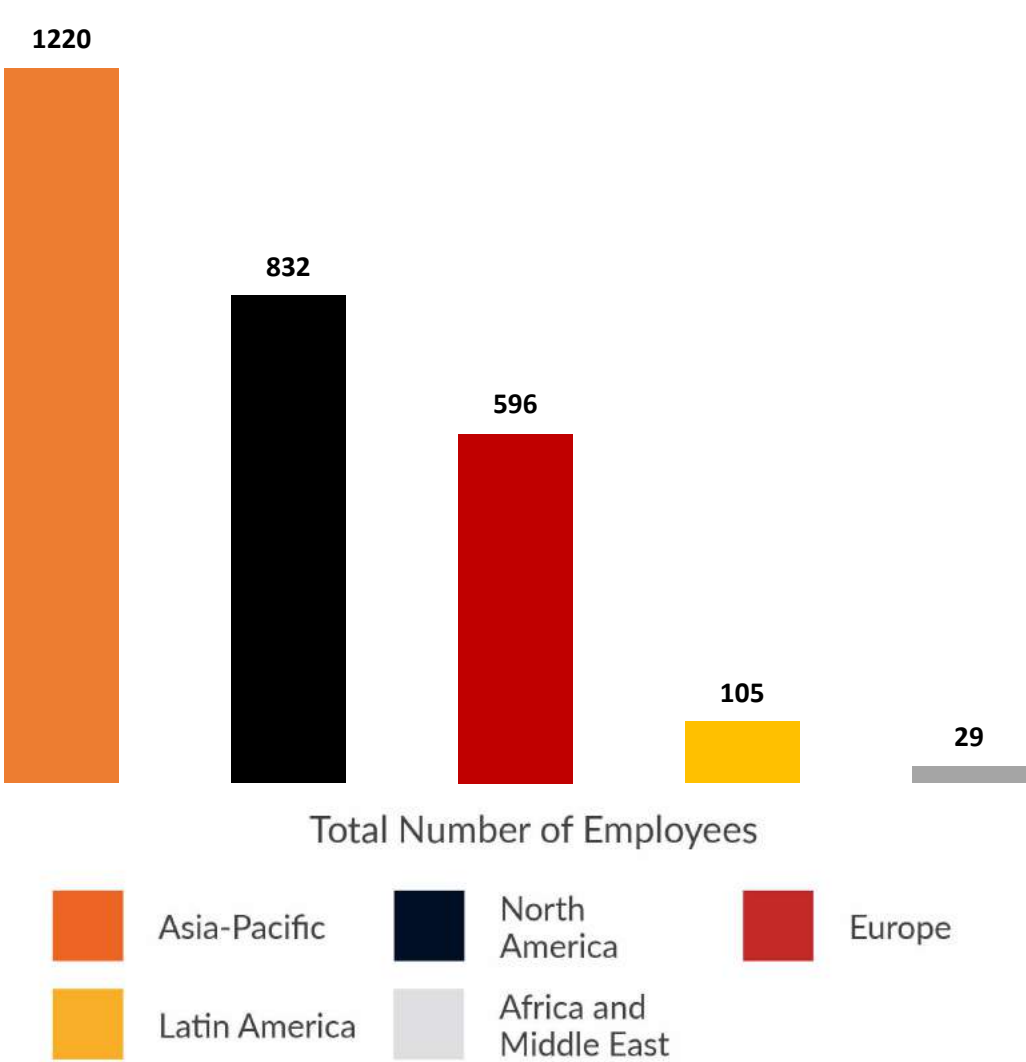


Cambridge Centre for Alternative Finance  
10 Trumpington Street  
Cambridge CB2 1QA  
United Kingdom  
E: ccaf@jbs.cam.ac.uk  
T: +44 (0)1223 339111

# Over hundred cryptocurrency companies as well as 30 miners included in study sample



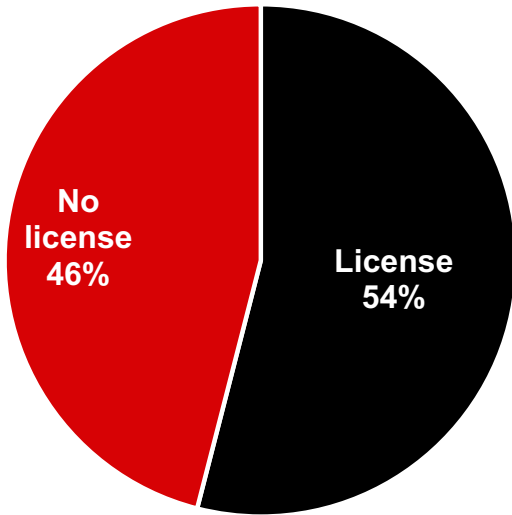
# Employment: at least 2,782 people are employed in the cryptocurrency industry; Asian-Pacific and North American firms have most headcount



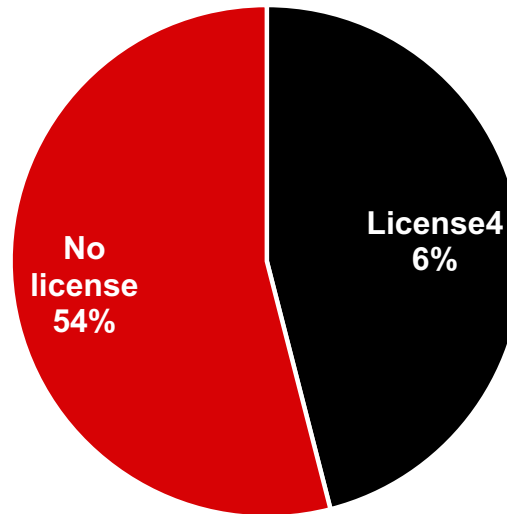
*\*Note: Well in excess of 3000 people likely work in the industry as this figure does not include dApps and companies that did not respond to the survey.*

Regulation: over half of payment companies hold a government license compared to 46% of exchanges and 24% of incorporated wallets

