BLOCKCHAIN

TRAINING ALLIANCE

BLOCKCHAIN
TRAINING ALLIANCE

BLOCKCHAIN

What is Blockchain

www.blockchaintrainingalliance.com

LETS START AT THE BEGINNING

No prior knowledge of blockchains required

We’ll be looking at Bitcoin, but mostly talking Blockchain

Start with a simplified overview of how it all works, then dive deeper into each section

OVERVIEW

- **Class time: (2 pm – 6 pm)**
- **6 modules organized into**
  - **45 minute sessions**
  - **5 min Q&A (flexible)**
  - **10 minute break**
  - **Start at top of the hour**
  - **Instructor available for additional Q&A at end of call**

OVERVIEW and OBJECTIVES

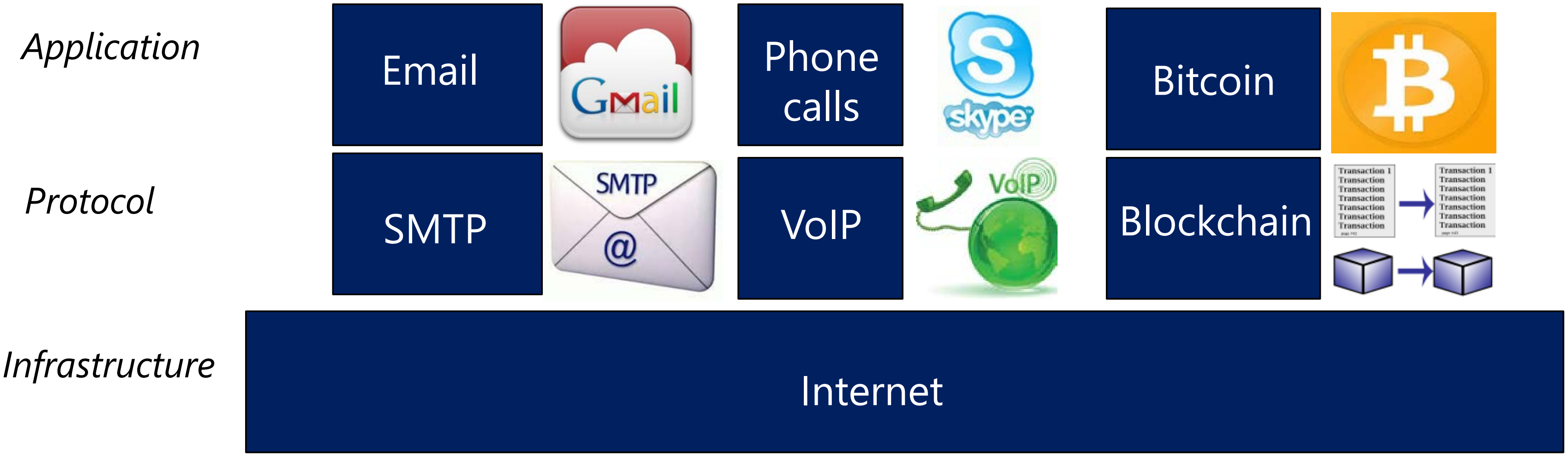
- **Objectives**
  - **What is blockchain, technical overview, business use cases**
- **Modules to cover**
  1. **What is Blockchain**
  2. **Money and Decentralized Networks**
  3. **Blockchain Basics**
  4. **Blockchain Transactions**
  5. **Use Cases**
  6. **Implementation**
- **Materials, Certificate of Completion, Feedback**

INTRODUCTION & PRIMER

What you need to know

What is Blockchain?

- **Blockchain technology is a software; a protocol for the secure transfer of unique instances of value (e.g. money, property, contracts, and identity credentials) via the internet without requiring a third-party intermediary such as a bank or government**
  - **Email over IP, Voice over IP, Money over IP**



Application

Protocol

Infrastructure

Email

SMTP

Phone calls

VoIP

Bitcoin

Blockchain

Internet

How does Bitcoin work?

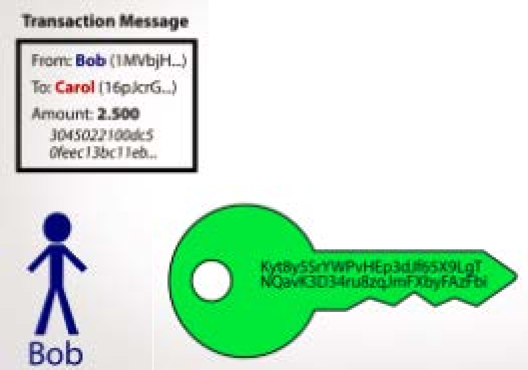
Use eWallet app to submit transaction

Amount:
2.500
To:
Send

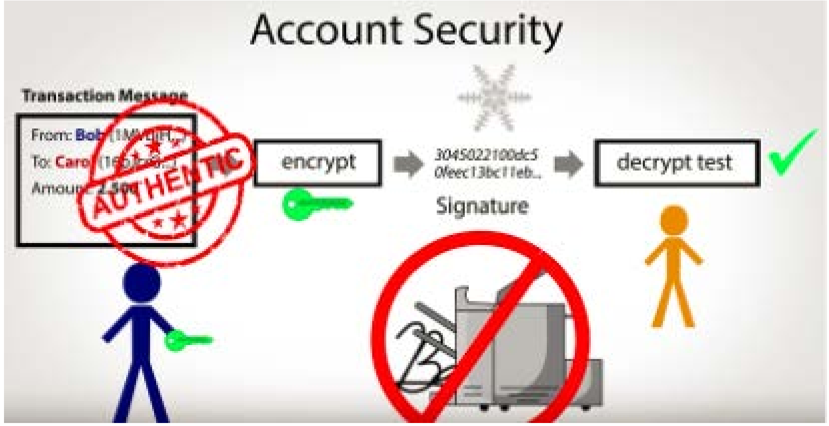
Scan recipient's address
and submit transaction

Amount:
2.500
To:
Send
+2.500

$ appears in recipient's eWallet



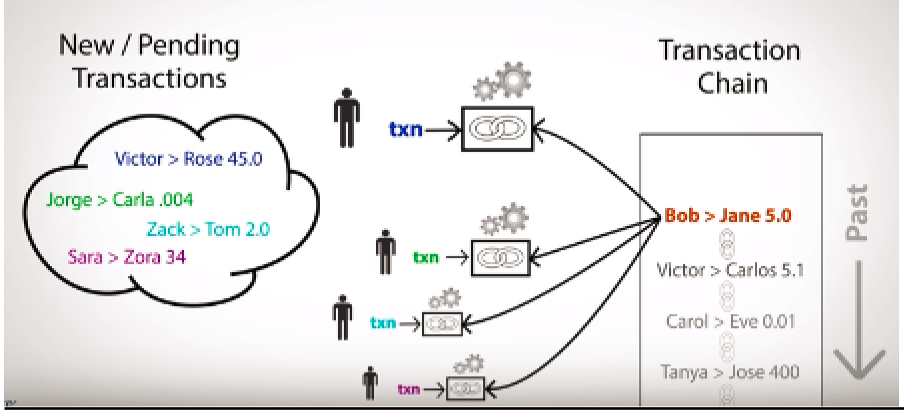
Wallet has keys not money
Creates PKI Signature address pairs



