# Cryptoasset Economics

## Blockchain & Economic Models

# Michael Hiles

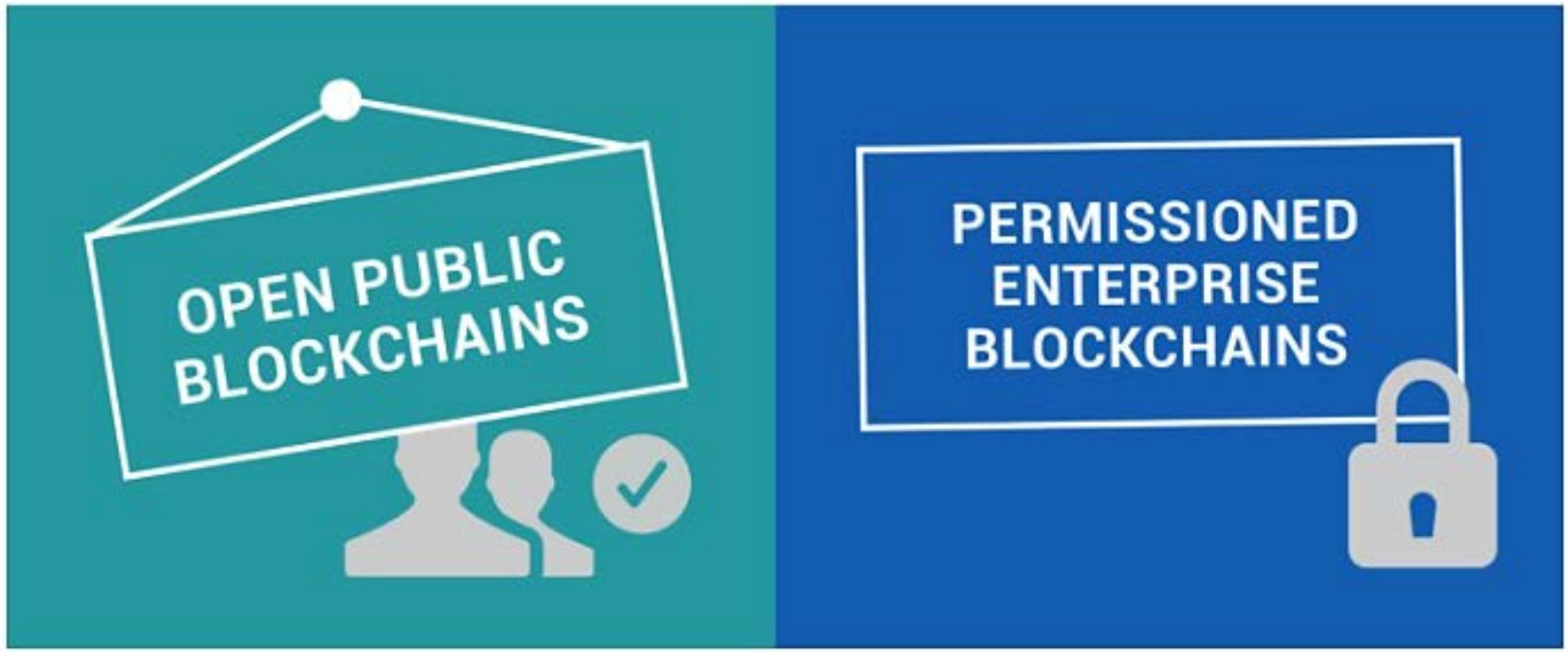
## CEO, 10XTS

FOUNDER INSTITUTE
GLOBALIZING SILICON VALLEY

10XTS

cincinnati crypto fund

# TYPES OF BLOCKCHAINS



# Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

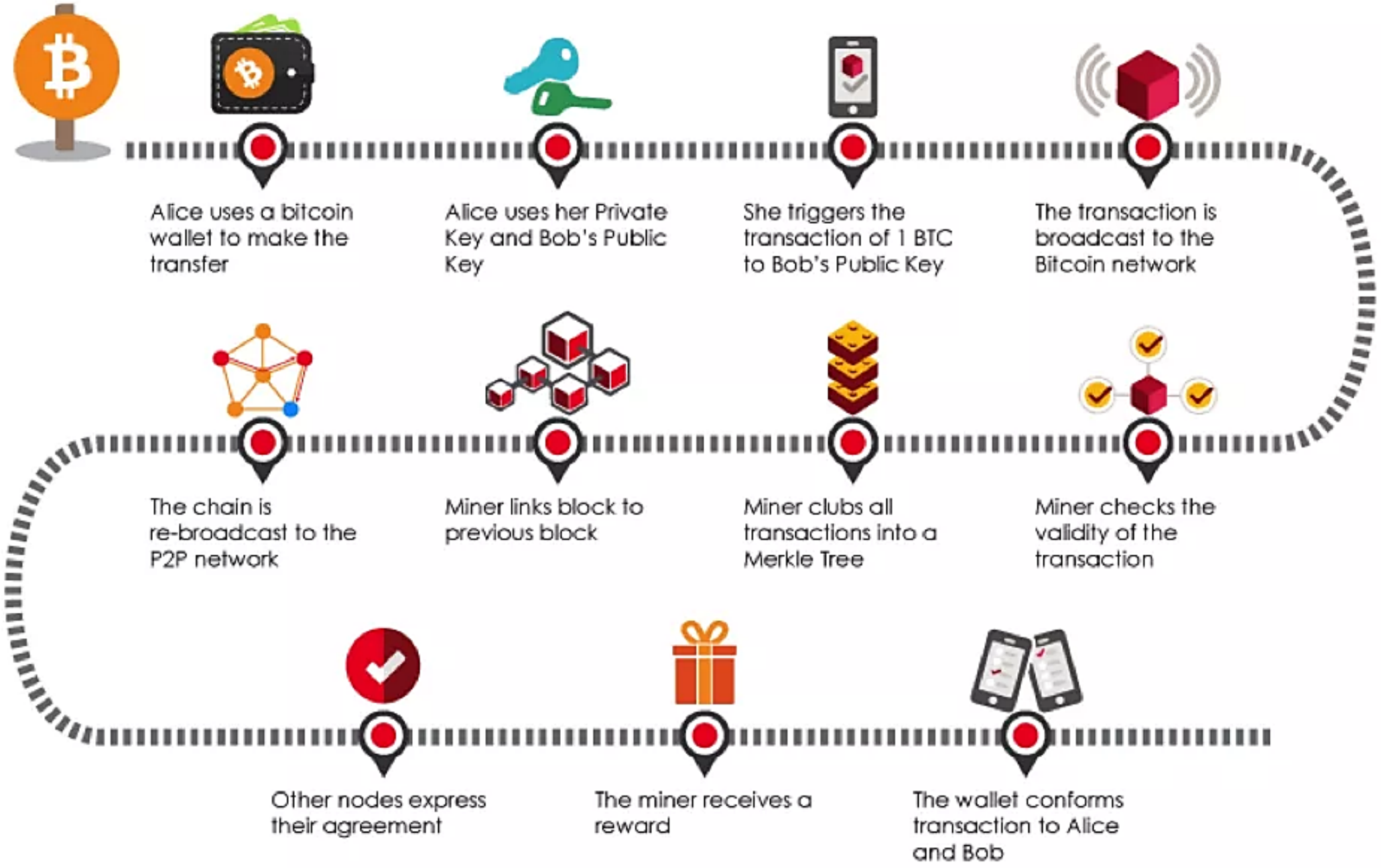
**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

## 1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

# Whitepaper released in 2008, network launched in 2009


Alice uses a bitcoin wallet to make the transfer
Alice uses her Private Key and Bob's Public Key
She triggers the transaction of 1 BTC to Bob's Public Key
The transaction is broadcast to the Bitcoin network
The chain is re-broadcast to the P2P network
Miner links block to previous block
Miner clubs all transactions into a Merkle Tree
Miner checks the validity of the transaction
Other nodes express their agreement
The miner receives a reward
The wallet conforms transaction to Alice and Bob

LEGO

# Blockchain

Ages/âge/edades

**9-99**

**18323**

**The Bitcoin Blockchain**

**285,800 pcs/pzs**

Building Toy
Jouet de Construction
Juguete para Construir

*Includes Winklevii & Bitcoin Miner mini-figurines*

Expert

## GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Tue Nov 21 2017 15:33:48 GMT-0800 (PST).

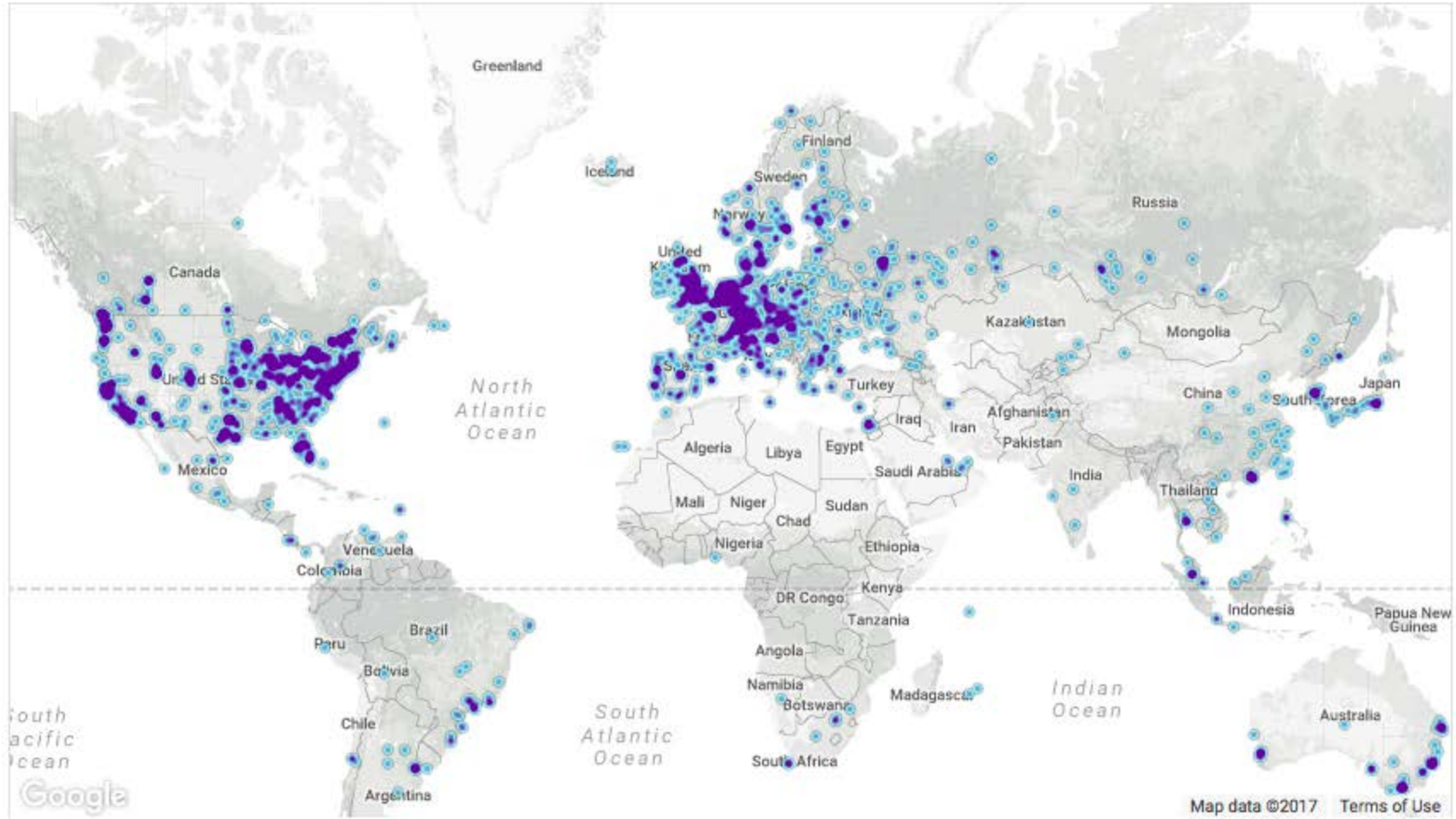
# 11008 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