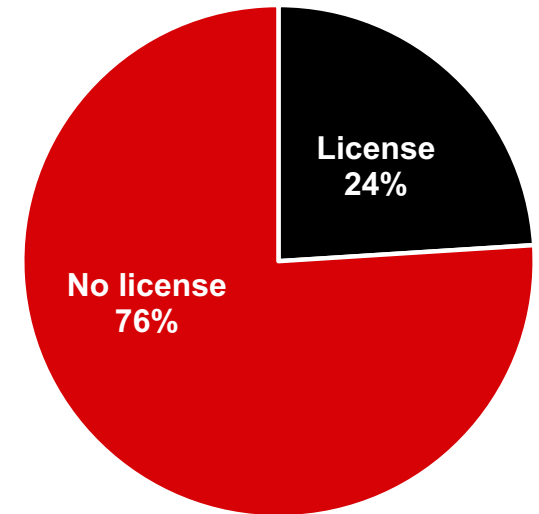
Payment Service Providers

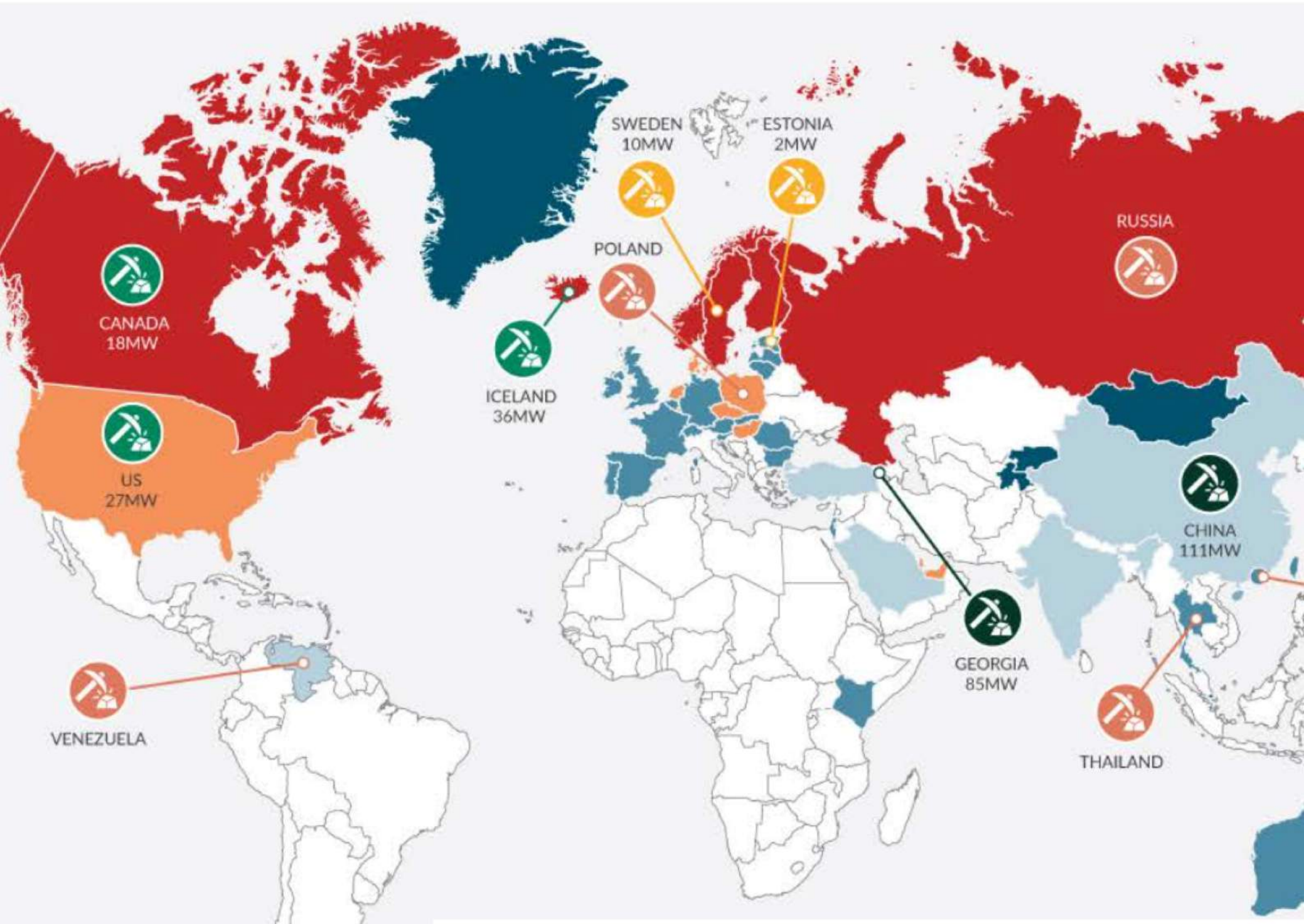


Exchanges



Incorporated wallets

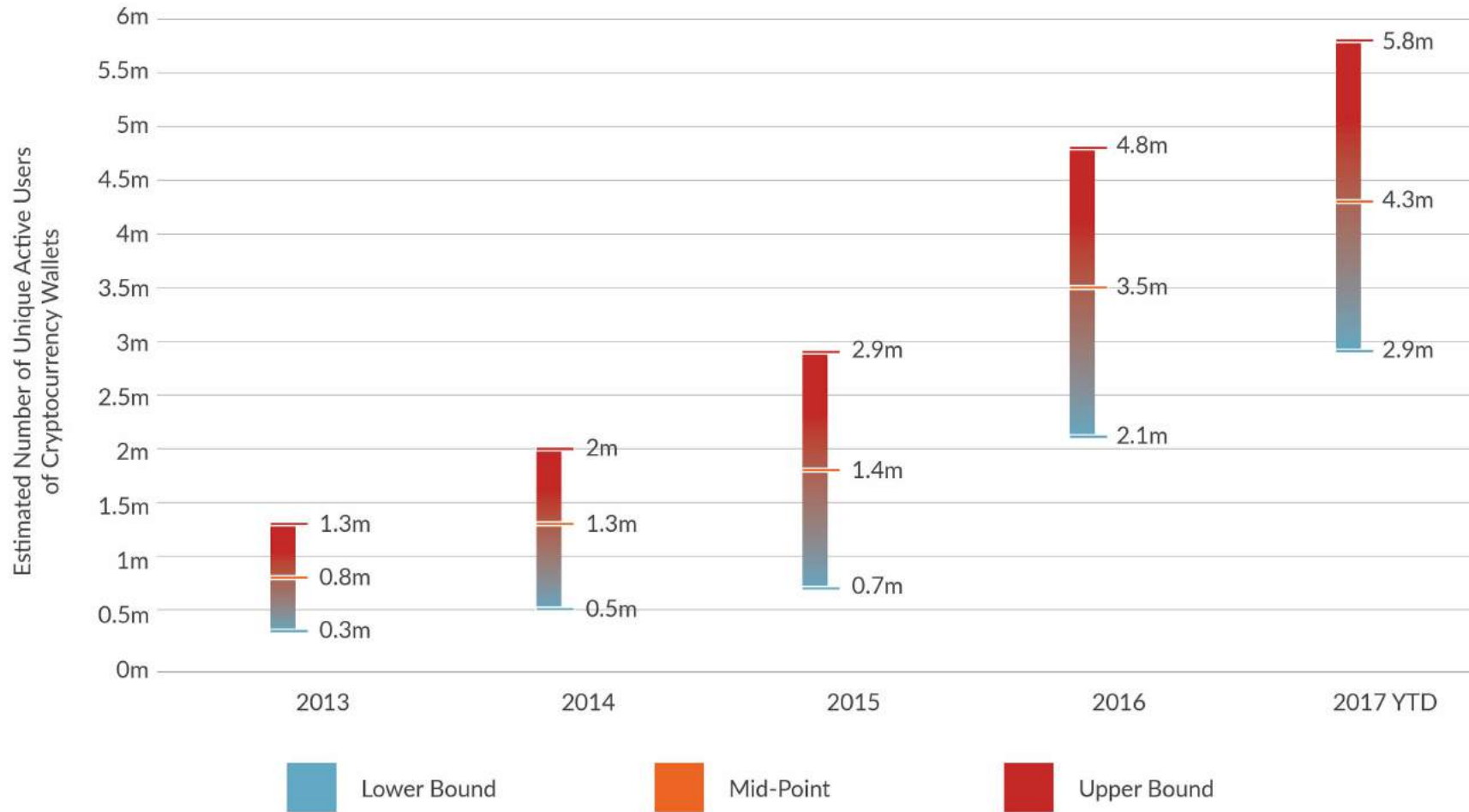





# China Cryptocurrency Mining Map



# Adoption: estimated number of *unique* and *active* users of cryptocurrency of 15-30 million



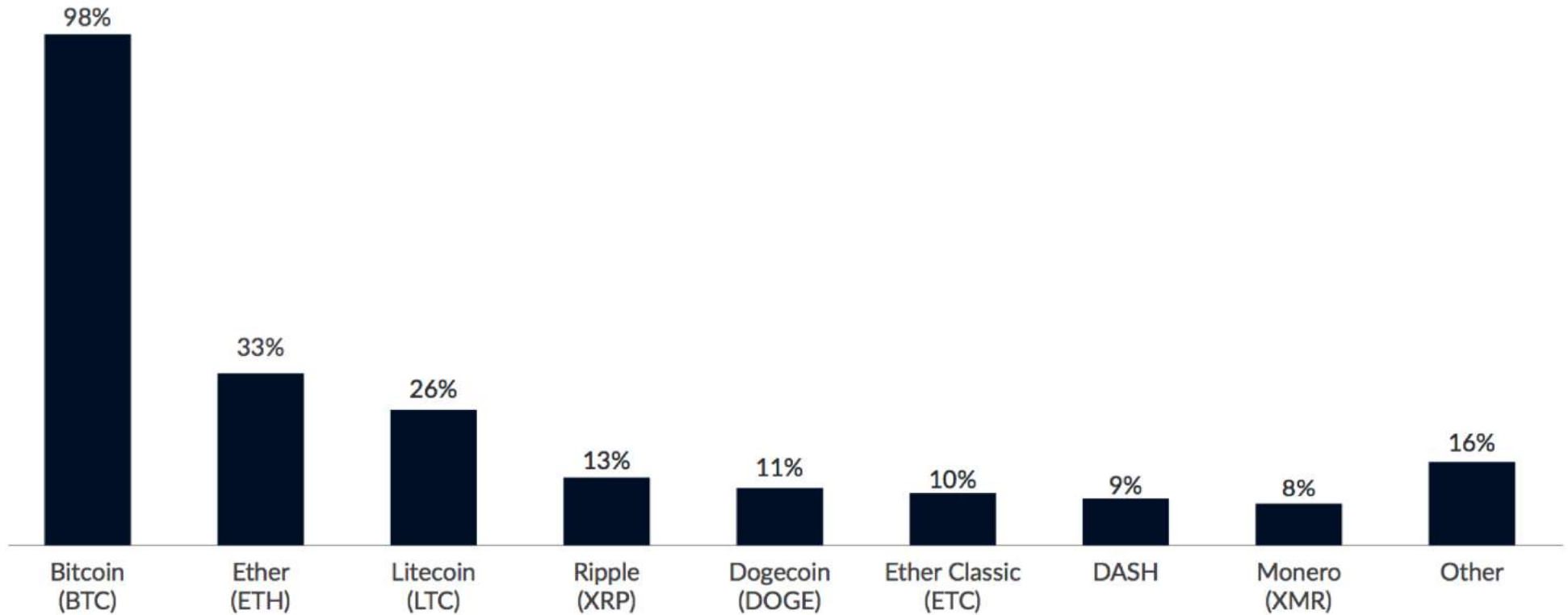
*Including exchanges and other services we estimate 5-10m unique total users of cryptocurrency in April 2017*



39% of wallets already offer multi-cryptocurrency support, and 31% of wallets that currently do not offer multi-cryptocurrency support have this feature on their roadmap