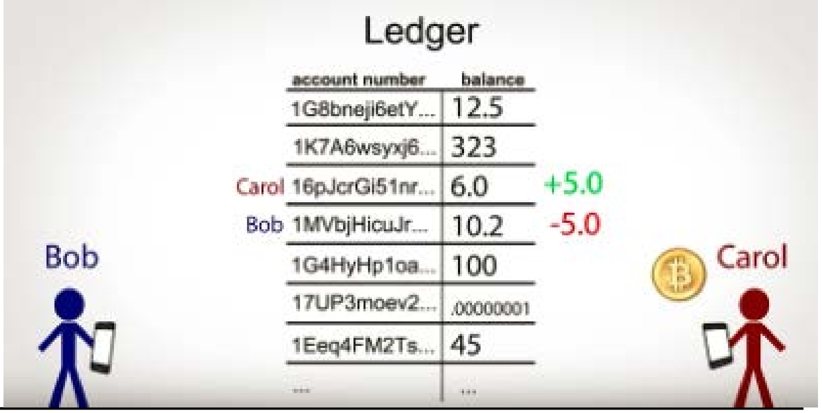
A new PKI hashed signature for each transaction

Source: https://www.youtube.com/watch?v=t5JGQXCTe3c

P2P network confirms & records transactions

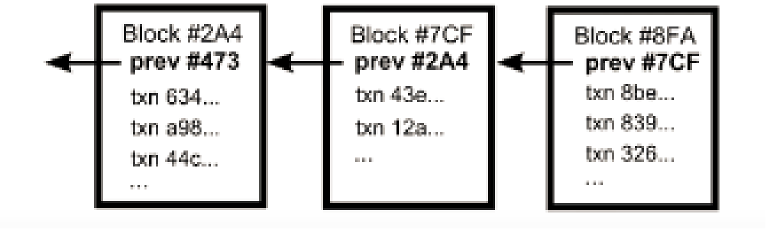


Transactions submitted to mempool, and miners assemble new batch (block) of transactions each 10 min



	account number	balance	
	1G8bneji6etY...	12.5	
	1K7A6wsyxj6...	323	
Carol	16pJcrGi51nr...	6.0	+5.0
Bob	1MVbjHicuJr...	10.2	-5.0
	1G4HyHp1oa...	100	
	17UP3moev2...	.00000001	
	1Eeq4FM2Ts...	45	
	...	...	

Transaction computationally confirmed
Ledger account balances updated



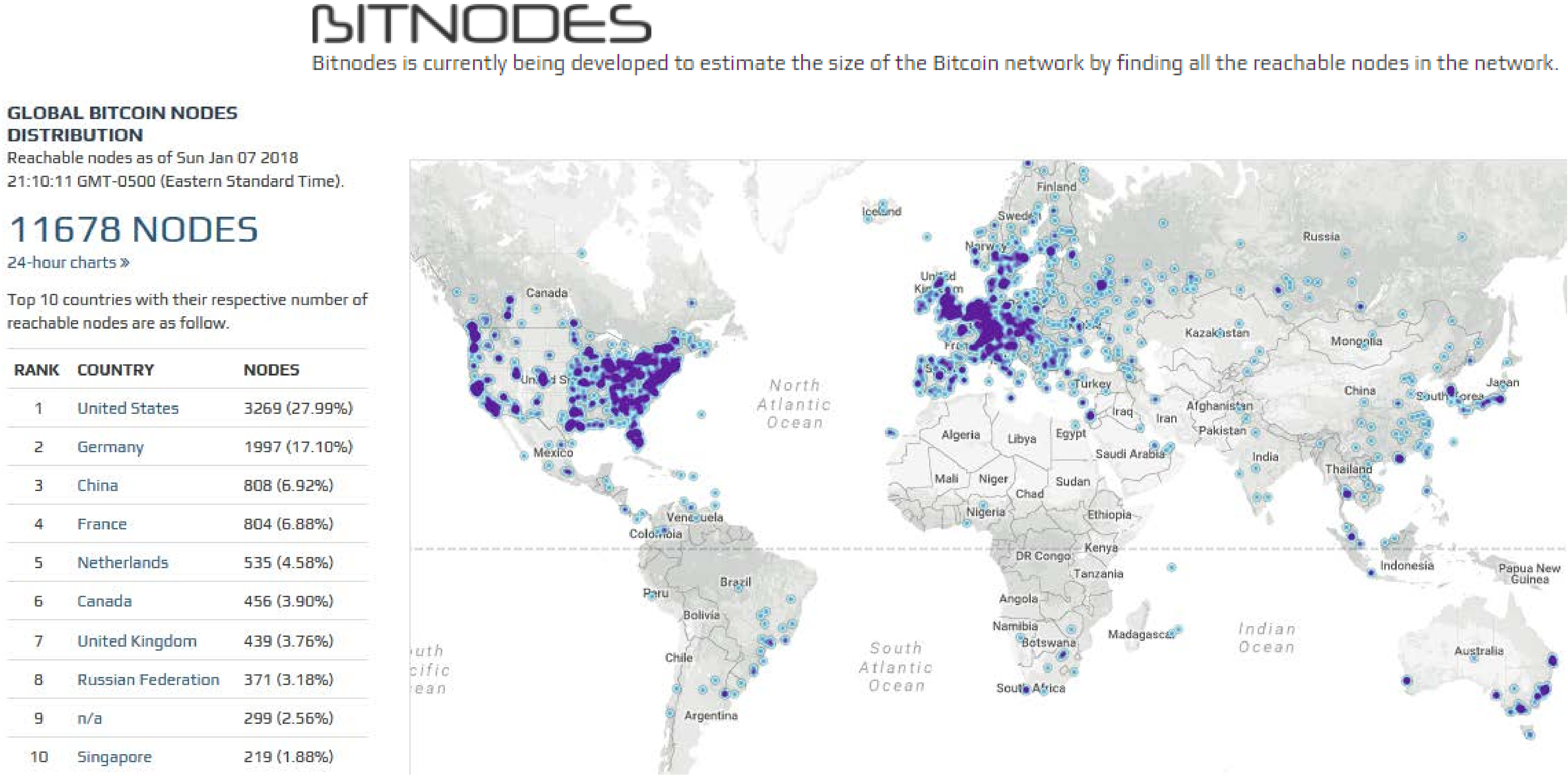
Each block includes a cryptographic hash of the last block, chaining the blocks, hence "Blockchain"

Peer nodes maintain distributed ledger

Source: https://www.youtube.com/watch?v=t5JGQXCTe3c

How robust is the Bitcoin p2p network?

- 11,678 global nodes run full Bitcoind (2/18); 160 gb



BITNODES

Bitnodes is currently being developed to estimate the size of the Bitcoin network by finding all the reachable nodes in the network.

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sun Jan 07 2018 21:10:11 GMT-0500 (Eastern Standard Time).