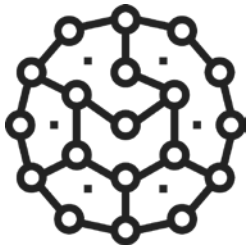
| RANK | COUNTRY | NODES |
|---|---|---|
| 1 | United States | 3120 (28.34%) |
| 2 | Germany | 1831 (16.63%) |
| 3 | France | 747 (6.79%) |
| 4 | China | 716 (6.50%) |
| 5 | Netherlands | 521 (4.73%) |
| 6 | Canada | 458 (4.16%) |
| 7 | United Kingdom | 437 (3.97%) |
| 8 | n/a | 366 (3.32%) |
| 9 | Russian Federation | 334 (3.03%) |
| 10 | Singapore | 232 (2.11%) |

More (97) »



# The Five Key Components of a Blockchain

Cryptography



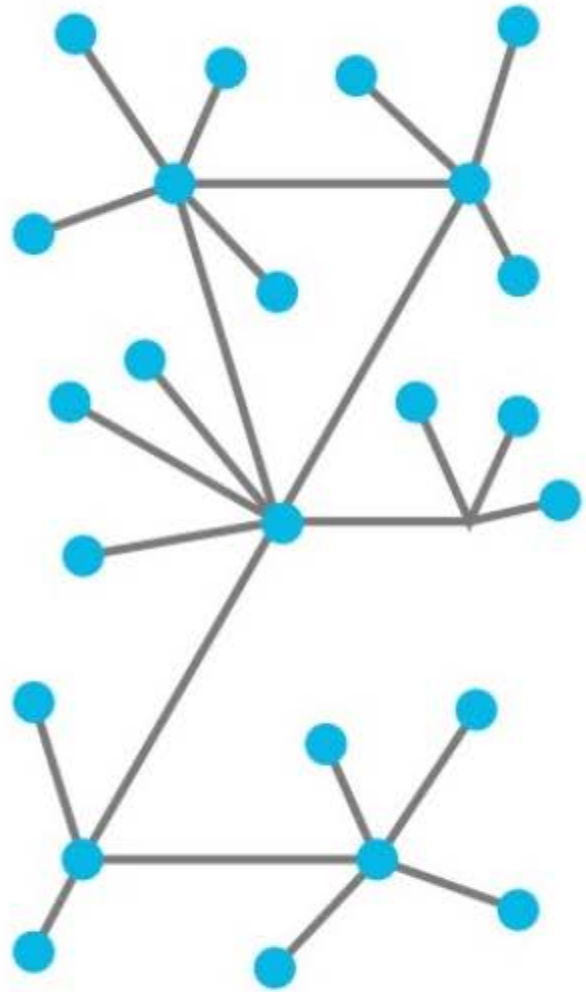
P2P Network

Consensus Mechanism

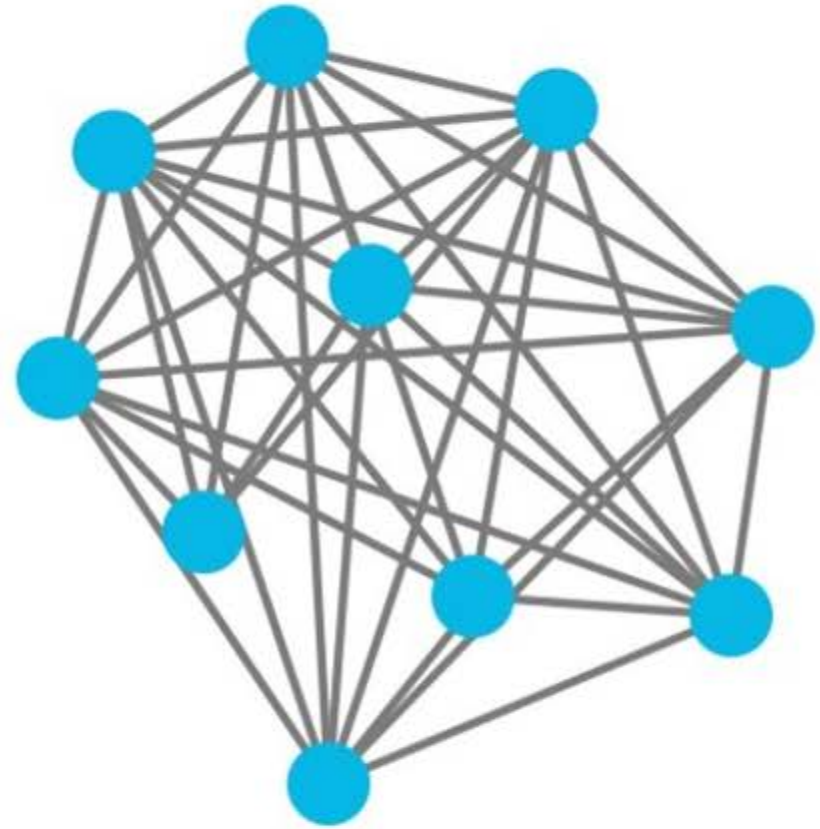
Ledger

Validity Rules

Centralized

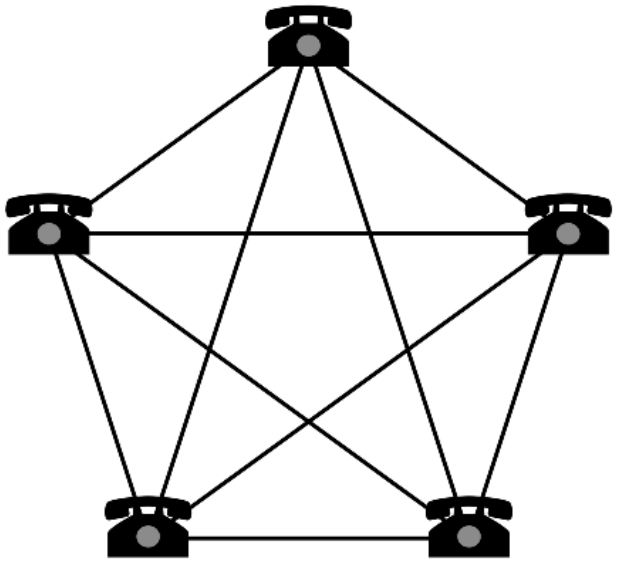


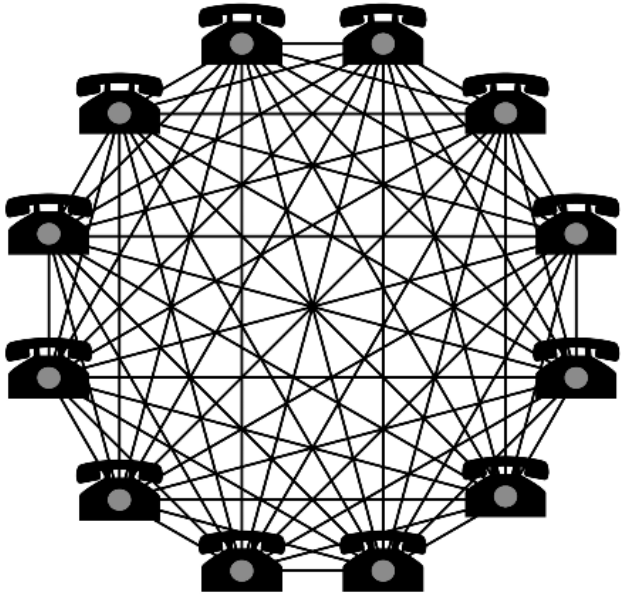
Decentralized



Distributed

# The Network Effect



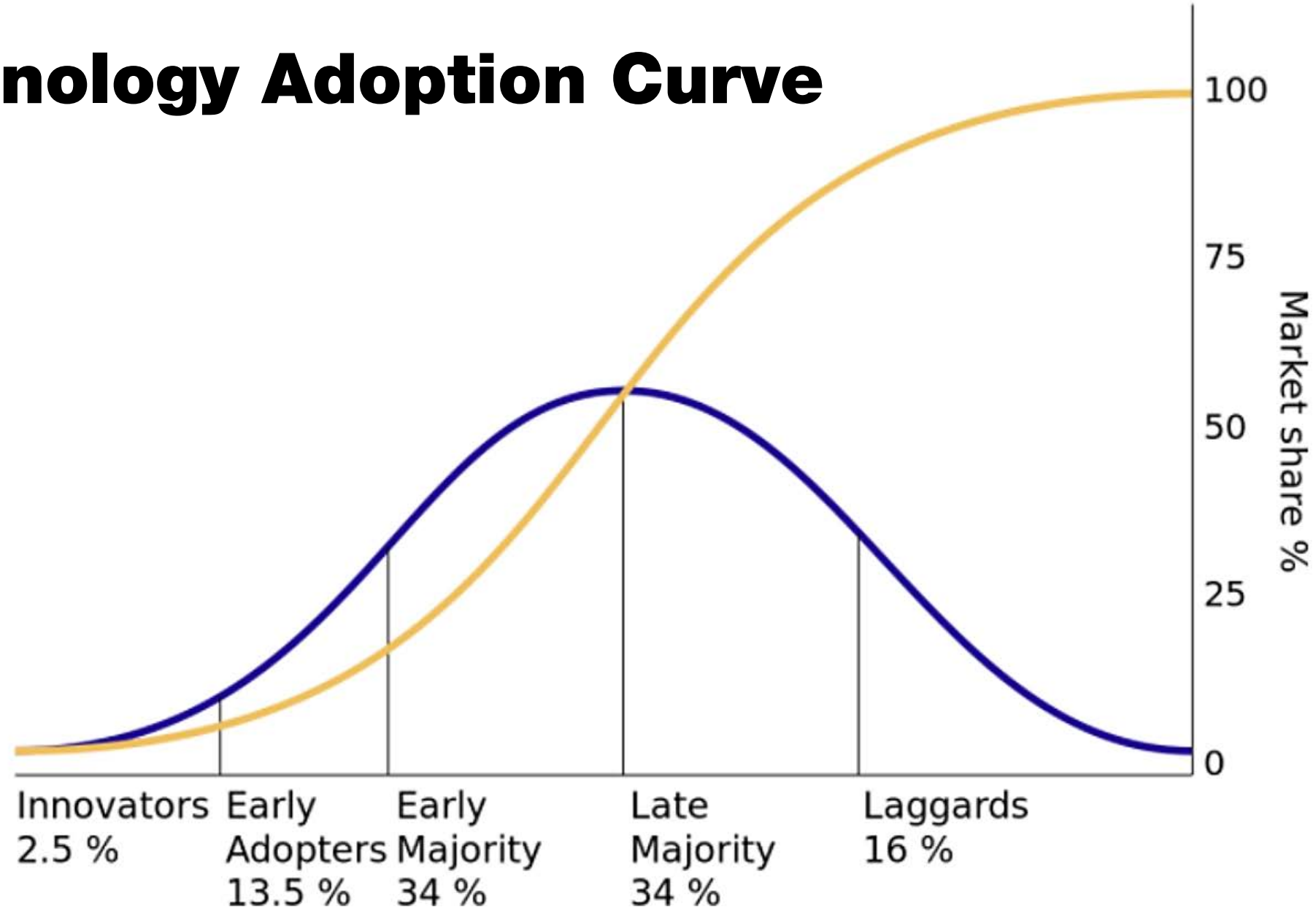


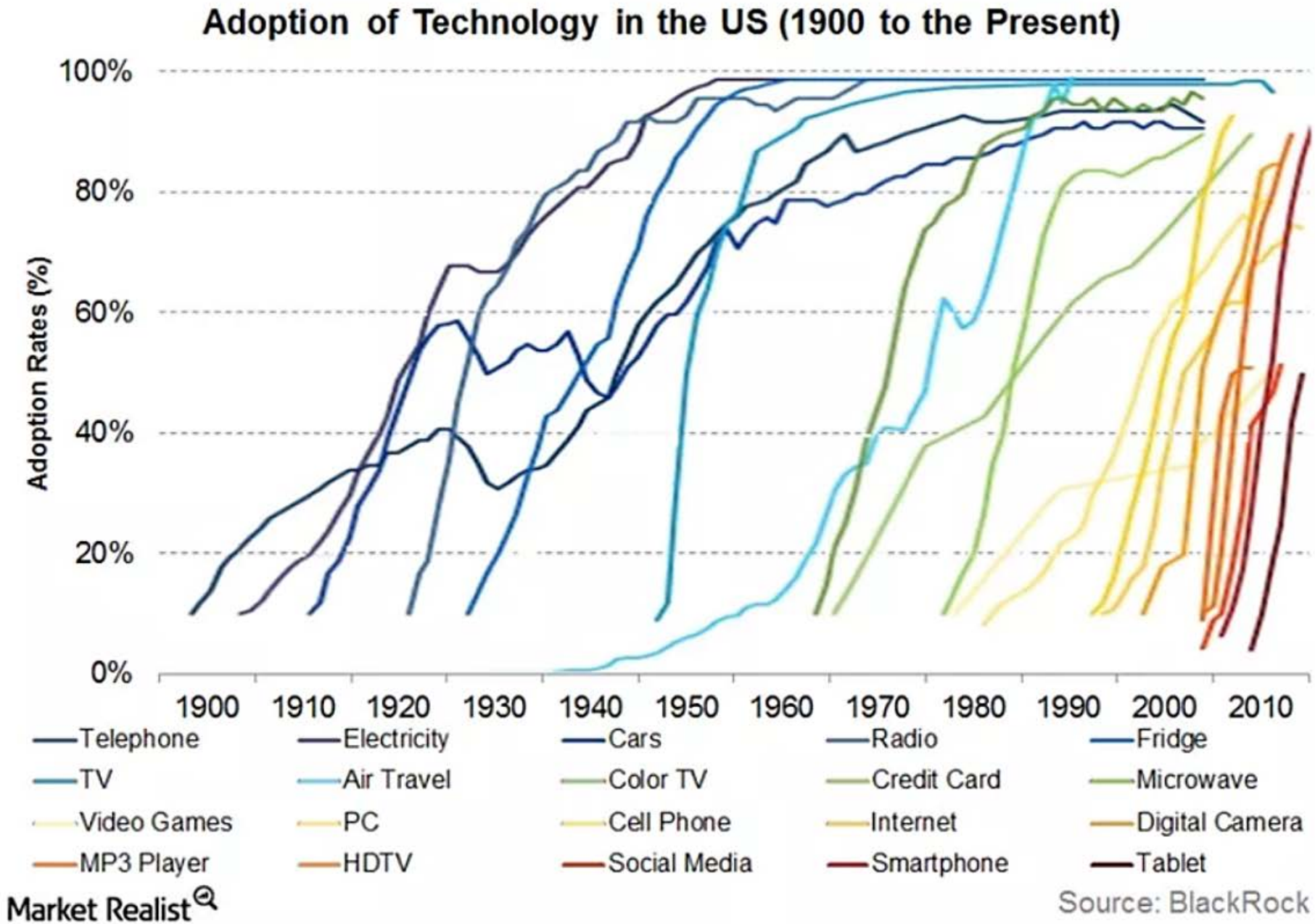