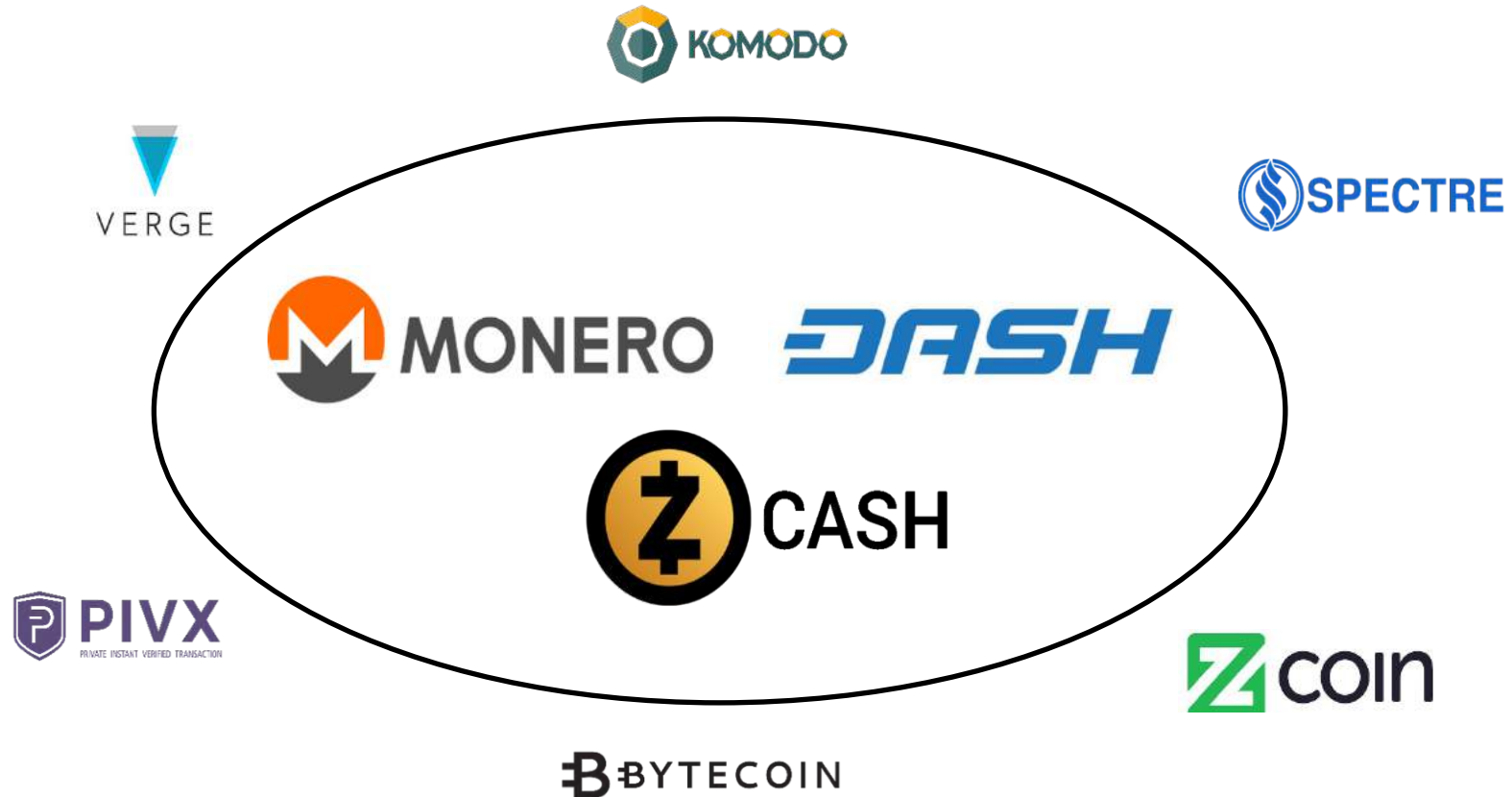


# Bitcoin still far and away the most widely supported cryptocurrency at exchanges, wallets, etc., but others gaining

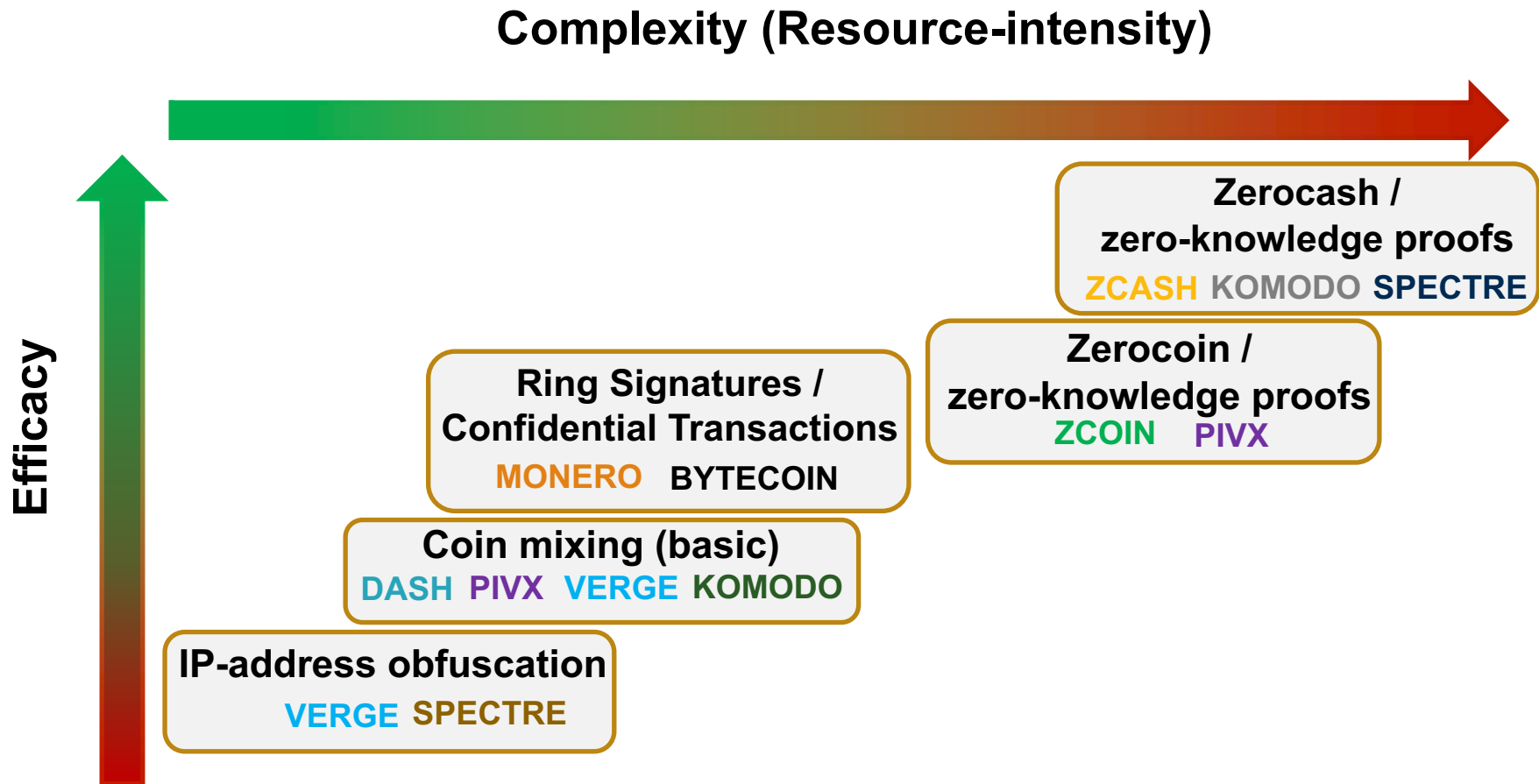


# **Beyond Bitcoin**

# Privacy coins: three main players dominate a host of competitors on the periphery



Each uses of a combination of technologies of varying efficacy and computational complexity



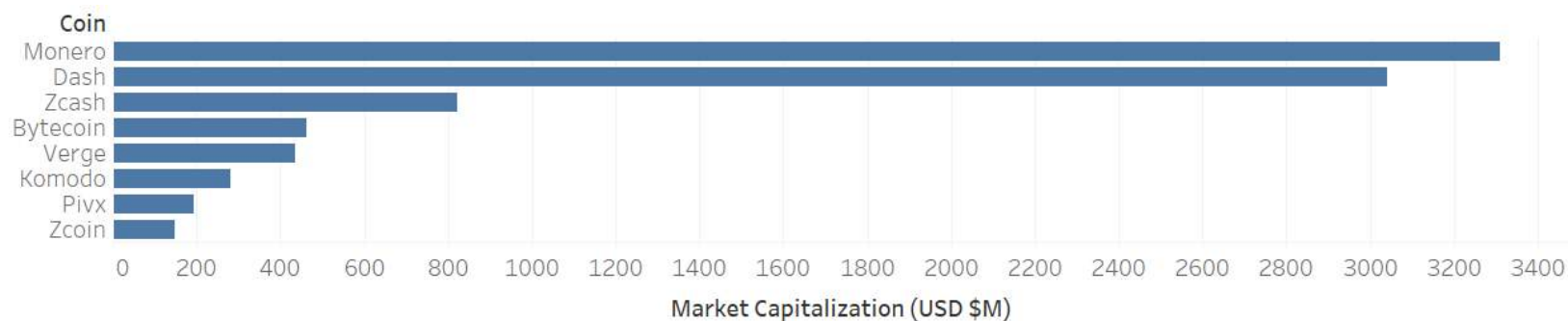
# The class has benefited immensely from crypto's 2017 valuation explosion...



March 2017

**\$559M**

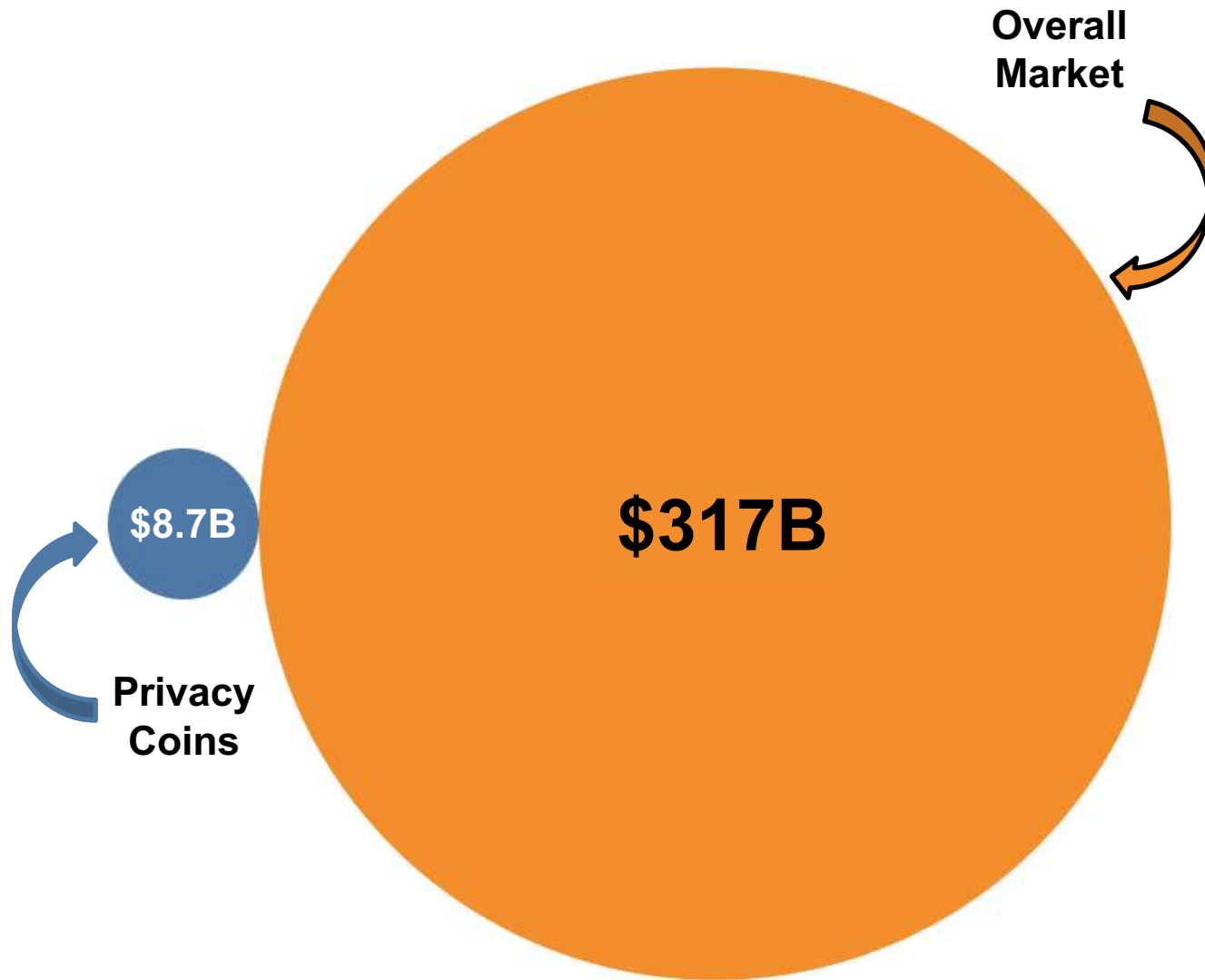
↓ **15x**



March 2018

**\$8,690M**

... but is still dwarfed by the overall market



\*Respective market capitalizations of top 8 privacy coins and overall market (including privacy coins) as of 19 March 2018