11678 NODES

24-hour charts »

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

RANK	COUNTRY	NODES
1	United States	3269 (27.99%)
2	Germany	1997 (17.10%)
3	China	808 (6.92%)
4	France	804 (6.88%)
5	Netherlands	535 (4.58%)
6	Canada	456 (3.90%)
7	United Kingdom	439 (3.76%)
8	Russian Federation	371 (3.18%)
9	n/a	299 (2.56%)
10	Singapore	219 (1.88%)

p2p: peer to peer; Source: https://bitnodes.21.co, https://github.com/bitcoin/bitcoin

What is Bitcoin mining?

Run the software yourself:

bitcoin / **bitcoin**

- Mining is the accounting function to record transactions, fee-based ($130,000/block each 10 min)
- Mining ASICs "discover new blocks"
    - Mining software makes nonce guesses to win the right to record a new block ("discover a block")
        - At the rate of 2^32 (4 billion) hashes (guesses)/second
    - One machine at random guesses the 32-bit nonce
- Winning machine confirms and records the transactions, and collects the rewards
    - All nodes confirm the transactions and append the new block to their copy of the distributed ledger
- "Wasteful" effort deters malicious players

Fast because ASICs represent the hashing algorithm as hardware

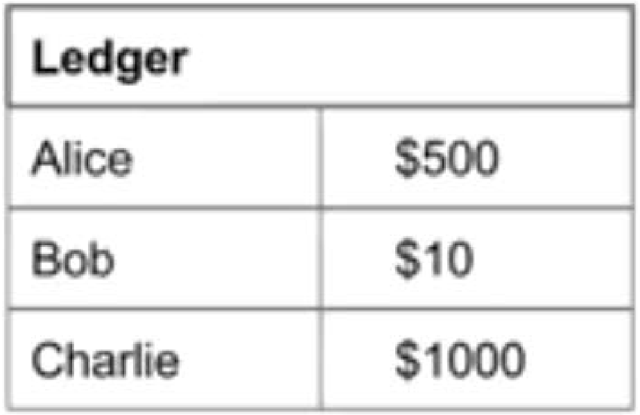
Key Blockchain Concepts

- Public-private networks
  - Trustless vs trusted
- Distributed network
- Consensus algorithms
- Immutability

- Blockchain: trustless, distributed (peer-based), consensus-driven, immutable

What is a Ledger?

- A ledger is like a database, a Google or Excel spreadsheet
- Add new records by appending rows
- Each row contains information
  - Account balances, who owns certain assets
  - Memory and execution state of a computer program



Ledger	
Alice	$500
Bob	$10
Charlie	$1000

Why Distributed?

- Distributed network
- Many nodes or peers that are connected in a network with no single point of failure or centralized control
- Security and resiliency: design the network so that if some peers crash or attack the network maliciously, the network can still operate (Byzantine Fault Tolerance)

What is Immutable?

- Cannot change the data once its committed to the ledger
- Data is auditable
- Change by issuing offsetting transaction
- Smart contract code

Cryptographic Identity

- To use the network, need a Cryptographic Identity
  - (sort of like an email address)
  - If want to access your email, you need the password, which functions similarly to a private key and your public key is like your address (more complicated)
- Authentication: peers sign transactions with their cryptographic identity, this enables account “ownership” and can attribute blame

Consensus in Distributed Networks

- In order to update the ledger, the network needs to come to consensus using an algorithm
- Consensus: what does it mean to come to consensus on a distributed network?
  - It means that everyone agrees on the current state (e.g. how much money does each account have) and making sure that no one is double-spending money (easy in Bitcoin, more complex in Ethereum, business networks)
- How do we come to consensus in this distributed manner?

Three Primary Consensus Algorithms

- POW: Proof of Work (Bitcoin)
  - Expensive, not ecological, wasteful computation
- POS: Proof of Stake (Ethereum)
- Next-gen: PBFT: Practical Byzantine Fault Tolerance (DFINITY, Algorand)
  - Law of large numbers: **diversity of participants**
  - For each block of transactions, randomly select a small, one-time group of users in a safe and fair way
  - To protect from attackers, the identities of these users are hidden until the block is confirmed
  - The size of this group remains constant as the network grows