$$\sum_{i=1}^{n+1} V_{i,j} > \sum_{i=1}^{n} V_{i,j}$$

**WARNING!**

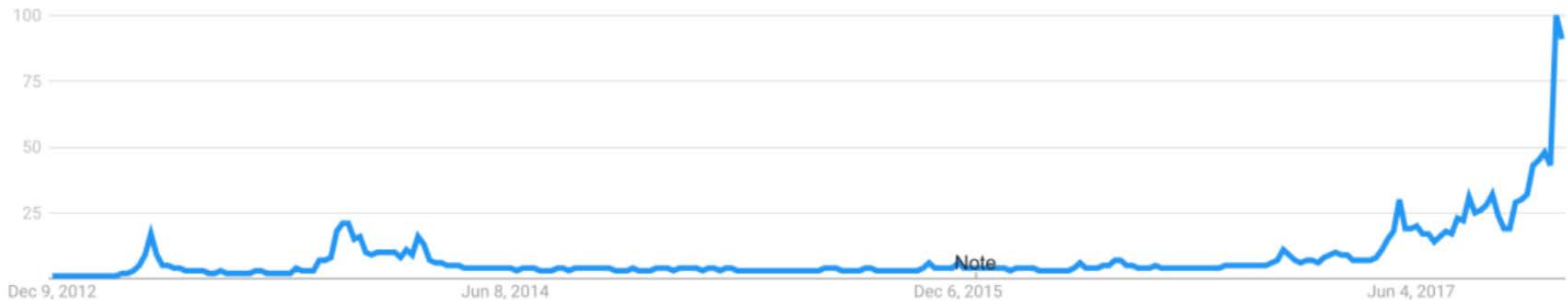
**complicated maths**

# Technology Adoption Curve




Adoption of Technology in the US (1900 to the Present)
100%
80%
60%
40%
20%
0%
Adoption Rates (%)
1900
1910
1920
1930
1940
1950
1960
1970
1980
1990
2000
2010
Telephone
Electricity
Cars
Radio
Fridge
TV
Air Travel
Color TV
Credit Card
Microwave
Video Games
PC
Cell Phone
Internet
Digital Camera
MP3 Player
HDTV
Social Media
Smartphone
Tablet
Market Realist
Source: BlackRock

Google searches for bitcoin



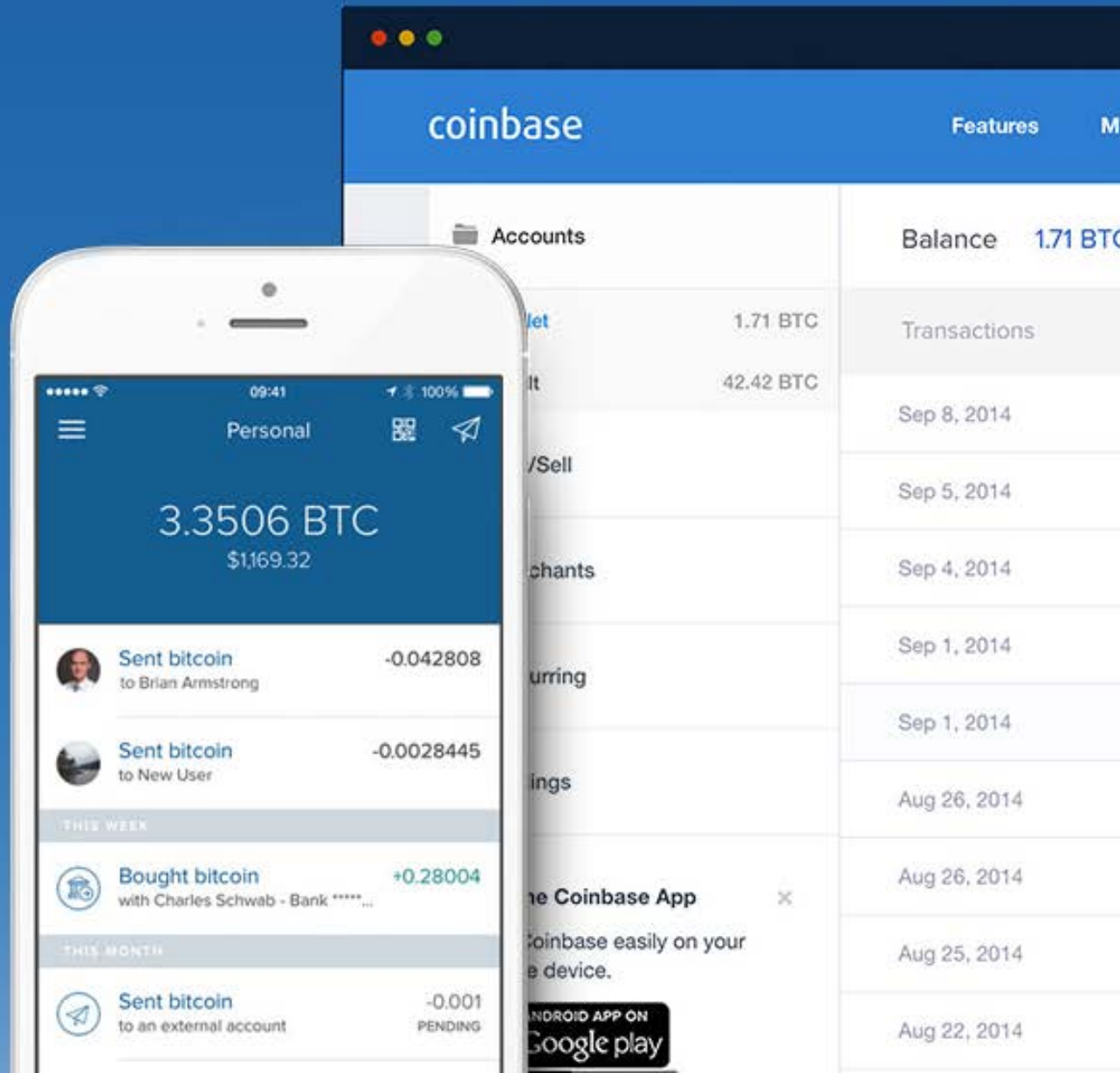

Coinbase users over time
12,500,000
10,000,000
7,500,000
5,000,000
2,500,000
0
Users
1-Jan-14
1-Jan-15
1-Jan-16
1-Jan-17


BITCOIN PRICES
$141.00
$140
$120
$100
$80
$60
$40
$20
$0
2011
2012
2013
Why yes, that was a bubble!