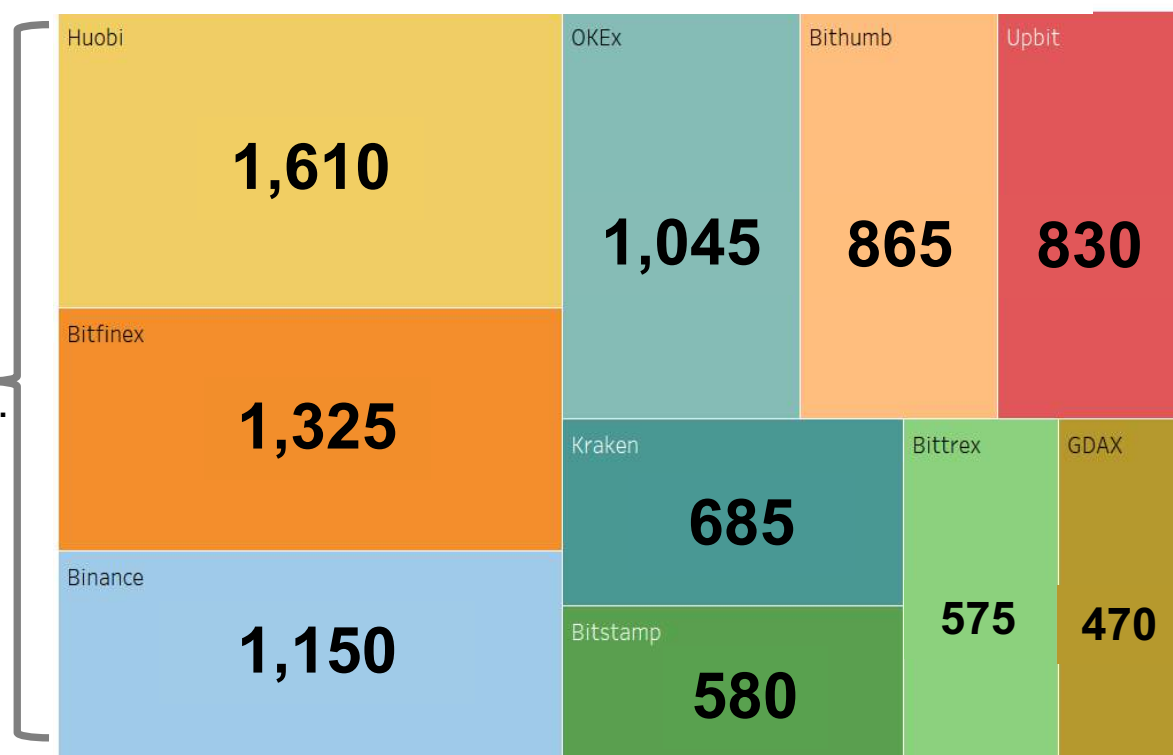
# Decentralized exchanges (DEX) can disrupt a surging centralized cryptoasset exchange market

DEX will likely claim a piece of the market by:

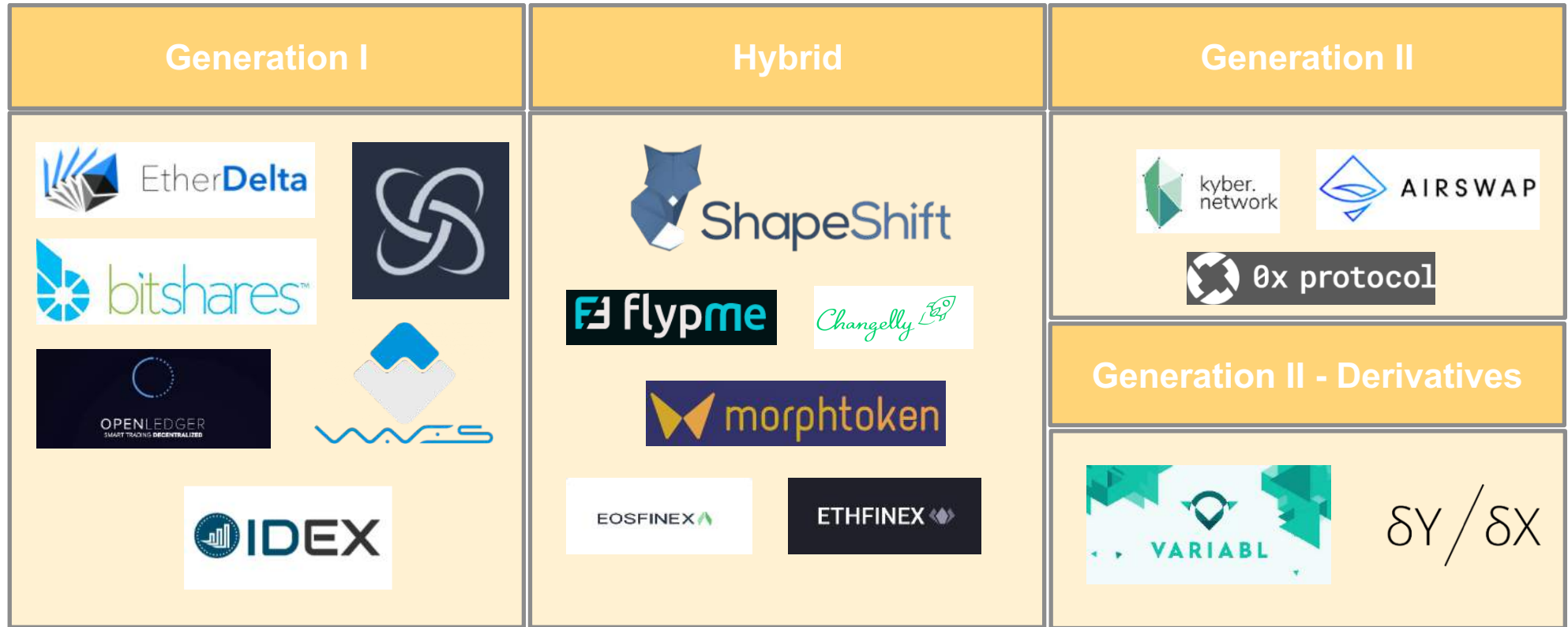
- Reducing counterparty/custodial risk (hacks, embezzlement)
- Limiting dependence on traditional institutional entities (banks, clearing houses)
- Providing transparent settlement via auditable smart contracts
- Creating deeper liquidity pools through combination of centralized exchange order books

**\$9B+**  
and growing...

## CEX Annualized Fee Revenue (est. USD \$M)

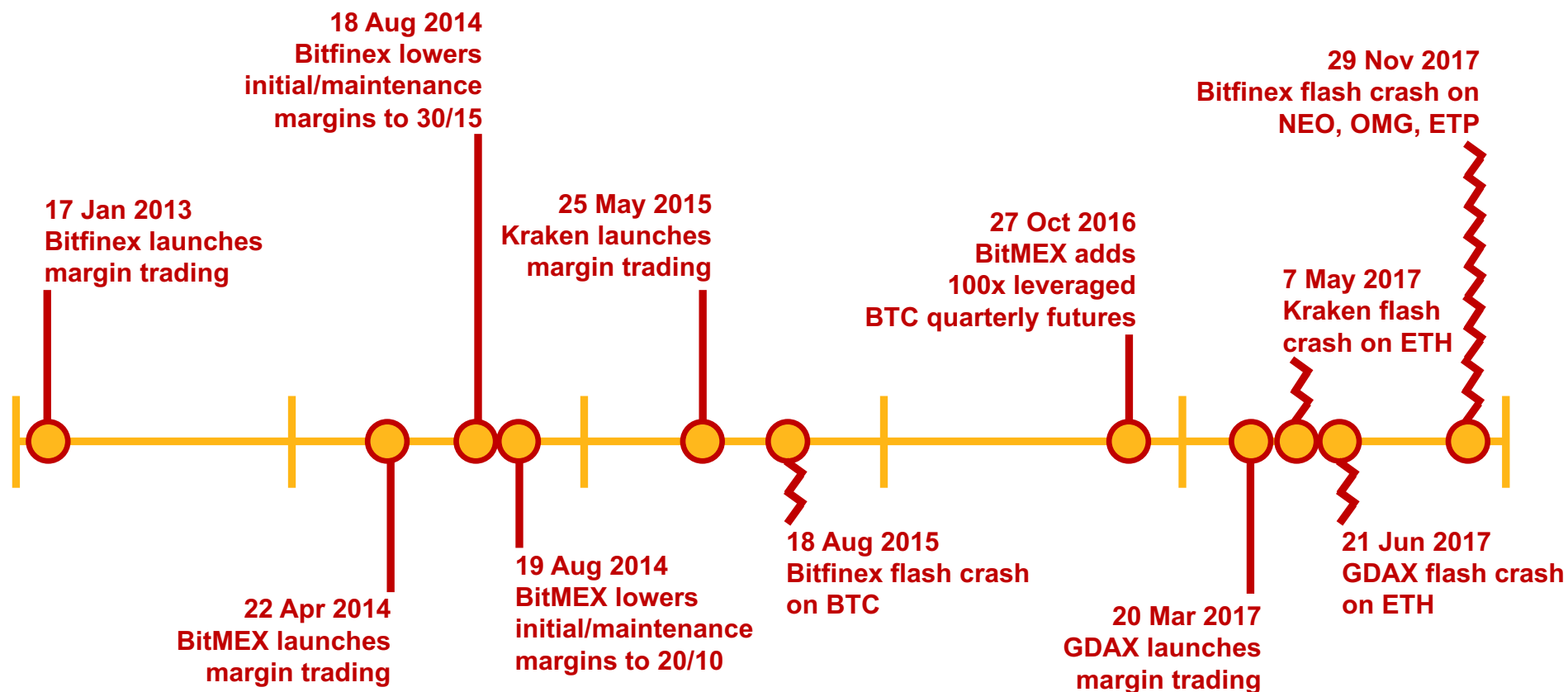


Functionality issues, exploits have kept DEX penetration low (<<1% by vol.); new entrants + hybrids can fare better