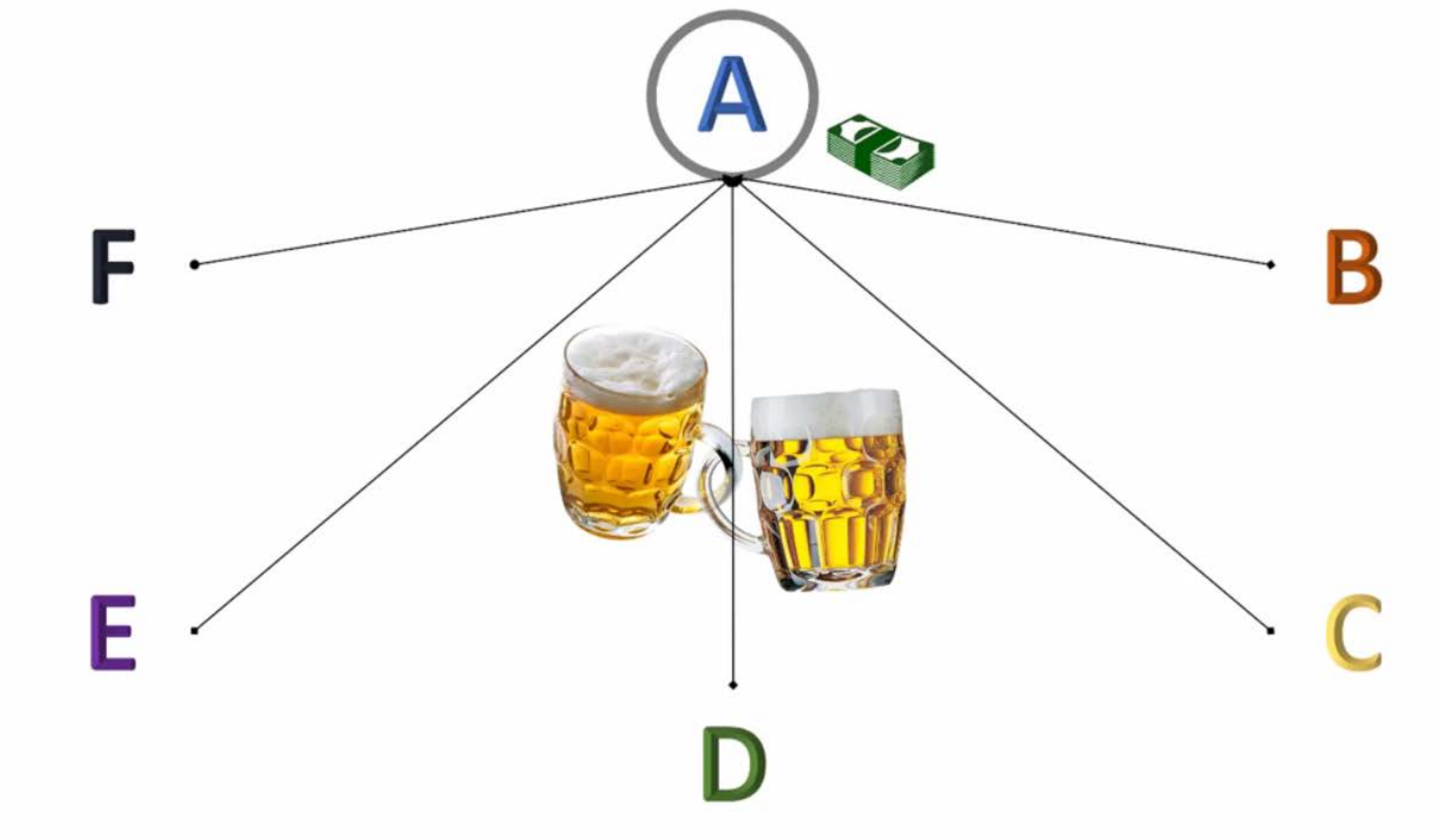
Key Blockchain Concepts

- Public-private networks
  - Trustless vs trusted
- Distributed network
- Consensus algorithms
- Immutability

- Blockchain: trustless, distributed (peer-based), consensus-driven, immutable

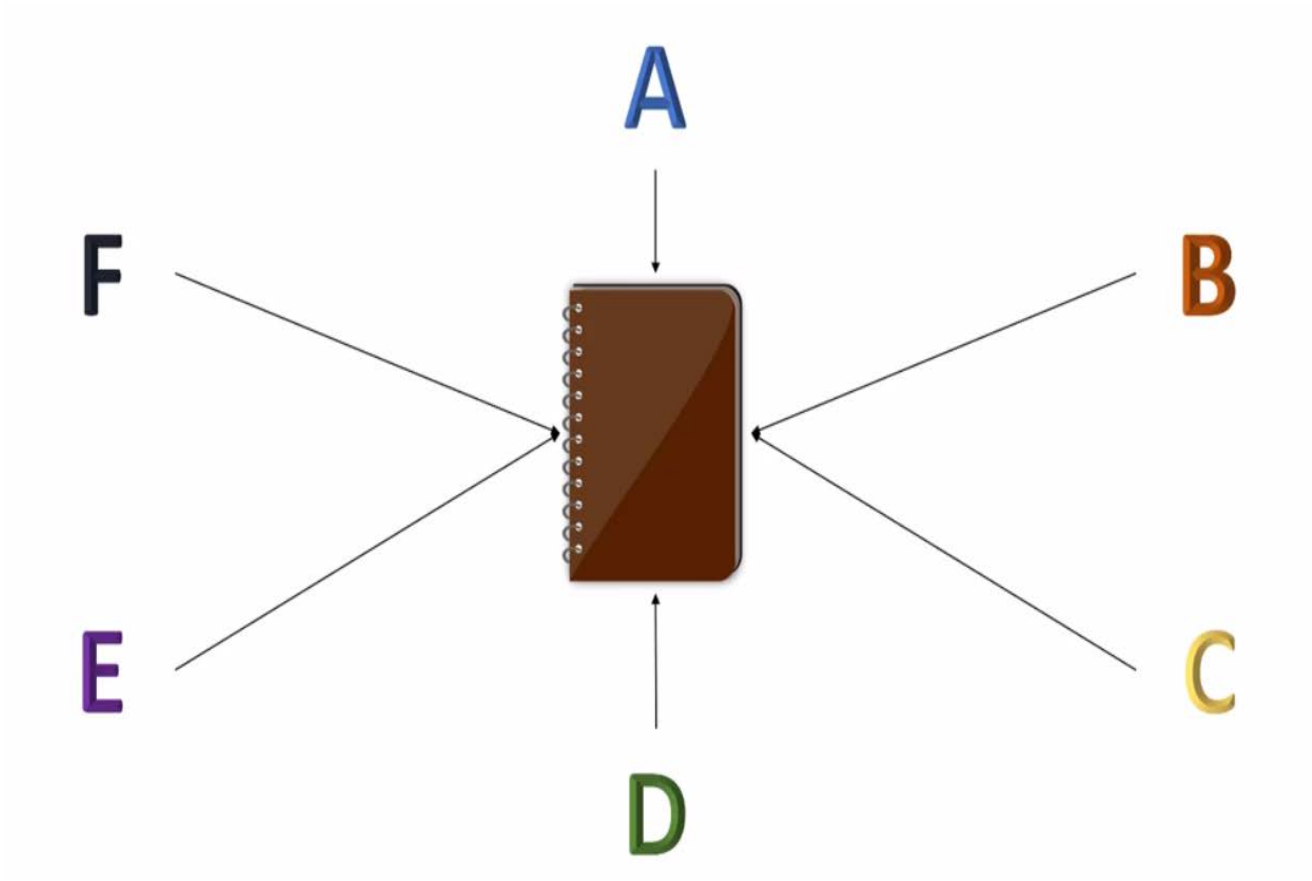
What problem does Blockchain solve?