Fred Ehrsam
Brian Armstrong

# coinbase

Coinbase is the world's most popular place to buy and sell bitcoin.




Marc Andreesen – he invented Netscape

coinbase
Bitcoin
Enterprise

Popular Posts

Download the new, completely redesigned TechCrunch mobile app

Tesla made only 260 Model 3 cars in Q3, but is 'confident' it can fix bottleneck

Papyrus creator speaks out after Ryan Gosling roasts the font on SNL

Airbus on track

# Coinbase Raises $25M Led By Andreessen Horowitz To Build Its Bitcoin Wallet And Merchant Services

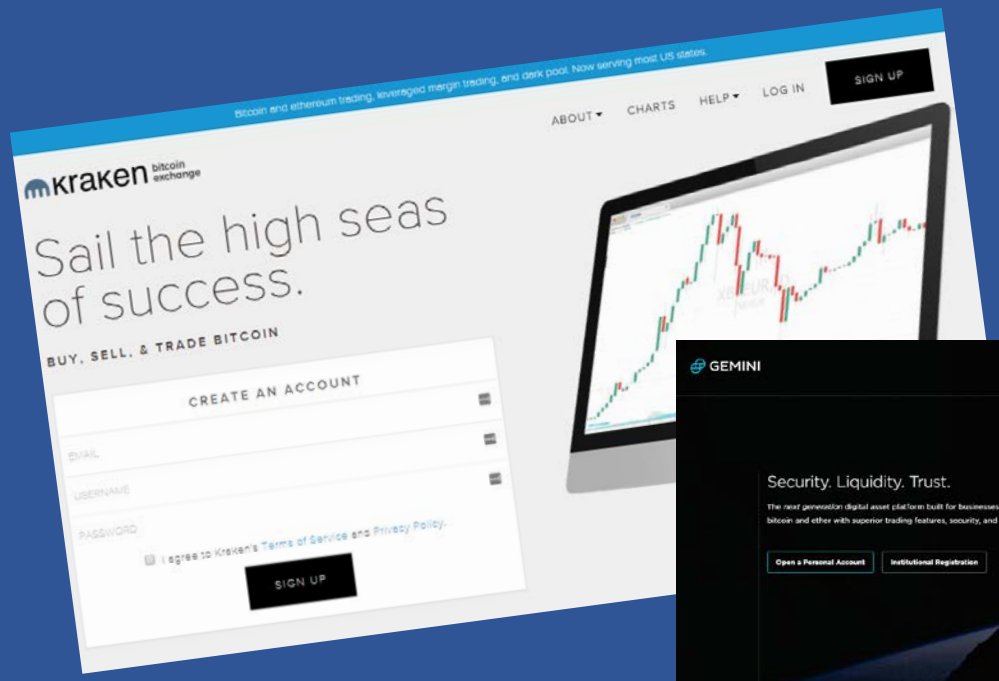
*Posted Dec 12, 2013 by* ***Alex Williams*** *(@alexwilliams)*

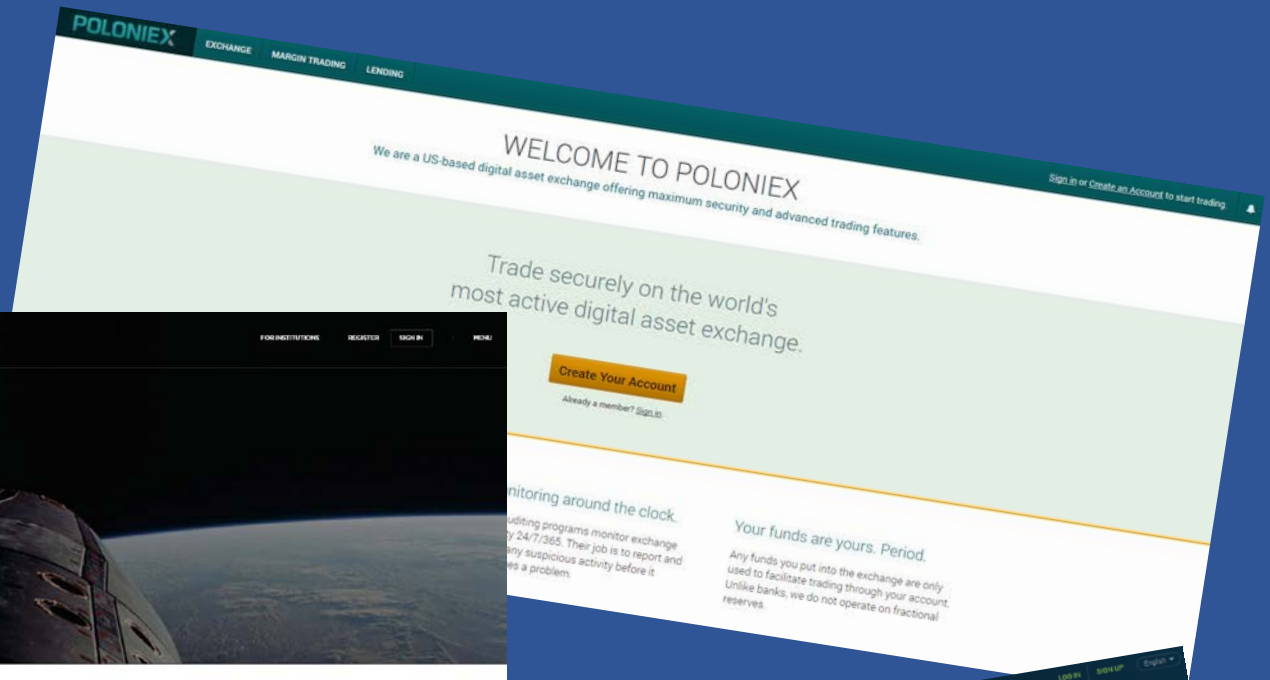


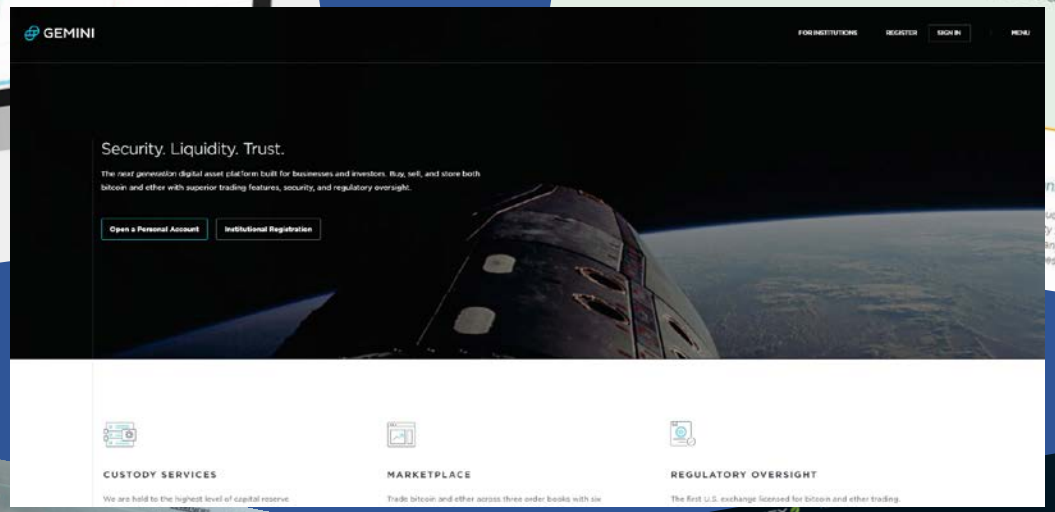
## Crunchbase

**Coinbase** –

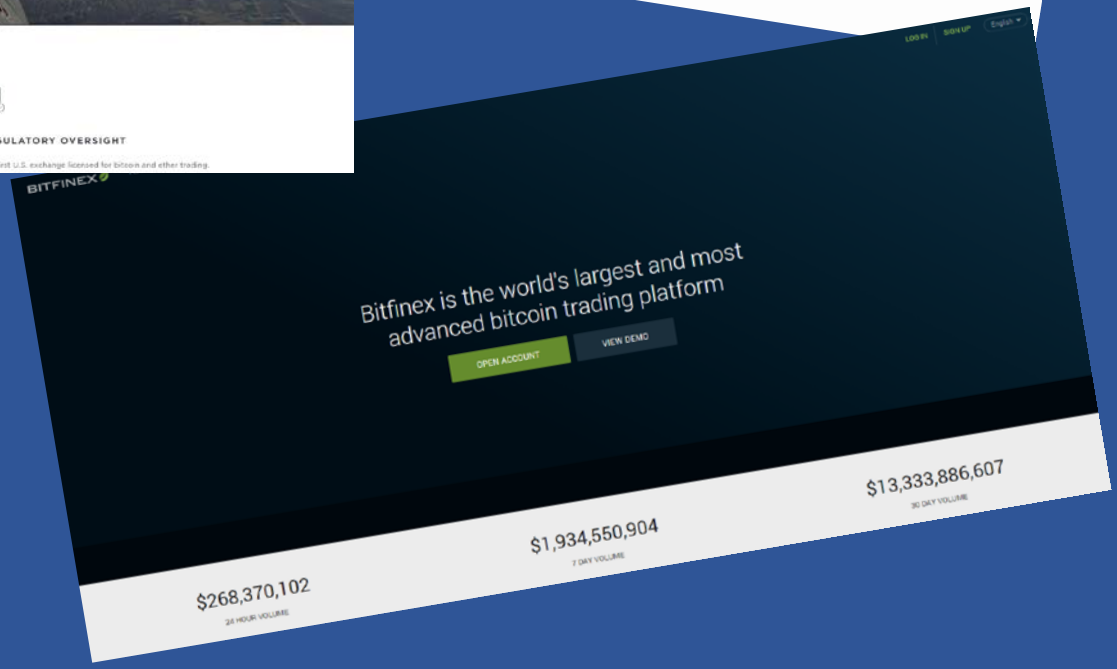
FOUNDED


Bitcoin and ethereum trading, leveraged margin trading, and dark pool. Now serving most US states.
ABOUT
CHARTS
HELP
LOG IN
SIGN UP
kraken bitcoin exchange
Sail the high seas of success.
BUY, SELL, & TRADE BITCOIN
CREATE AN ACCOUNT
EMAIL
USERNAME
PASSWORD
I agree to Kraken's Terms of Service and Privacy Policy.
SIGN UP


POLONIEX
EXCHANGE
MARGIN TRADING
LENDING
WELCOME TO POLONIEX
We are a US-based digital asset exchange offering maximum security and advanced trading features.
Sign in or Create an Account to start trading.
Trade securely on the world's most active digital asset exchange.
Create Your Account
Already a member? Sign in.
Your funds are yours. Period.
Any funds you put into the exchange are only used to facilitate trading through your account. Unlike banks, we do not operate on fractional reserves.