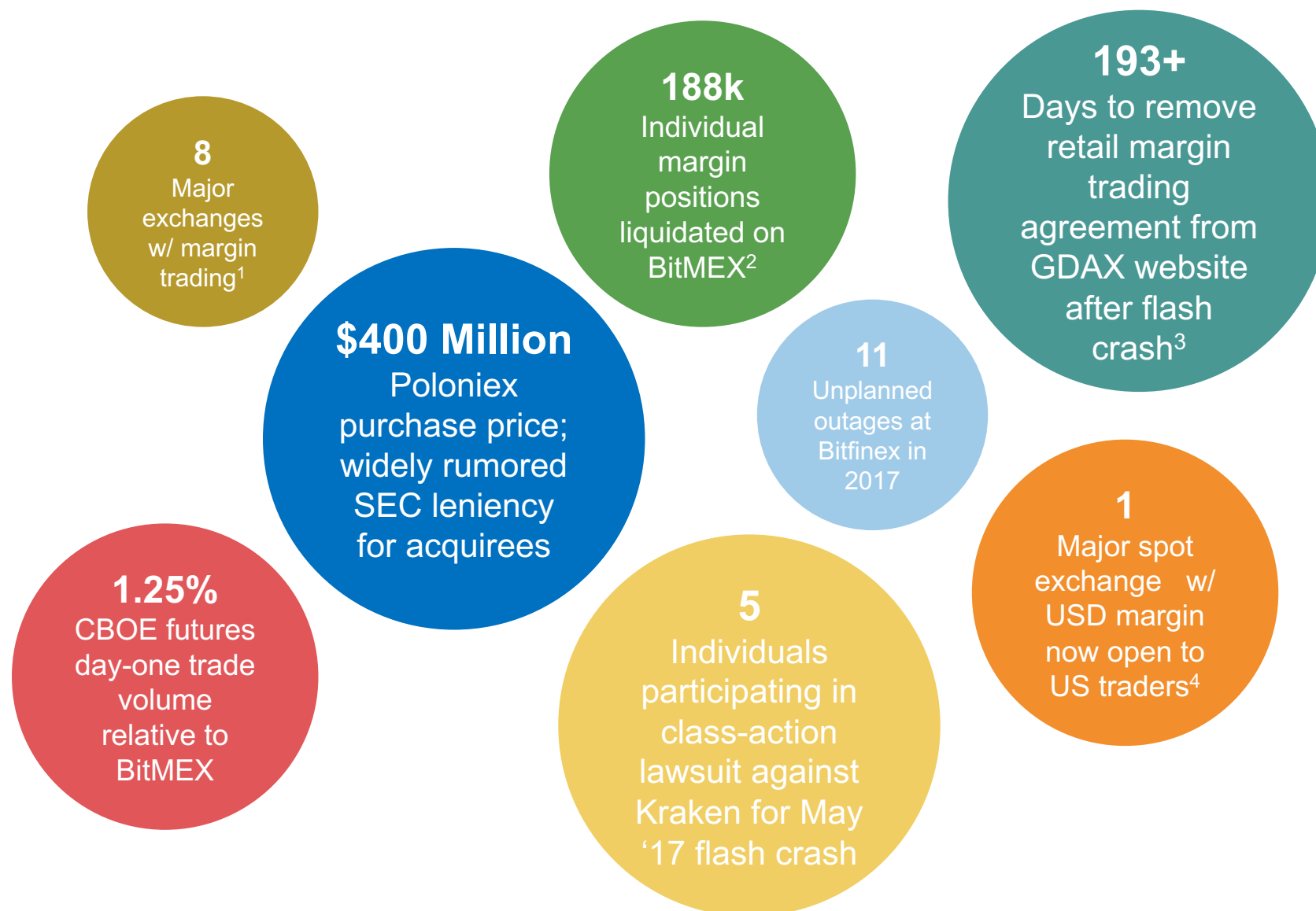




# Margin has fueled speculation on many crypto exchanges; flash crashes more likely on thinly-traded books



# Regulation, maturation of existing platforms, and consolidation will likely play a larger role in 2018

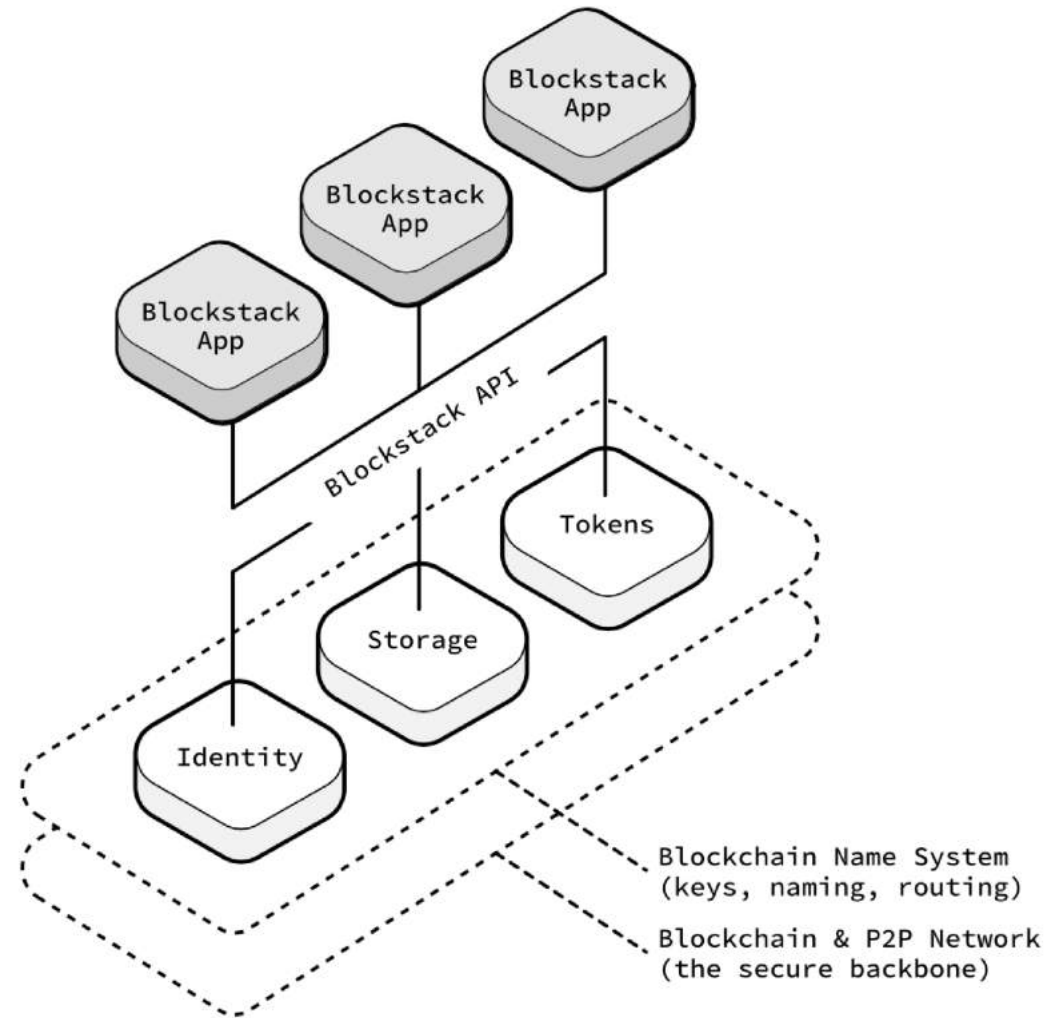


# Internet 2.0 – a new, decentralized web



*“Blockchains can help us advance from a ‘don’t be evil’ world to a ‘can’t be evil’ world.”*

Muneeb Ali, Blockstack Co-Founder



**Will cryptocurrencies become more widely adopted and used?**

# A view from Silicon Valley...



By Darryn Pollock

NOV 09, 2017

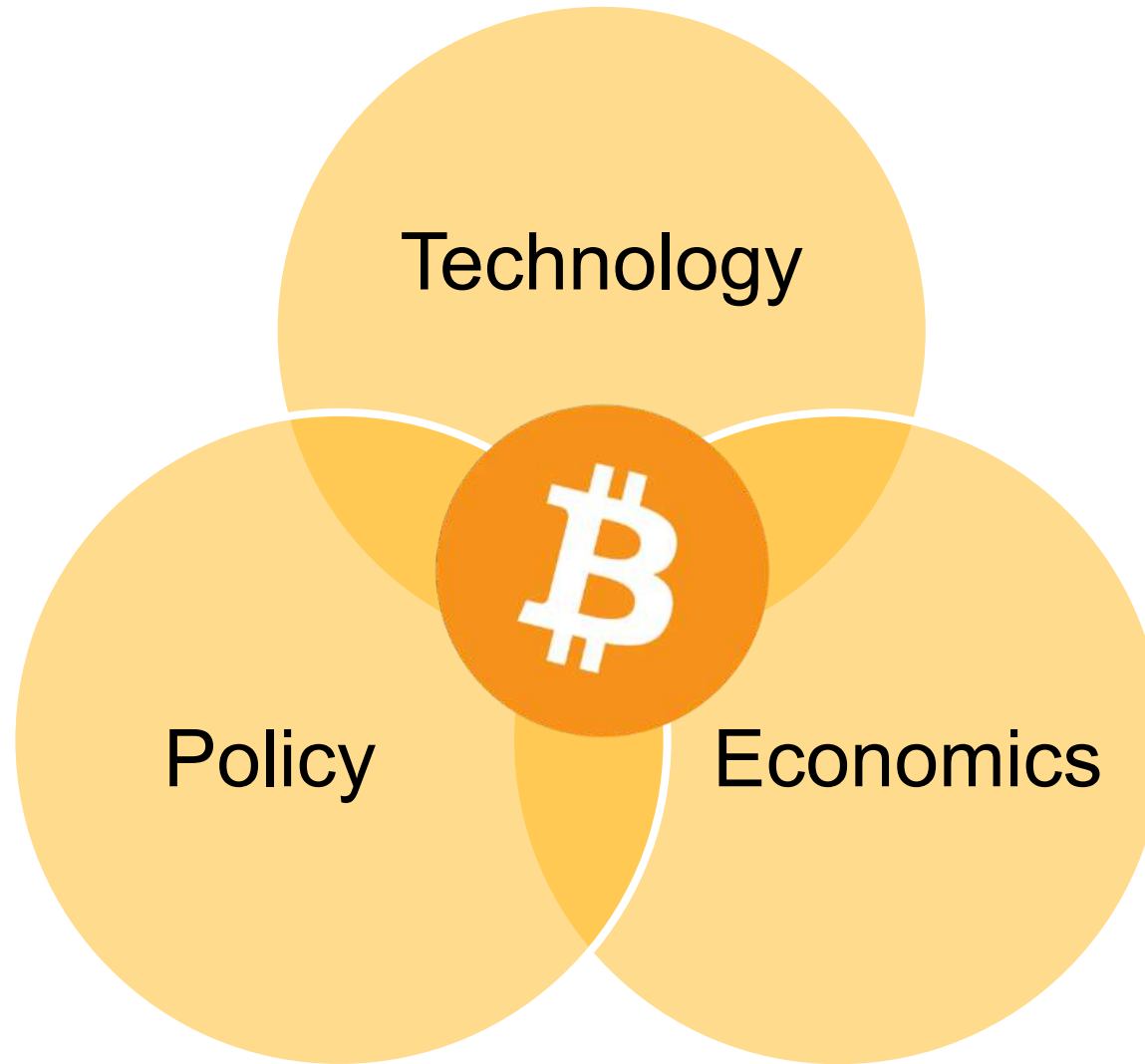
## Fiat Currency Will be Laughable in Five Years Says Billionaire Tim Draper