- **Trip to the Bar**



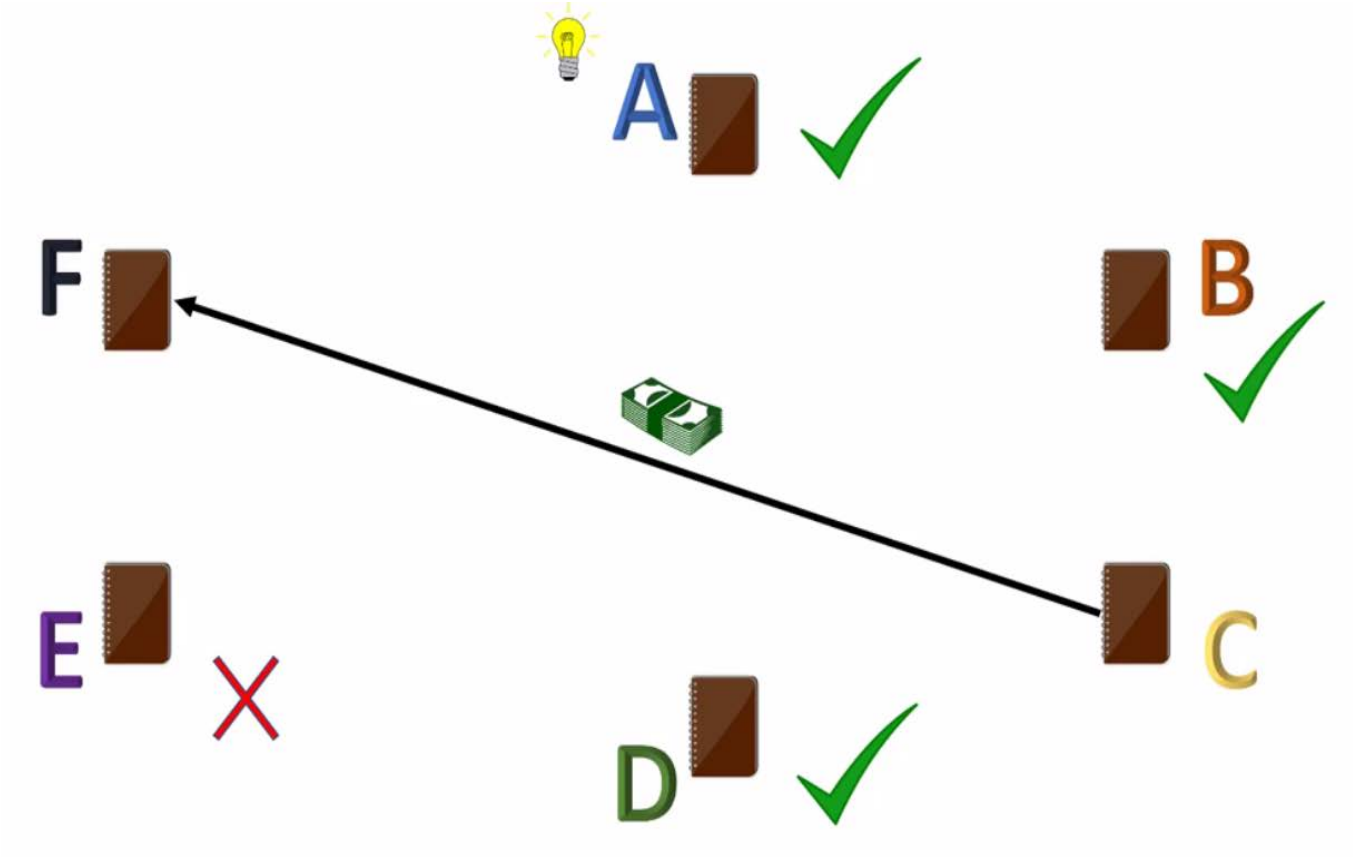
What is Blockchain

- **Common Ledger**



What is Blockchain

- **A More Common Ledger**



BLOCKCHAIN ADOPTION

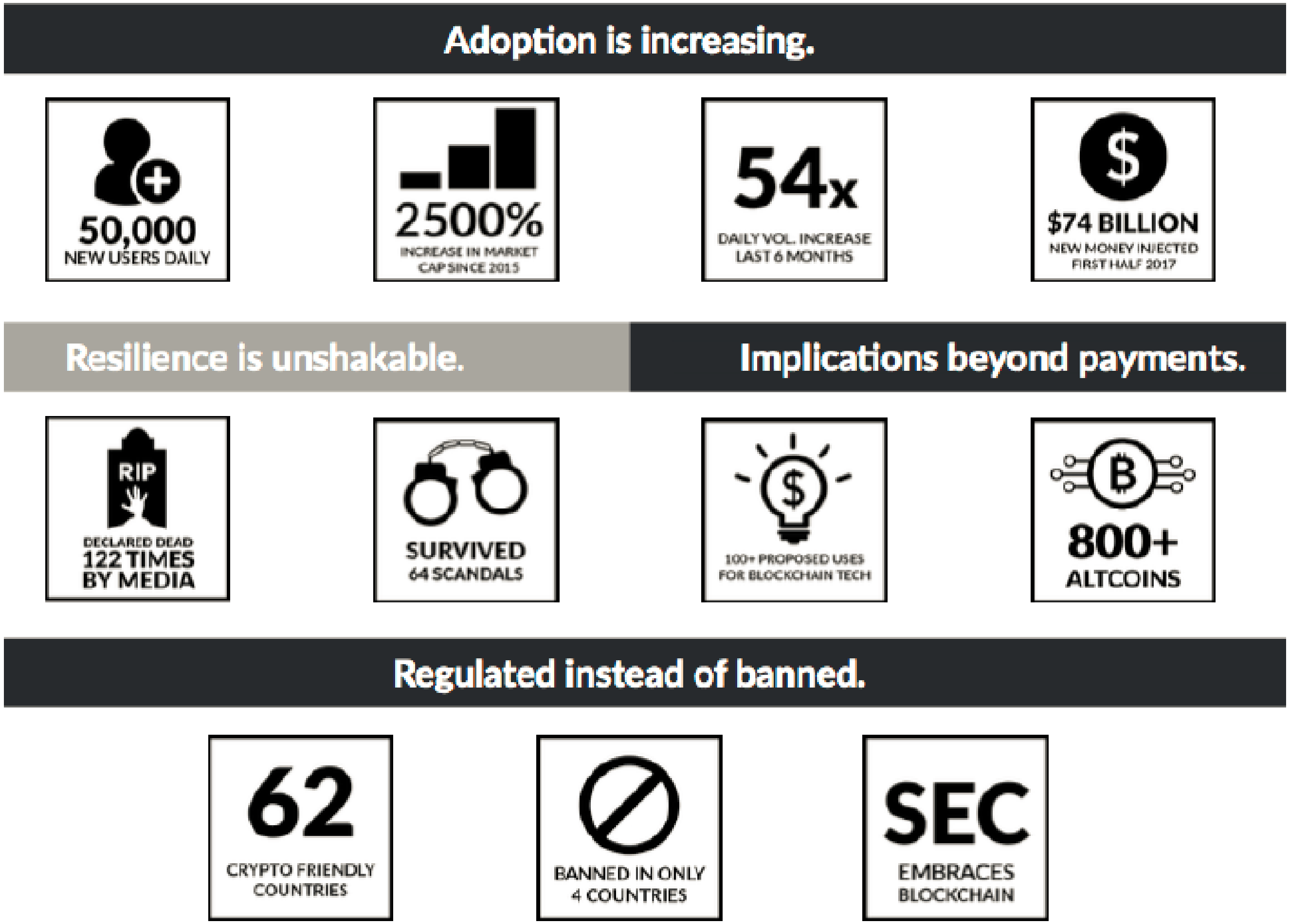
One of the fastest-moving technology adoptions

Blockchain Adoption

- Blockchain (distributed ledger technology) is being considered by more than half of the world's big corporations, according to a Juniper market research survey released Jul 2017
  - 57 percent of large corporations – defined as any company with more than 20,000 employees – were either actively considering or in the process of deploying blockchain
  - Two-thirds of companies surveyed by Juniper said that they expected the technology to be integrated into their systems by the end of 2018
- IDC: $2.1 billion estimated global blockchain spend 2018

https://www.cnbc.com/2017/07/31/blockchain-technology-considered-by-57-percent-of-big-corporations-study.html

Blockchain Adoption



Adoption is increasing.

50,000
NEW USERS DAILY

2500%
INCREASE IN MARKET CAP SINCE 2015

54x
DAILY VOL. INCREASE LAST 6 MONTHS

$74 BILLION
NEW MONEY INJECTED FIRST HALF 2017

Resilience is unshakable.

RIP
DECLARED DEAD 122 TIMES BY MEDIA

SURVIVED 64 SCANDALS

Implications beyond payments.

100+ PROPOSED USES FOR BLOCKCHAIN TECH

800+ ALTCOINS

Regulated instead of banned.