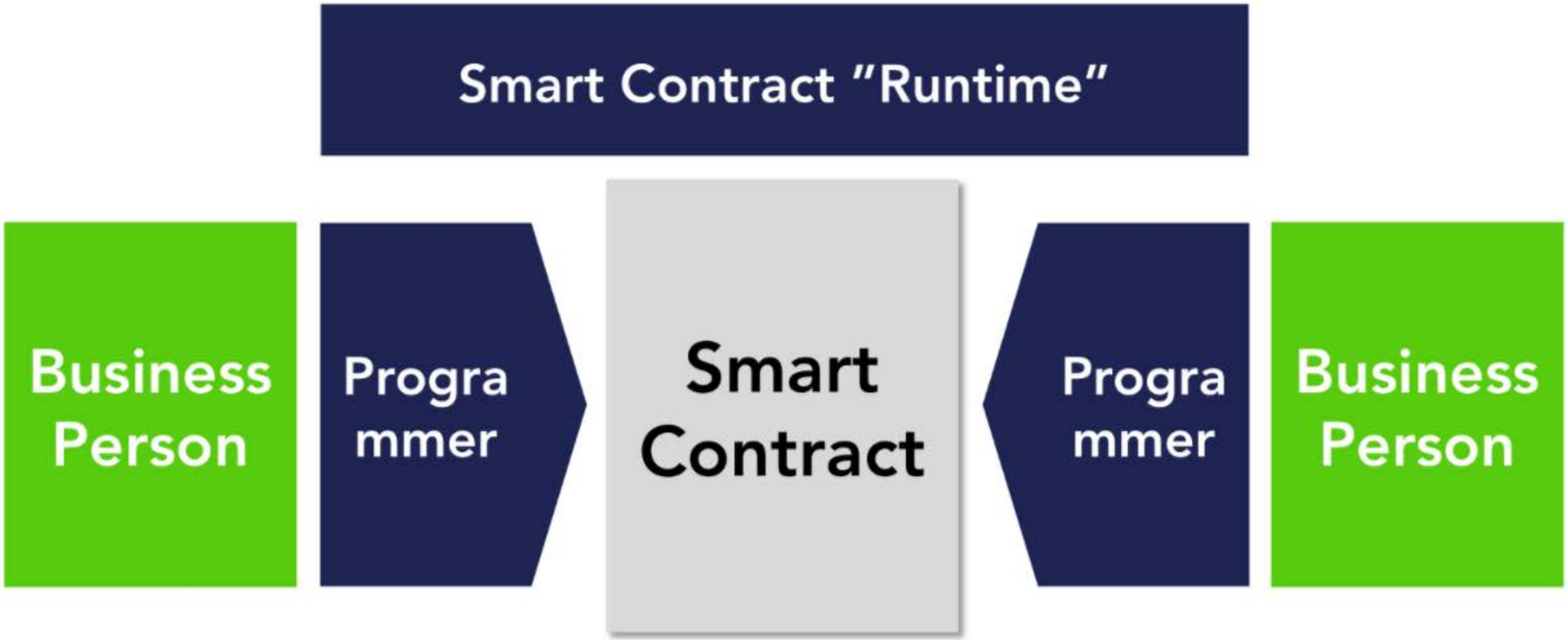

GEMINI
FOR INSTITUTIONS
REGISTER
SIGN IN
MENU
Security. Liquidity. Trust.
The next generation digital asset platform built for businesses and investors. Buy, sell, and store both bitcoin and ether with superior trading features, security, and regulatory oversight.
Open a Personal Account
Institutional Registration
CUSTODY SERVICES
MARKETPLACE
REGULATORY OVERSIGHT


BITTREX
BITTREX
THE NEXT-GENERATION DIGITAL CURRENCY EXCHANGE


BITFINEX
LOG IN
SIGN UP
Bitfinex is the world's largest and most advanced bitcoin trading platform
OPEN ACCOUNT
VIEW DEMO
$268,370,102
24 HOUR VOLUME
$1,934,550,904
7 DAY VOLUME
$13,333,886,607
30 DAY VOLUME


ethereum

# Replace “attorney” with “programmer” and “legal system” with “runtime code” and we have smart contracts



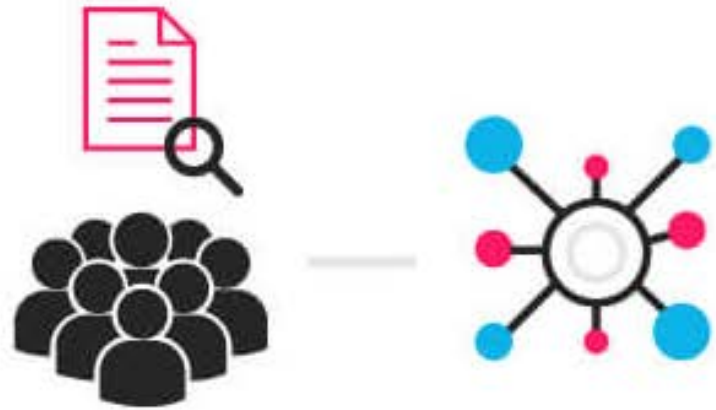
1

An option contact between parties is written as code into the blockchain. The individuals involved are anonymous, but the contact is the public ledger.

2

A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

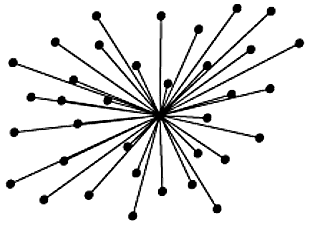
3



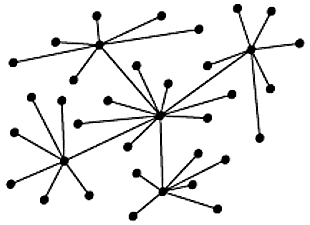
Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions

# Blockchain Startups

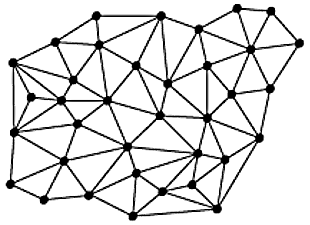
## Top Blockchain startups



**PAST**



**PRESENT**



**FUTURE**

THE WALL STREET JOURNAL.

THE TIMES

HM Government

Hilton

facebook

twitter

Dropbox

UBER

airbnb

Cloud storage

Filecoin

TIERION

STORJ.IO

Smart Contracts

TRUST

ETHERPARTY

appliedblockchain

Social Networking

synereo

GEMS

Anti-Counterfeiting

everledger

BLOCKVERIFY

Governance

AUTONOMOS

Swarm

followmyvote

BITNATION

GOVERNANCE 2.0

Digital Identity

ONENAME

ShoCard

Supply Chain

Tradle

thingchain

Art & Ownership

VERISART

Bitproof.io

MONEGRAPH

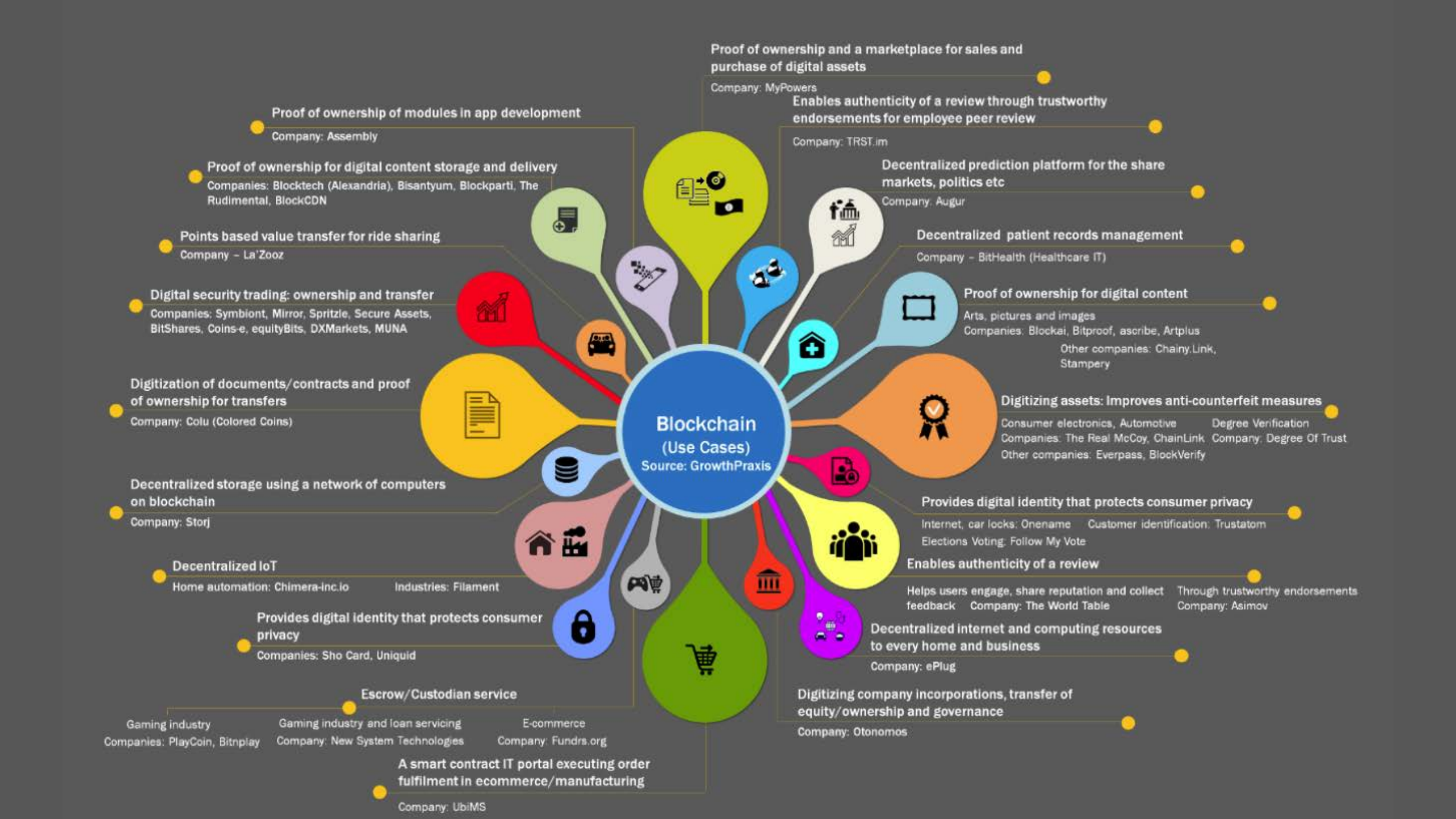
colu.