30402 Total views 1777 Total shares



*"In five years, if you try to use fiat currency, they will laugh at you. Bitcoin and other cryptocurrencies will be so relevant ... there will be no reason to have the fiat currencies."*  
– **Tim Draper, VC**

Cryptocurrency is situated at a complex, continuously evolving three-way intersection



# Cryptoasset (store of value) vs. Cryptocurrency (medium of exchange)



**Vs.**



**+**



# Death by regulation

- Started by Austrian town during Great Depression to kickstart economy
- Featured demurrage – cost built into holding currency
- Banned by Austrian Central Bank in 1933





# Death by lack of adoption

- LETS is a barter-based currency system started in UK
- Began in late 1980s following UK leaving European Exchange Rate Mechanism (ERM)
- Steady decline due to declining use: 350 chapters in 1995, 303 in 2001, 186 in 2005, etc.



Not everyone wants to “be your own bank”

---

**UK news**

---

## Cryptocurrency trader 'forced at gunpoint to make bitcoin transfer'

**Police seek witnesses after four armed men break into family home in Moulsoford, Oxfordshire**

#WORLD NEWS DECEMBER 29, 2017 / 10:34 PM / A MONTH AGO

## Ukraine kidnappers free bitcoin analyst after \$1 mln ransom paid

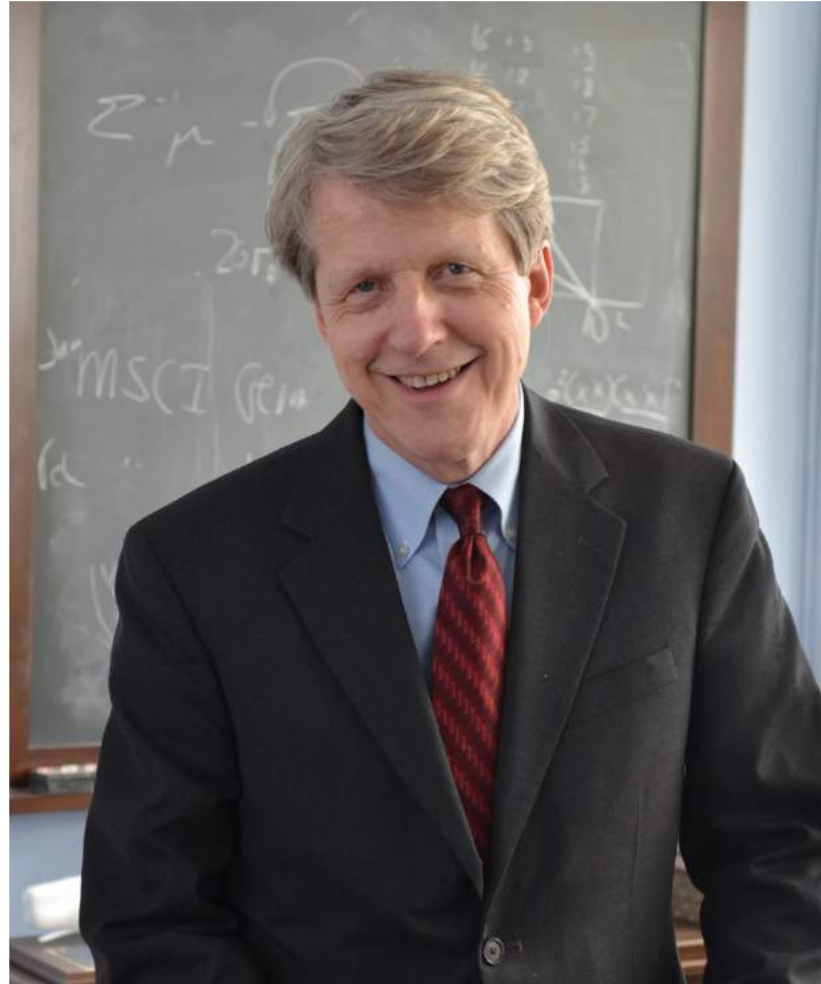
“I’ll use bitcoin when I’m paid in bitcoin!”



“How much a bitcoin is worth, nobody knows.”

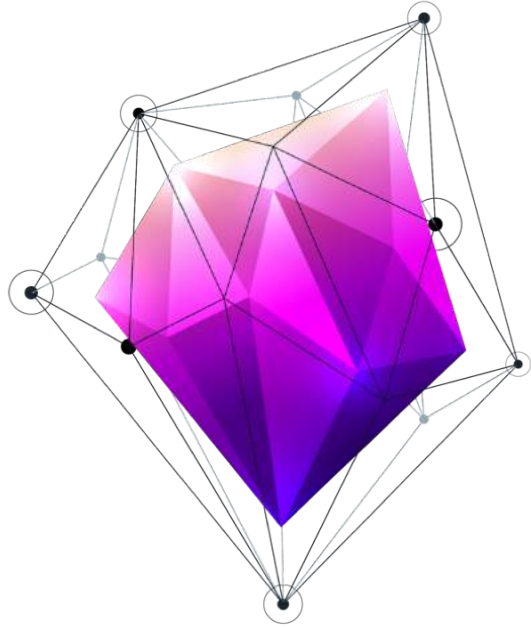


**Thomas Peterffy**  
Chairman, Interactive Brokers



**Robert Shiller**  
Nobel Prize winner

Cryptoasset valuation frameworks are in their nascency



**mosaic**

**Mosaic.io**

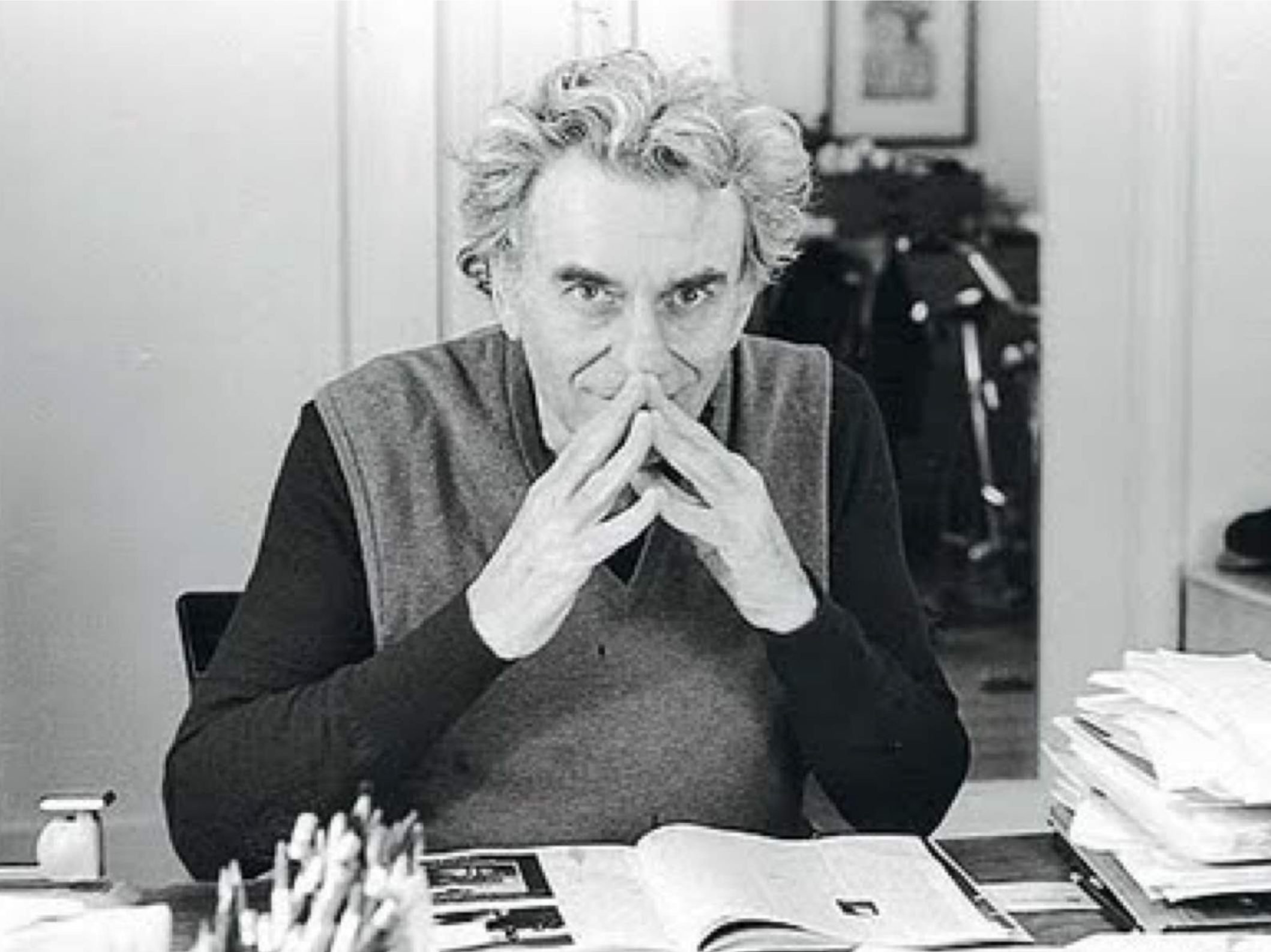
# Merchant tokens – history's most successful alternative currency?