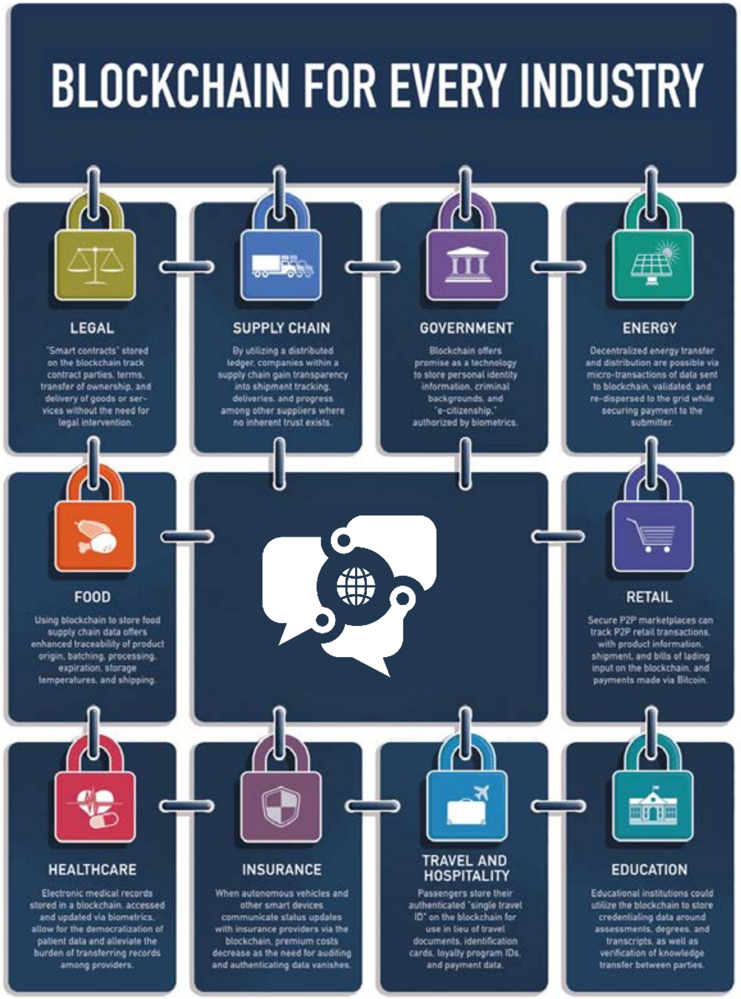
62
CRYPTO FRIENDLY COUNTRIES

BANNED IN ONLY 4 COUNTRIES

SEC
EMBRACES BLOCKCHAIN

https://www.slideshare.net/SebastianCochinescu/vlad-andrei-tokens-deep-dive-presentation

The Future of Blockchain



BLOCKCHAIN FOR EVERY INDUSTRY

LEGAL

"Smart contracts" stored on the blockchain track contract parties, terms, transfer of ownership, and delivery of goods or services without the need for legal intervention.

SUPPLY CHAIN

By utilizing a distributed ledger, companies within a supply chain gain transparency into shipment tracking, deliveries, and progress among other suppliers where no inherent trust exists.

GOVERNMENT

Blockchain offers promise as a technology to store personal identity information, criminal backgrounds, and "e-citizenship," authorized by biometrics.

ENERGY

Decentralized energy transfer and distribution are possible via micro-transactions of data sent to blockchain, validated, and re-dispersed to the grid while securing payment to the submitter.

FOOD

Using blockchain to store food supply chain data offers enhanced traceability of product origin, batching, processing, expiration, storage temperatures, and shipping.

RETAIL

Secure P2P marketplaces can track P2P retail transactions, with product information, shipment, and bills of lading input on the blockchain, and payments made via Bitcoin.

HEALTHCARE

Electronic medical records stored in a blockchain, accessed and updated via biometrics, allow for the democratization of patient data and alleviate the burden of transferring records among providers.

INSURANCE

When autonomous vehicles and other smart devices communicate status updates with insurance providers via the blockchain, premium costs decrease as the need for auditing and authenticating data vanishes.

TRAVEL AND HOSPITALITY

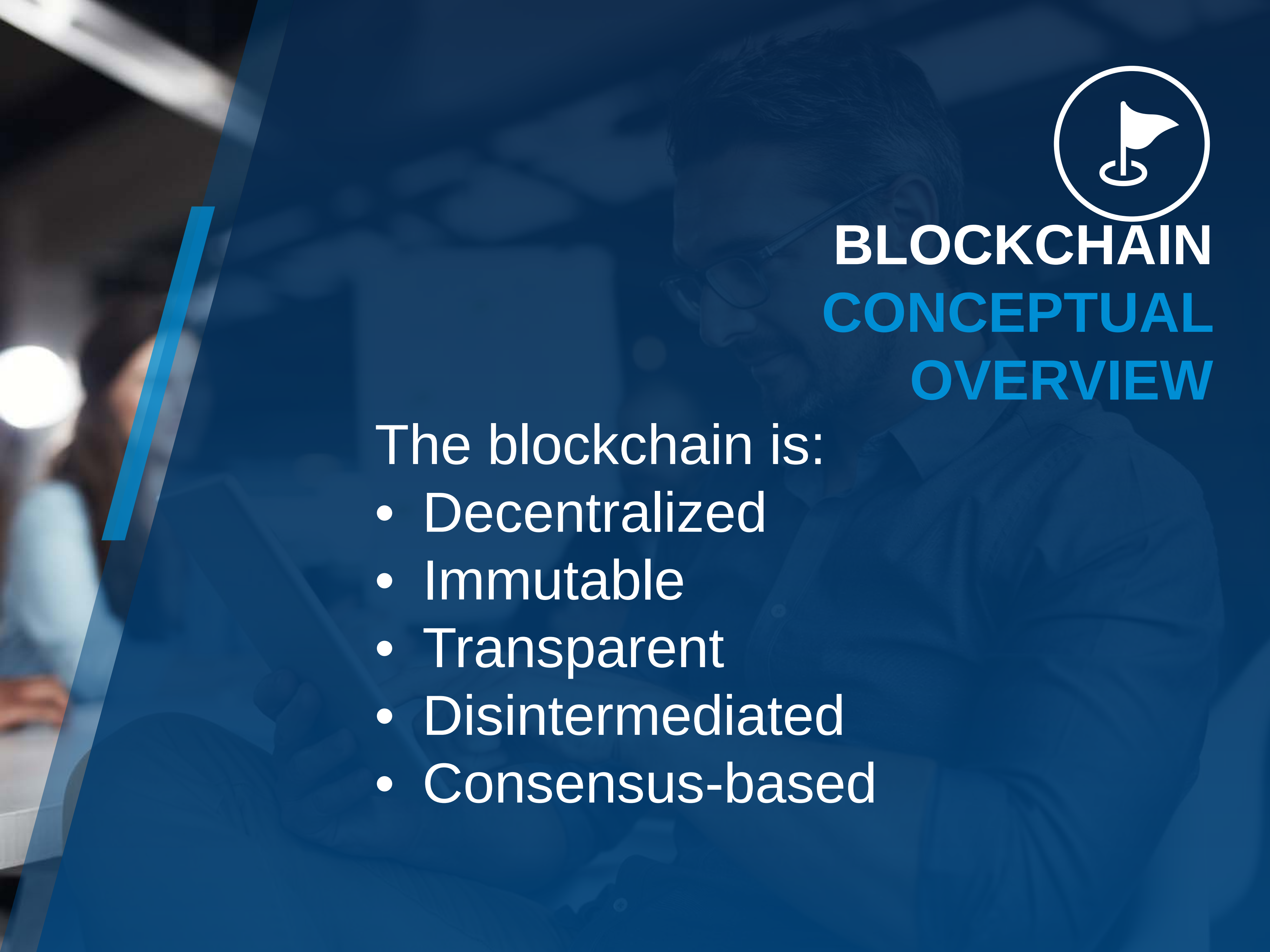
Passengers store their authenticated "single travel ID" on the blockchain for use in lieu of travel documents, identification cards, loyalty program IDs, and payment data.