Prediction Markets

augur

Internet of Things

FILAMENT


Blockchain
(Use Cases)
Source: GrowthPraxis
Proof of ownership and a marketplace for sales and purchase of digital assets
Company: MyPowers
Enables authenticity of a review through trustworthy endorsements for employee peer review
Company: TRST.im
Decentralized prediction platform for the share markets, politics etc
Company: Augur
Decentralized patient records management
Company – BitHealth (Healthcare IT)
Proof of ownership for digital content
Arts, pictures and images
Companies: Blockai, Bitproof, ascribe, Artplus
Other companies: Chainy.Link, Stampery
Digitizing assets: Improves anti-counterfeit measures
Consumer electronics, Automotive
Companies: The Real McCoy, ChainLink
Other companies: Everpass, BlockVerify
Degree Verification
Company: Degree Of Trust
Provides digital identity that protects consumer privacy
Internet, car locks: Onename
Customer identification: Trustatom
Elections Voting: Follow My Vote
Enables authenticity of a review
Helps users engage, share reputation and collect feedback
Company: The World Table
Through trustworthy endorsements
Company: Asimov
Decentralized internet and computing resources to every home and business
Company: ePlug
Digitizing company incorporations, transfer of equity/ownership and governance
Company: Otonomos
Proof of ownership of modules in app development
Company: Assembly
Proof of ownership for digital content storage and delivery
Companies: Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN
Points based value transfer for ride sharing
Company – La'Zooz
Digital security trading: ownership and transfer
Companies: Symbiont, Mirror, Spritzle, Secure Assets, BitShares, Coins-e, equityBits, DXMarkets, MUNA
Digitization of documents/contracts and proof of ownership for transfers
Company: Colu (Colored Coins)
Decentralized storage using a network of computers on blockchain
Company: Storj
Decentralized IoT
Home automation: Chimera-inc.io
Industries: Filament
Provides digital identity that protects consumer privacy
Companies: Sho Card, Uniquid
Escrow/Custodian service
Gaming industry
Companies: PlayCoin, Bitnplay
Gaming industry and loan servicing
Company: New System Technologies
E-commerce
Company: Fundrs.org
A smart contract IT portal executing order fulfilment in ecommerce/manufacturing
Company: UbiMS


What is an ICO / ITO / TGE?

STARTUP NEWS & ANALYSIS

# The new crowdfunding? Ethereum ICOs raise close to $1 billion in June alone

ANGELA CASTLES / Tuesday, July 4, 2017

In just 19 days, Ethereum initial coin offerings have raised close to $1 billion dollars, according to estimates, with speculations this could be the biggest decentralised venture funding event in history.

Tech news site *Trust Nodes* has crunched the numbers and estimates $US642 million has been raised by prominent initial coin offerings (ICOs) in the first three weeks of June, with another estimated $US60 million raised from smaller events.



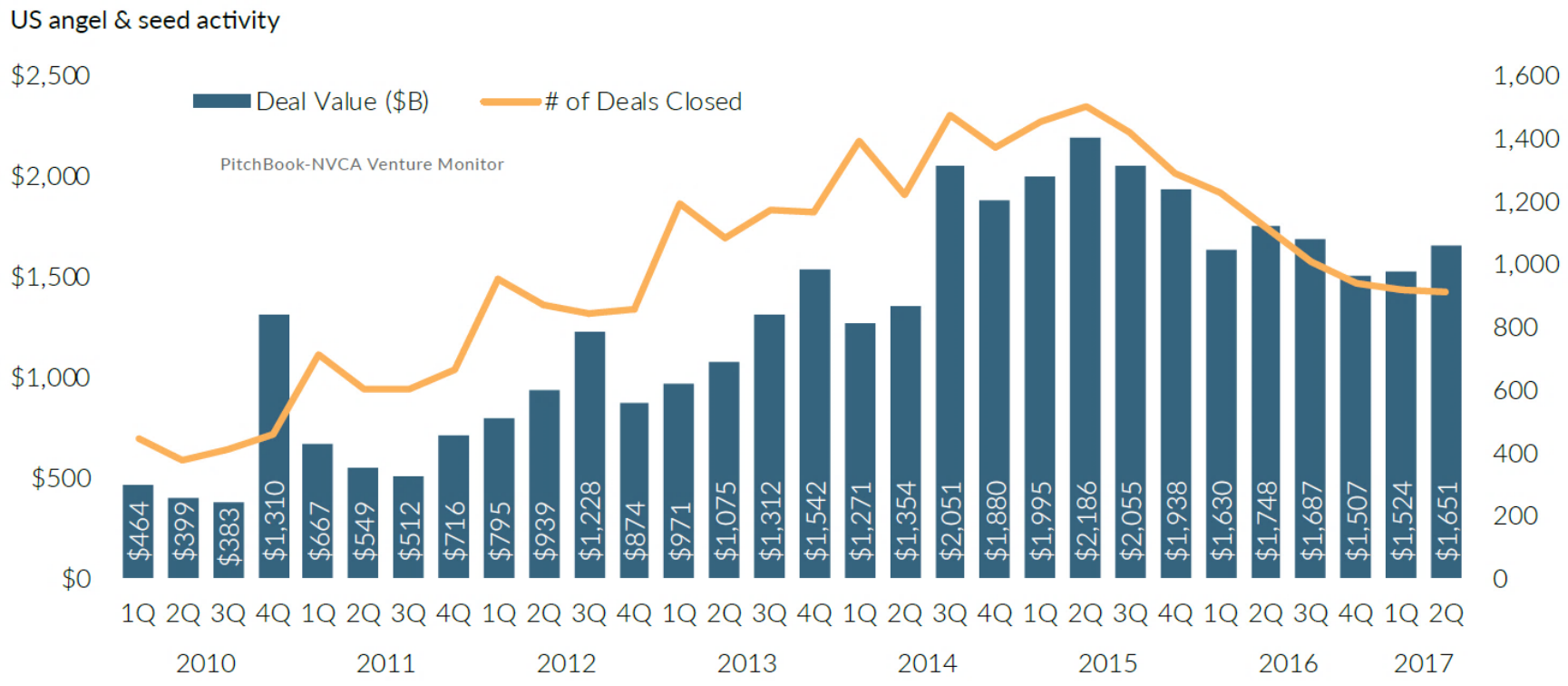
MOST READ

1 Business posts CCTV footage of customer on phone after she posted one-star review: How far should you go to fight online criticism?

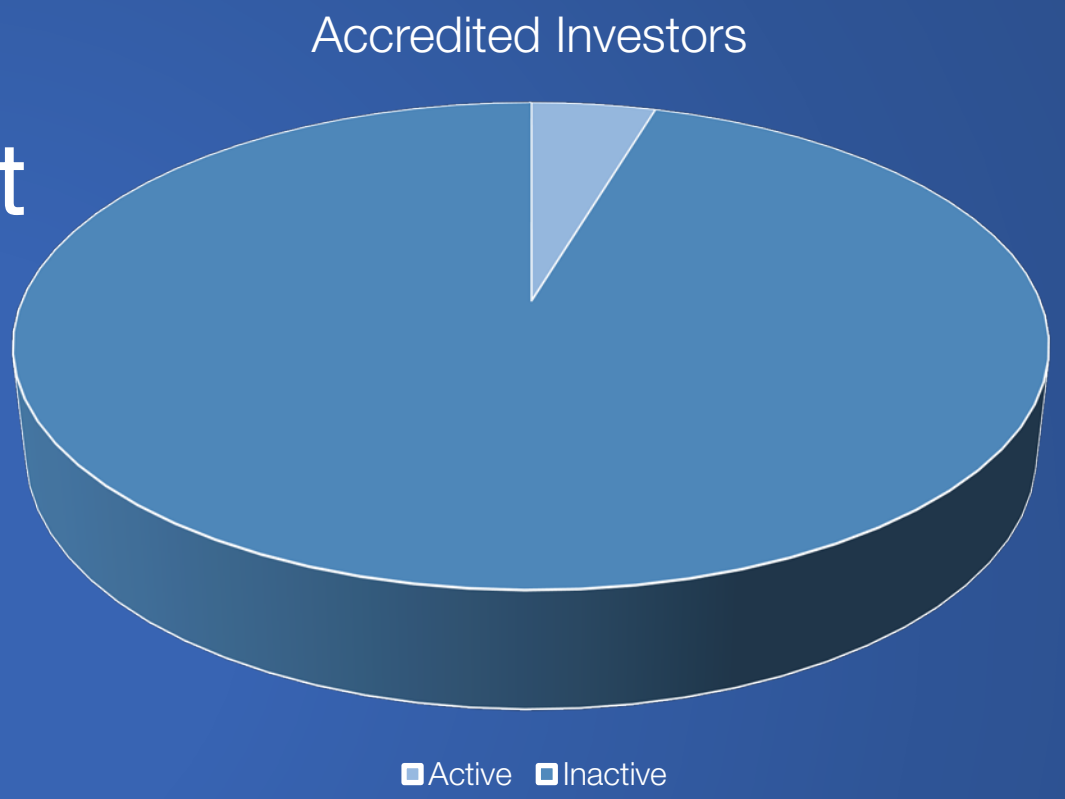
2 Seven phrases you should never use at work

3 Tsunami of customers wage war on Domino's over this six-year deal

# As of 2Q 2017, angel & seed stage funding has seen consecutive declines for eight quarters



Approximately 8,000,000 in the U.S. are allowed to invest in unregistered, Reg D securities as accredited investors