- Merchants issued tokens in Britain and elsewhere to address the 'big problem of small change'
- Long lived and widely used in 17<sup>th</sup> - 19<sup>th</sup> centuries
- Survived legal bans but not the advent of low-cost minting and 'standard formula'



Lyceum Theatre Coin  
Half-penny, metal alloy  
18<sup>th</sup> century London














+



The image features a stack of US dollar bills on the left side, partially obscured by a large, intense fire that consumes a portion of the bills on the right. The fire is bright orange and yellow, with black smoke rising from it. The background is dark, making the fire and the details of the currency stand out. The text 'THE CURSE OF CASH' is overlaid on the left side of the image in a white, bold, sans-serif font.

THE  
CURSE  
OF  
CASH

KENNETH S.  
ROGOFF



# Major bitcoin price crashes (Sept. 2010 – present)

Correction Period	# Days	Bitcoin High	Bitcoin Low	% Decline	% Return to New High	New High Date	# Days to New High
12/17/2017 to 2/6/2018	51	\$ 19,783	\$ 5,922	-70%	?	?	?
11/8/2017 to 11/12/2017	4	\$ 7,879	\$ 5,507	-30%	43%	11/16/2017	8
9/2/2017 to 9/15/2017	13	\$ 5,014	\$ 2,951	-41%	70%	12/10/2017	40
6/11/2017 to 7/16/2017	35	\$ 3,025	\$ 1,837	-39%	65%	5/8/2017	55
3/10/2017 to 3/24/2017	14	\$ 1,326	\$ 892	-33%	49%	4/27/2017	48
11/30/2013 to 1/14/2015	410	\$ 1,166	\$ 170	-85%	585%	2/23/2017	1181
4/10/2013 to 7/7/2013	88	\$ 266	\$ 63	-76%	323%	7/11/2013	211
6/8/2011 to 11/17/2011	162	\$ 32	\$ 1.99	-94%	1504%	2/28/2013	631
5/13/2011 to 5/21/2011	8	\$ 8.45	\$ 5.58	-34%	51%	5/25/2011	12
2/10/2011 to 4/4/2011	53	\$ 1.10	\$ 0.56	-49%	96%	4/17/2011	66
11/6/2010 to 11/10/2010	4	\$ 0.50	\$ 0.14	-72%	257%	1/31/2011	86
9/14/2010 to 10/8/2010	24	\$ 0.17	\$ 0.01	-94%	1600%	10/24/2010	40
<b>Average - Top 5 declines</b>	<b>138</b>						<b>430</b>
<b>Median - Top 5 declines</b>	<b>88</b>						<b>211</b>

Bitcoin will almost certainly remain significantly more volatile than central bank managed currencies

*“The main volatility in bitcoin comes from variability in speculation, which in turn is due to the genuine uncertainty about its future.*

*More efficient liquidity mechanisms don't help reduce genuine uncertainty.”*



**Nick Szabo**  
Cryptocurrency pioneer

# Stablecoins



iea

F. A. Hayek

# Denationalisation of Money

The Argument Refined



*"A private currency would prevail if it is essentially stable in value and prevent both excessive stimulation of investment and the consequent periods of contraction."*

# The blockchain ecosystem needs a stable cryptocurrency

- **Bitcoin's volatility has been a feature, not a bug:** volatility has accelerated adoption and raised awareness for cryptocurrencies....
- ....but bitcoin is ineffective for pricing day-to-day transactions (unit of measure) or holding stable funds (store of value)
- A stable cryptocurrency key for facilitating a multitude of initiatives:
  - Retailing and pricing
  - Savings and loans
  - Funds transfer
  - Insurance
  - Performance monitoring

# Stabelcoins + smart contract-based insurance

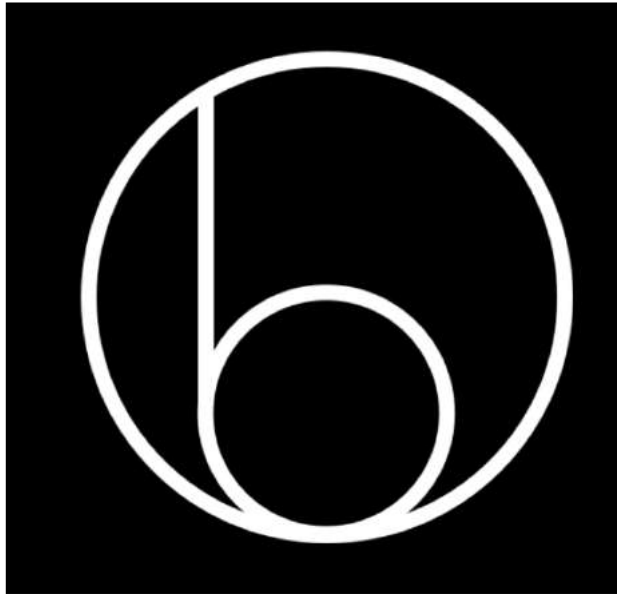


- A delayed flight is a public record, can be used in a smart flight cancellation insurance contract
- If event occurs smart contract is triggered and payout automatically made
- Approximately 600k annual passengers do not file eligible insurance claims for delayed/cancelled UK flights

The number of stablecoin projects has increased dramatically in the past several months



tether



AAA

# Overview of different stablecoins

	Tether	Dai	Basecoin	AAA
Type	Asset-backed	Asset-backed	Fiat	Asset-backed
Collateral	USD	Unknown	n/a	Multi-currency; fixed-income
Stability Benchmark / Reference Peg	USD	SDR	USD (CPI in long run?)	Real-terms: G10 inflation
Regulatory Status	Money Service Business with the Financial Crimes Enforcement Network of the US Dept. of Treasury	TBD	TBD	TBD
Legal Jurisdiction	British Virgin Islands	n/a - DAO	TBD	Jersey (Bailiwick of Jersey)
Functional Transparency	Low (eg is there a \$1 for every Tether?)	High	High	Medium-to-High
Ownership	iFinex (Bitfinex parent)	Token holders?	A16Z, Pantera, etc. (Intangible Labs)	n/a
Legal Entity	Hong Kong-based Ltd company (Tether Limited)	Unknown	TBD	Non-For-Profit SPV (AAA Fiduciary Ltd)
Platform	Omni Protocol	Ethereum	TBD	Ethereum
Decentralization	Low-Medium	Medium-High	TBD	Medium
Automation	Medium	Medium-Full	Full	Low-Medium
Complexity	Low/High (opaque, security issues)	High	High	Medium
Launch Date	Live	Q4 2017	TBD	Q4 2017
Website	<a href="https://tether.to/">https://tether.to/</a>	<a href="https://makerdao.com">https://makerdao.com</a>	<a href="http://www.getbasecoin.com">www.getbasecoin.com</a>	<a href="http://www.AAAcy.org">www.AAAcy.org</a>





# Thank You

Website

**GarrickHileman.com**

Email

**gh434@cam.ac.uk**



# Appendix



# **AAA Reserve Currency (Ticker: AAA)**

**THE DIGITAL STABLECOIN**

# Introduction

# AAA is an asset-backed stable cryptocurrency

Asset-backed: cash and fixed income investments are held in a ring-fenced SPV (AAA Fiduciary Ltd)

- Supports value of AAA Coin
- Provides liquidity for fiat currency redemptions

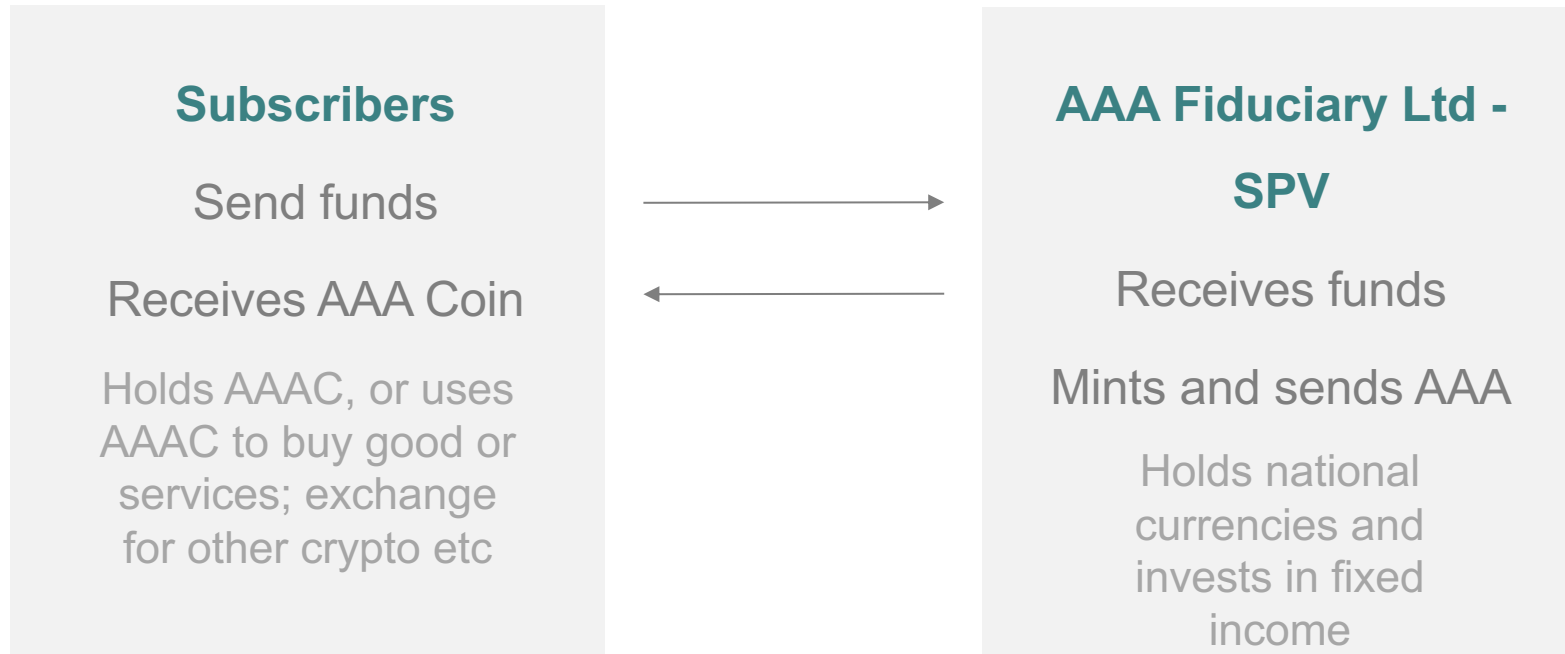
Stable: similar volatility to USD; tracks G10 inflation

- Exchange rate controls to manage pricing
- Store-of-value: lower volatility; effective for savings, loans and investments
- Unit of measure: effective for retailing

AAA has been signed-off by the Jersey regulator as a debt security. AAA is one of the first 'security tokens' - a new breed of asset-backed and regulated cryptocurrencies.