EDUCATION

Educational institutions could utilize the blockchain to store credentialing data around assessments, degrees, and transcripts, as well as verification of knowledge transfer between parties.

Transforming Society

- Blockchain technology is bringing us the Internet of value: a new platform to reshape the world of business
- It transcends all physical and geographical barriers and uses math and cryptography to enable transactions globally.
- The uniqueness of blockchain lies in its capacity to store and retain person-to-person transactional history, so that chances of fraud, hacking, and third-party interference are eliminated.



BLOCKCHAIN CONCEPTUAL OVERVIEW

The blockchain is:

- Decentralized
- Immutable
- Transparent
- Disintermediated
- Consensus-based

Blockchain combines existing technologies to prevent the double-spend problem

Cleverly combined software components

- Distributed Systems
- Peer-to-peer networks
- Hashing functions
- Public - Private key cryptography
- Cryptographic signatures
- Elliptic curve cryptography

USE CASES

- **Background checks: education credentials, criminal records**
- **Secure document storage: home deed, auto title**
- **Birth registries**
- **Land registries**
- **Financial services: securities clearing, syndicated loans**
- **Global supply chain: automotive recalls and counterfeit airbags**
- **Healthcare: EMRs, insurance claims, genome research**
- **Airlines: registration, re-booking, vouchers, loyalty**
- **Tokenized economy: Tech Coworking space 1 token = 1 seat**
- **Payment channels: Starbucks or for bandwidth consumption**

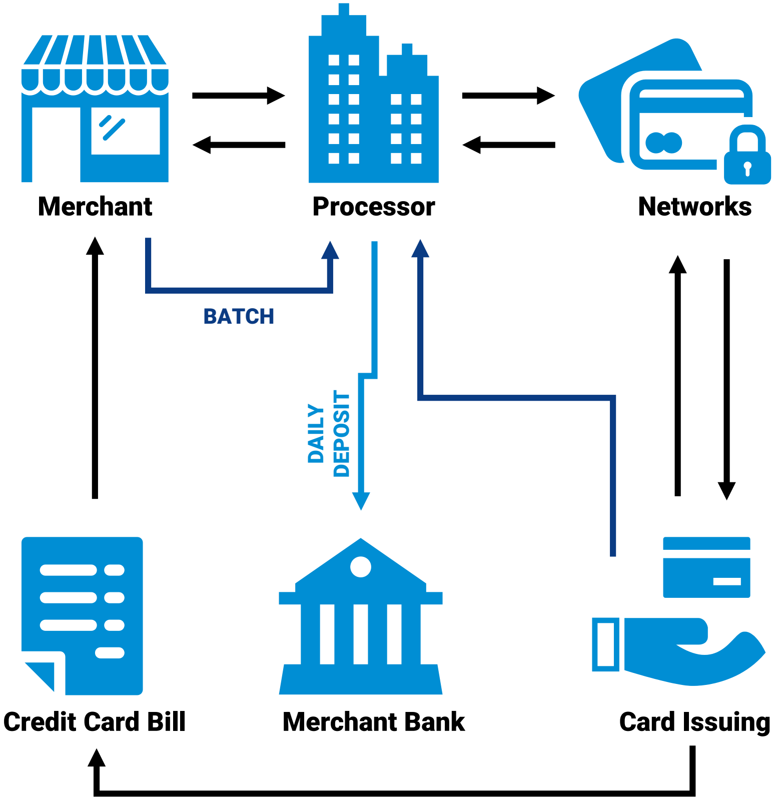
IT’S ALL
ABOUT TRANSACTIONS

CASH IS PEER TO PEER

Observations:

- No middleman required
- DIY Fraud detection
- Sufficient trust for the value of the transaction
- Anonymous/Private
- Distributed

ELECTRONIC MIDDLEMEN



Observations:

- Requires 3rd party trust
- The more complex the flow, the more middlemen required
- Specialized equipment needed (e.g. POS terminal, connection to Txn networks
- Fraud detection by 3rd parties
- Every step adds cost

MIDDLEMEN ADDING VALUE

- **Provision of infrastructure (Terminals, network connections, etc.)**
- **Management of commercial relationships between parties (Lots of lawyers)**
- **Abstraction of complexity**
- **Fraud detection**
- **Customer service**
- **Regulatory compliance KYC, AML, Risk reporting**
- **Removal of bad-actors from the ecosystem**

Until now, this is the best way we’ve been able to achieve the goal of person-to-person transactions at a distance.

BLOCKCHAIN POWERED PAYMENT NETWORKS

Now:

- Online banking transaction growth
- SME’s/Retail acceptance of electronic transactions
- Online purchases/Commerce
- In-App purchases
- Virtual currencies in games
- International Transaction growth (Commerce and Remittance)
- Value storage cards (loyalty cards, ERP, gift cards etc etc)

Future:

- Internet of Things
- Autonomous Objects
- Programmable money/Finance automation

IN GENERAL...

The easier it is to conduct transactions the more people transact.

LIMITATIONS

- Cash is king….but only useful locally and small amounts
- Electronic transactions require Credit/Debit card
  - Fees are high for merchants (Fixed Fee + 1-3%)
  - Settlement is slow (multiple days)
  - Chargebacks shift risk to merchant
  - Microtransactions are cost prohibitive
- Walled garden/In-country solutions are piecemeal
- International Transfers ITT/Swift
  - Slow, costly, mistake prone
- High onboarding costs/bureaucracy

2 billion world-wide underbanked (PWC 2016)

BLOCKCHAIN POWERED PAYMENT NETWORKS

Solved:

- Return to Peer-to-Peer
- Speed
- Trustless trust
- No special equipment needed
- Fraud
- Minimal Cost
- No chargebacks
- No monthly fees
- Transparency

Ignored:

- Policing bad-actors
- KYC/AML
- Insurance
- Onboarding process
- Customer service
- Commercial Relationships

Challenges:

- Technical Complexity
- Regulatory Uncertainty
- Getting the currency in the first place

MANY BLOCKCHAINS

- It's easy to create your own, and there are many.