# Only 370,000 are active

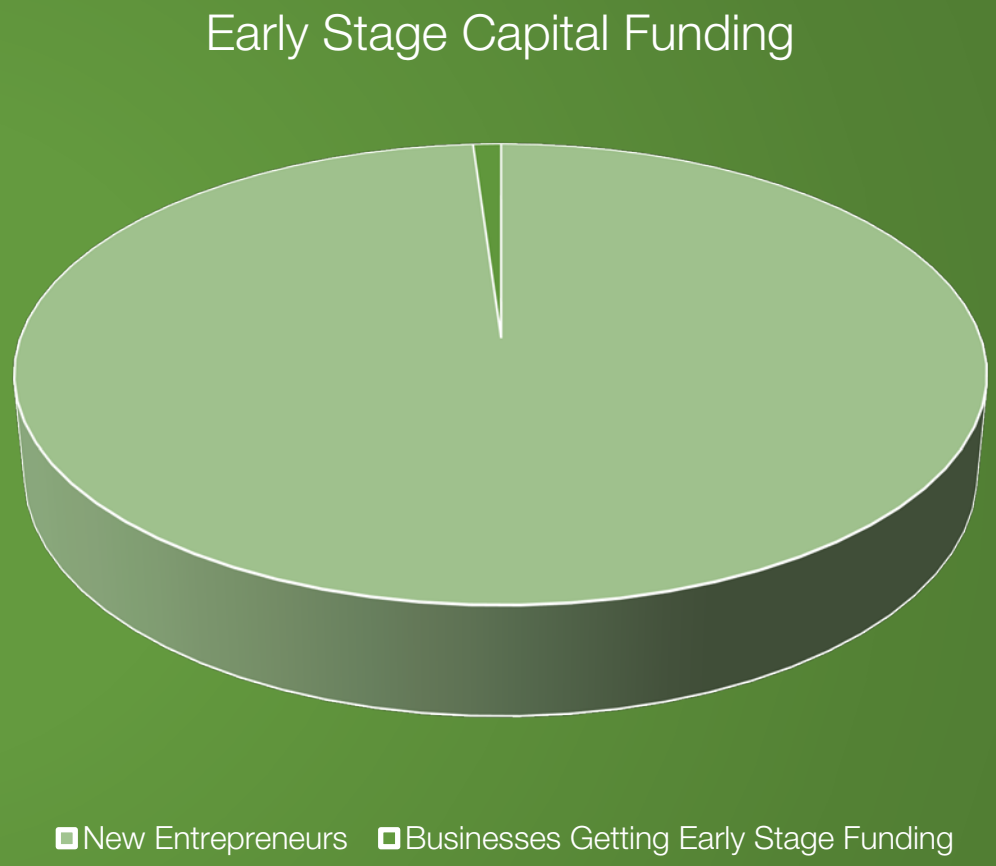
* NVCA / Pitchbook

In 2016, approximately 6,480,000 new entrepreneurs in the USA

* Kauffman Foundation

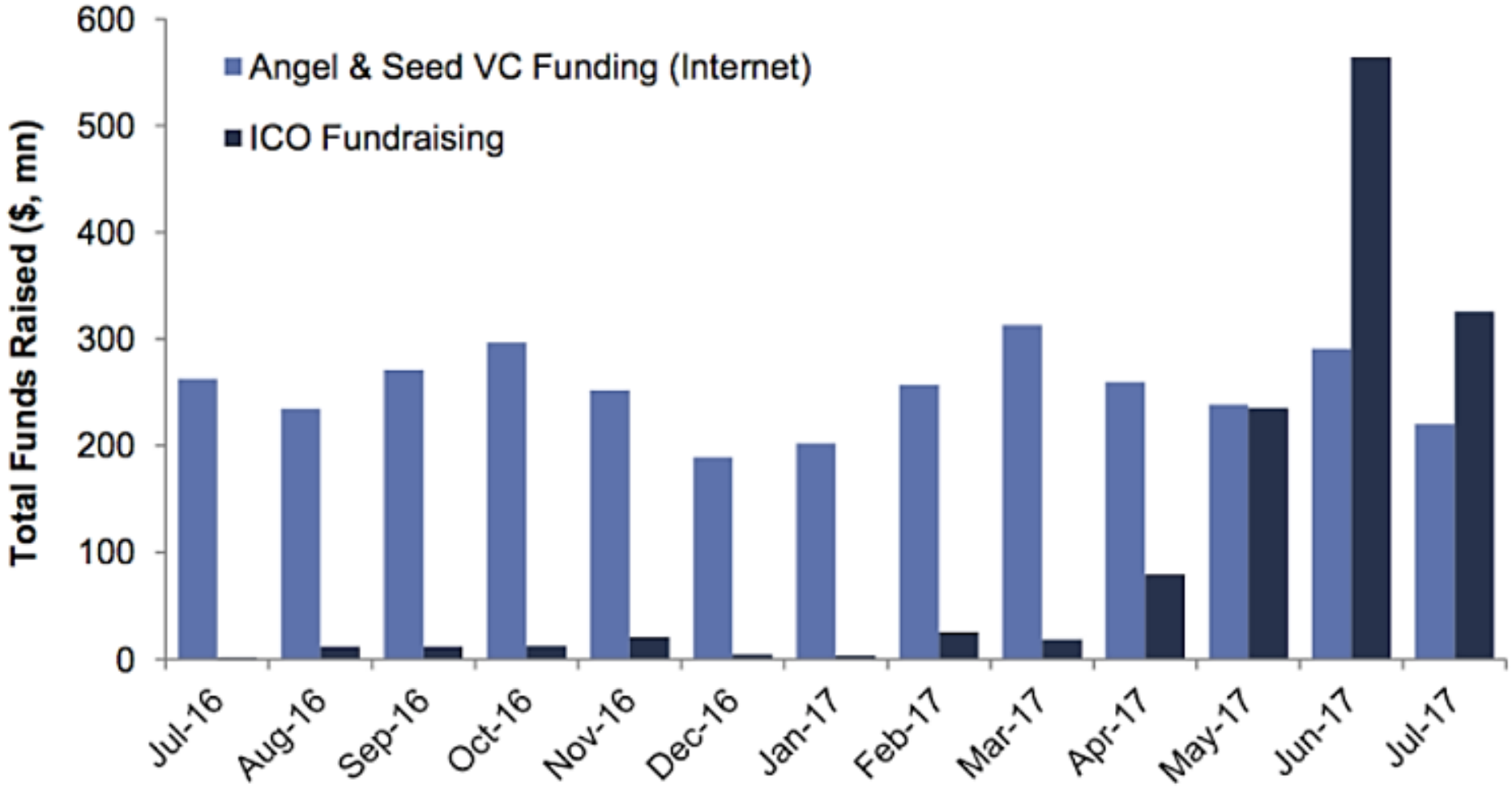
**But only an estimated 70,000 received funding to support their business**