**How it works**

# Proceeds from the new issuance of AAA Coins are placed into a ring-fenced SPV (AAA Fiduciary Ltd)



AAA coin holders can sell AAA coins back to AAA Fiduciary Ltd in exchange for national currencies and cryptocurrencies.

# **Assets of SPV are allocated across (i) multiple currencies and (ii) cash and fixed income**

## Multi-currency

- Basket of currencies are less volatile than a single currency
- Top 6 trade-weighted currencies as reported by Bank of International Settlements (e.g. USD, EUR, GBP...)

## Cash and fixed income

- Cash: bank deposits
  - liquidity
- Fixed income: loans, gilts, bonds etc.
  - to target return to track inflation across G10 countries
  - to be paid for credit risk (vis a vis holding significant deposits of cash in a bank account)

## **Exchange rate controls provide price stability: 3 scenarios keep the price per AAA Coin and NAV closely aligned**

Scenario 1: Price = NAV (Net Asset Value per Coin)

- If the price always equals NAV, then nothing needs to be done.

Scenario 2: Price more than NAV

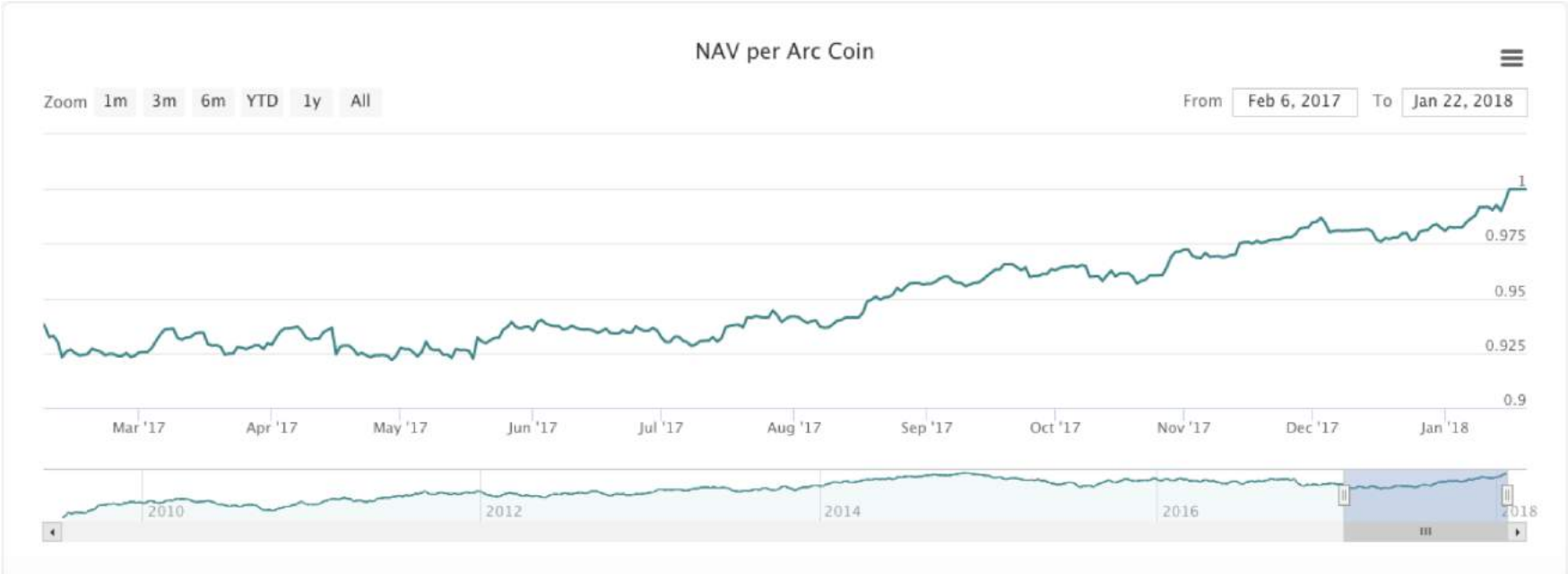
- If the price increases above NAV on an exchange, then, at any time, people can buy newly issued coin at a price equal to NAV from AAA Fiduciary Ltd, and then sell it on the exchange at a profit. This rewards the community for keeping the price of AAA down.

Scenario 3: Price less than NAV

- AAA Fiduciary Ltd keeps an amount of its holdings in cash deposits and is willing to buy back AAA (price based on a formula—see [Technical Whitepaper](#)). If the price on an exchange falls, then anyone can buy AAA from the exchange, sell it at a higher price to AAA Fiduciary Ltd, and make a profit. This rewards the community for keeping the price up. AAA Fiduciary then burns the repurchased AAA.



# AAA has been back-tested using historical data



# Use cases

# Enabling savers in developing countries

Approximately 2 billion people live in countries with high inflation or significant political and financial instability.

- Without a reliable currency and somewhere safe to store their savings it is very difficult to save and plan for their futures.

The AAA Reserve Currency can enable people to save and plan for their future globally - beating inflation and out of reach of untrusted counterparties.

- This is why [we are passionate about a stable cryptocurrency.](#)

# Cryptocurrency on-ramp and off-ramp

It can be difficult, costly and time consuming to transact between national currencies and cryptocurrencies.

- Holding funds in most cryptocurrencies will expose you to significant volatility in the value of your holdings.

AAA Reserve Currency is an efficient and effective way a trusted method for moving back and forth between national currencies and cryptocurrency.

- You can also hold your cryptocurrency balances with lower volatility.

# Crypto retailing

Many retailers want to accept cryptocurrencies but the transaction costs of using BTC and the high volatility of other cryptocurrencies makes it difficult for retailers to accept crypto.

AAA Reserve Currency is well suited to retailers, enabling customers and sellers alike to benefit from better price certainty in their day-to-day transactions.

# AAA has been created in collaboration between financial investment experts, economists and developers

## CO-FOUNDERS



### Stephen Findlay

Co-founder and CEO of BondMason, a fintech platform that enables fixed income investment.

15+ years financial services and investment management experience with Fidelity, Deloitte and Andersen.

Qualified chartered accountant (FCA – ICAEW) and approved person of the UK's Financial Conduct Authority.



### Dr. Garrick Hileman

Economic Historian at the University of Cambridge and LSE.

15+ years experience in private sector with Bank of America, IDG and Allianz.

He has served on the boards of publicly traded and private companies and is known for his research on cryptocurrency and DLT.

The co-founders have been supported by a broad team of financial and technology experts, including people with experience at: Goldman Sachs, Blackstone, a specialist forex hedge fund; as well leading cryptocurrency experts.

**Get in touch**  
**hello@arccy.org**

# **FAQs and Technical details**



# How can I buy AAA Coins?

1. Create an account on [www.arccy.org](http://www.arccy.org)
2. Complete AML/KYC
3. Wire funds
  - Minimum subscription of USD 25,000 (or equivalent)
  - You will need an ERC20 compliant wallet to receive your AAA Coins

# How can we trust that AAA Fiduciary Ltd holds the cash and investments?

(Answer: audited Proof of Reserves and governance)

## Publication

- the value of the reserves is displayed on the website, with a breakdown at all times. See <https://www.arccy.org/arc-nav>

## Audit

- these balances are audited annually by Grant Thornton

## The ERC20 code

- for any new coin to be minted (at any time) they need to pass a 'Proof-of-Reserves' check, this verifies the collateral, and value of it, before any coins can be minted.

## Regulation

- The AAA Reserve Currency has been signed off by the Jersey regulator, and the operations of AAA Fiduciary Ltd, with an independent trust company acting as a local director.
- AAA may be regulated in other jurisdictions.

## Legal

- The Information Memorandum forms a legal contract between AAA Fiduciary Ltd and the purchasers of AAA Coins. If AAA Fiduciary Ltd fails act in accordance with this contract (e.g. by not reporting reserves correctly) this would represent a breach of contract.

## What if there's a 'run' on AAA ?

(Answer: natural buoyancy supports the price of AAA Coin)

AAA Fiduciary Ltd (AFL) holds a certain proportion in cash

- The Target Cash Amount, initially 25% of holdings; but flexed based on liquidity of other investment holdings, and average day traded volumes.

AAA Fiduciary will maintain a buy (any holder can sell AAA Coins back to [www.arccy.org](http://www.arccy.org) ) at a price below NAV

- A small discount based on typical market spreads, so that this repurchase activity doesn't impact normal exchange trading.

If Actual cash is less than 50% of Target cash (cash starting to run out), then the buy price offered by AAA Fiduciary Ltd begins to fall (this is the 'bank run' scenario)

However, each trade becomes increasingly profitable (e.g. NAV = 100; but coin is repurchased at 96)

- AAA Coins are burnt as soon as repurchased by AFL – so a bank run is the only scenario where the NAV per AAA coin starts to increase faster than usual.

If this continues then each repurchase by AFL trades become more and more profitable; so this creates a 'natural buoyancy' for the price of AAA, for the benefit of all holders, and negates the bank run.

- Once the dust has settled, all of the sellers during the bank run have funded the profits for the AAA Coin holders.

## **How does the ER20 contract issue AAA Coins?**

(Answer: AAA Coins are issued when 3 tests are met)

1. The purchaser of AAA coins sends sufficient funds.
2. The purchaser passes regulatory tests, such as KYC and AML.
3. The purchaser pays the correct price per coin. This is the net asset value per coin (NAV), which is the value of all the assets held by AAA Fiduciary Ltd divided by the total number of coins in issue.

New issuances are unlimited, instantaneous, and non-dilutive for existing coin holders. This is a critical feature of AAA, and vital for any stablecoin.