* Angel Capital Association



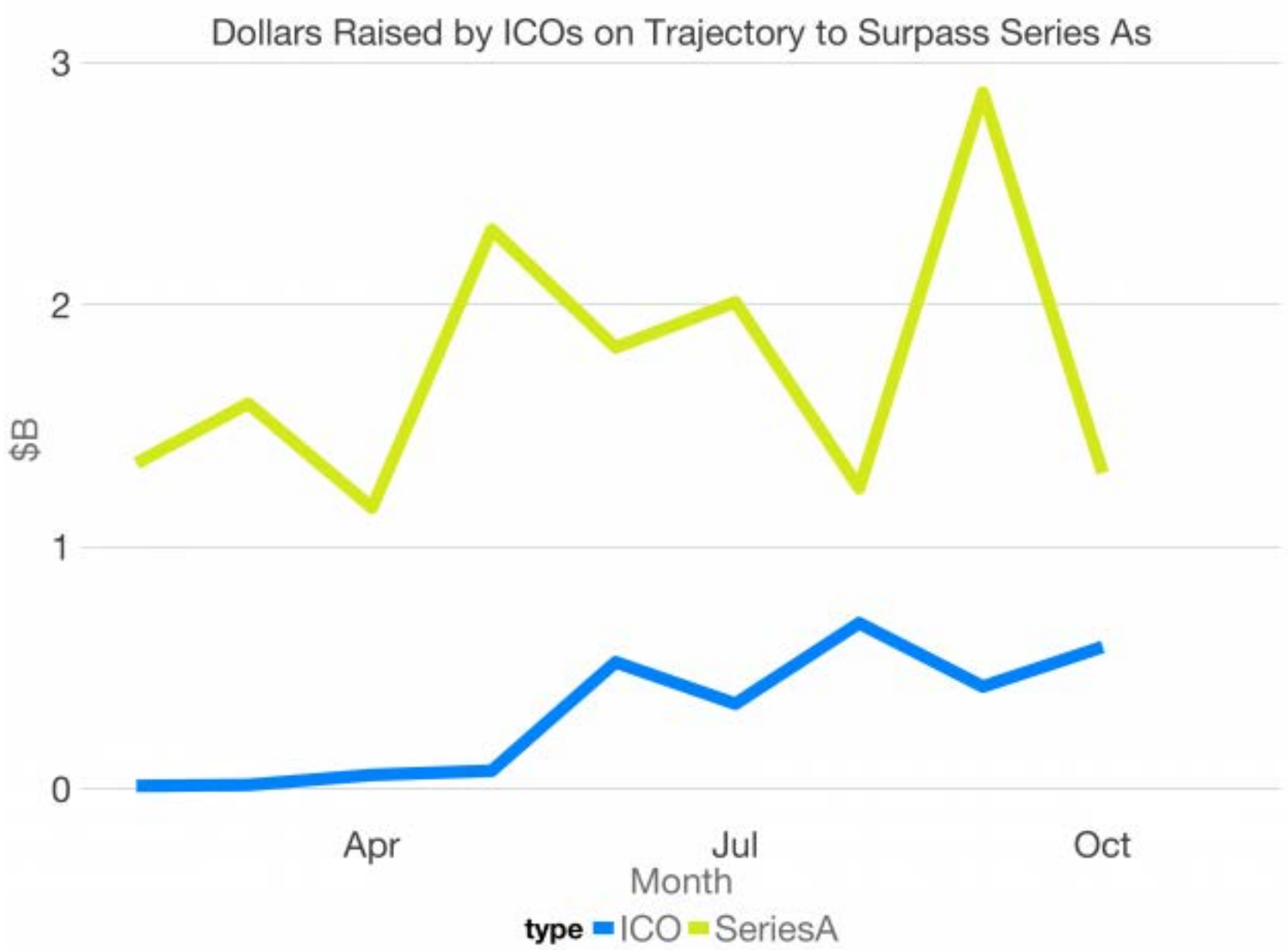

Token sales raised more than angel investors in 2017
$4 billion

## Total Funds Raised by month ($, millions)

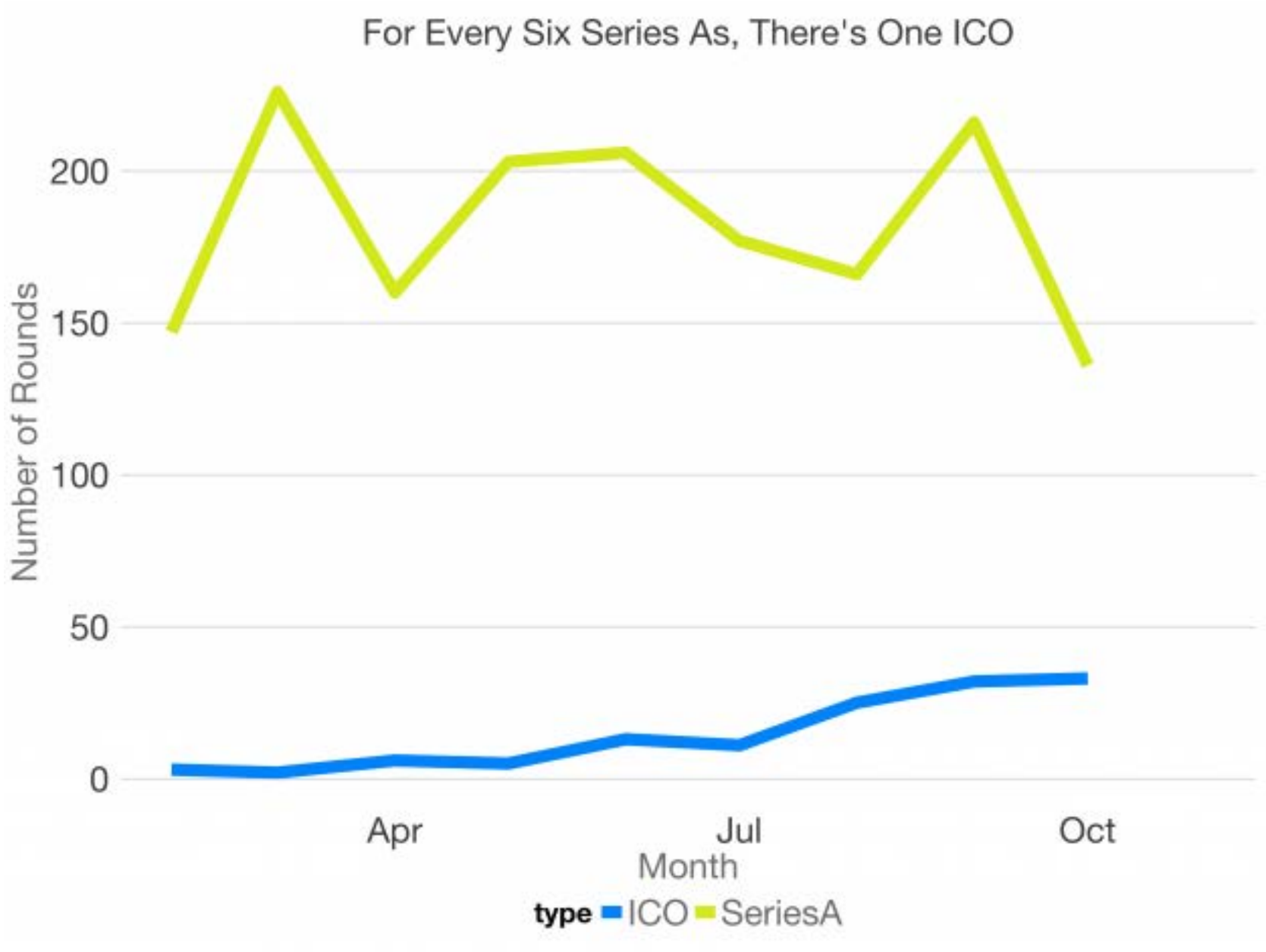



Note: ICO fundraising as of July 18th, 2017, per Coin Schedule. Angel & Seed VC funding data as of July 31st, 2017 and does not include "crowdfunding" rounds.

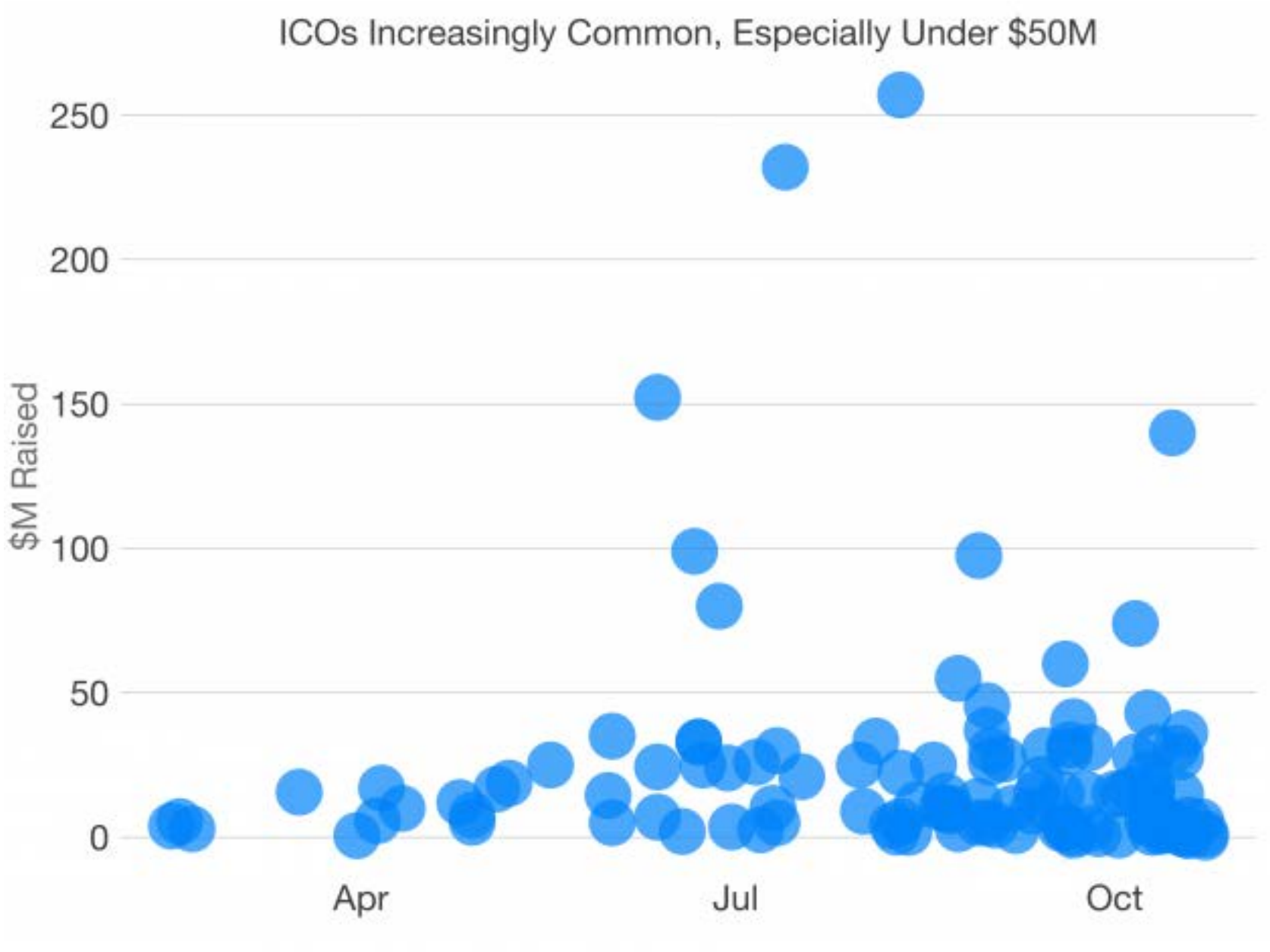
*Source: CoinSchedule, CB Insights, Goldman Sachs Global Investment Research.*


Dollars Raised by ICOs on Trajectory to Surpass Series As
3
2
1
0
$B
Apr
Jul
Oct
Month
type ICO SeriesA

* Crunchbase


For Every Six Series As, There's One ICO
200
150
100
50
0
Number of Rounds
Apr
Jul
Oct
Month
type
ICO
SeriesA

* Crunchbase


ICOs Increasingly Common, Especially Under $50M
$M Raised
250
200
150
100
50
0
Apr
Jul
Oct

* Crunchbase


Global capital mobility creates opportunity

# Three types of tokens

- Cryptocurrency - Bitcoin, Ethereum
- Utility Token
- Asset / Securities Token

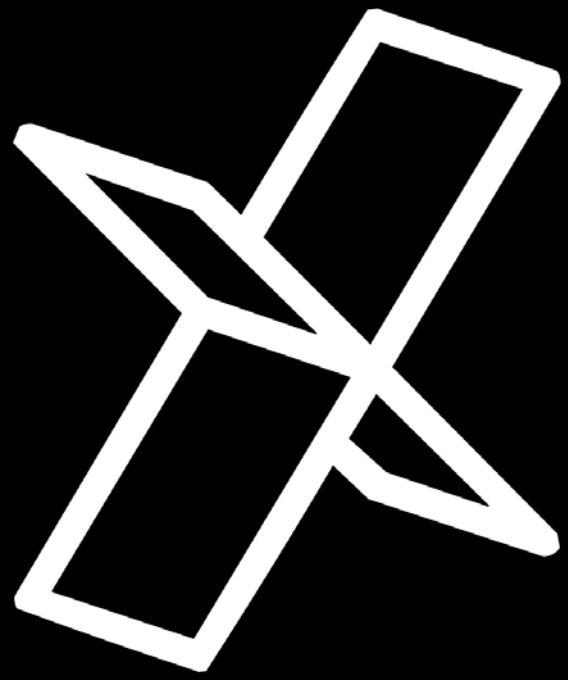

Blockchain platforms must support
REGULATORY
COMPLIANCE

# SEC vs. W.J. Howey Company (1946)

Under the Howey Test, a transaction is an investment contract if:

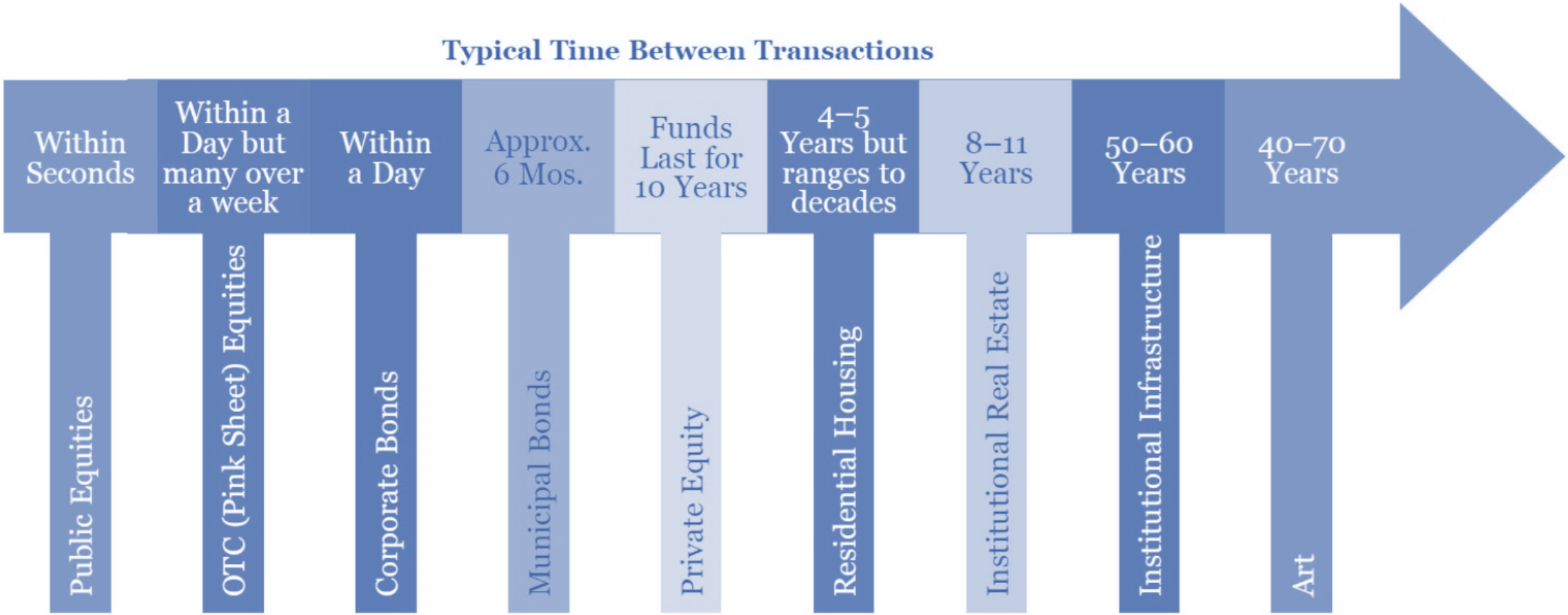
- It is an investment of money
- There is an expectation of profits from the investment
- The investment of money is in a common enterprise
- Any profit comes from the efforts of a promoter or 3rd party


10XTS



# XDEX

# Traditional Asset Liquidity / Fungibility



# Q&A

FOR MORE INFO, CONTACT: MICHAEL@10XTS.COM