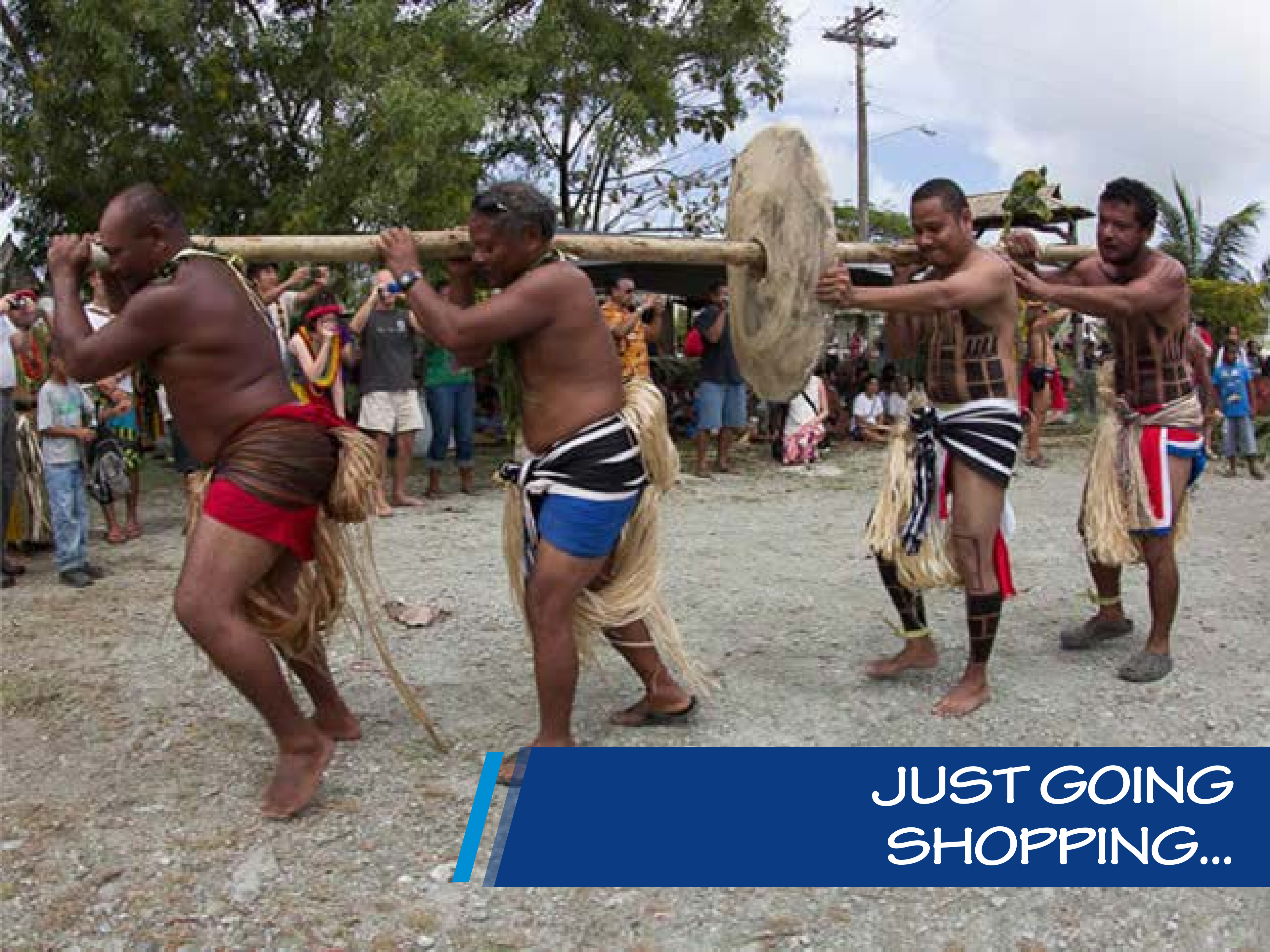
- Each is separate and runs its own blockchain

- The value transferred in each blockchain is primarily its own currency

WHAT IS A BLOCKCHAIN?

What you need to know

IT ALL STARTS HERE



JUST GOING SHOPPING...

A CENTRALISED LEDGER

IMPORTING THE STONES

SOME INTERESTING OBSERVATIONS

- **The stones themselves had no non-monetary value**
- **Eventually, spending your stones didn't require physically moving the stone – just acknowledgement of a change of ownership**
- **Impossible to do a trade in secret**
- **They developed a form of distributed ledger, but...**
- **It couldn't scale!**

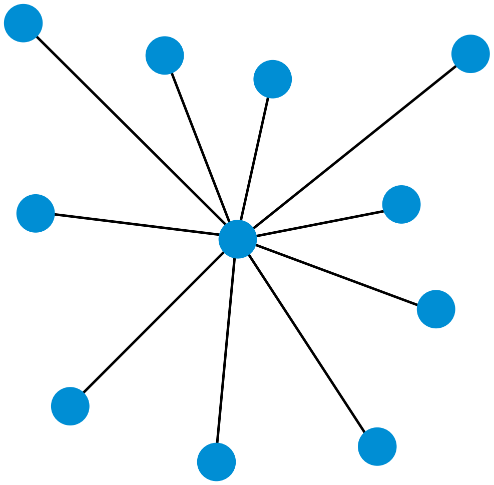
A BLOCKCHAIN IS AN IMPLEMENTATION OF A LEDGER

- **Ledgers record transactions - the passing of value from owner to owner**
- **Transactions are time based**
- **Once a Txn is recorded you can't alter them**
- **You need to be able to detect if your ledger has been altered**

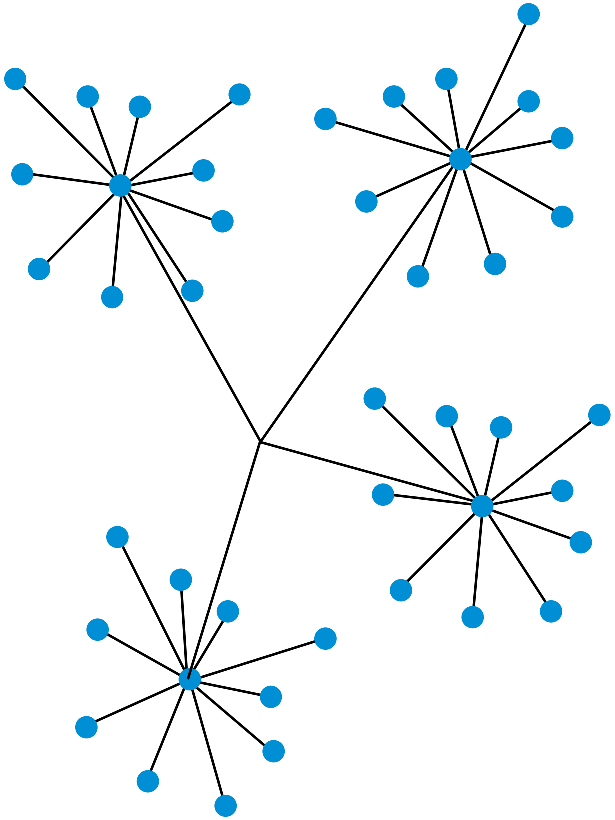
A blockchain is a protocol for building an immutable historical record of transactions

BLOCKCHAINS ARE DISTRIBUTED

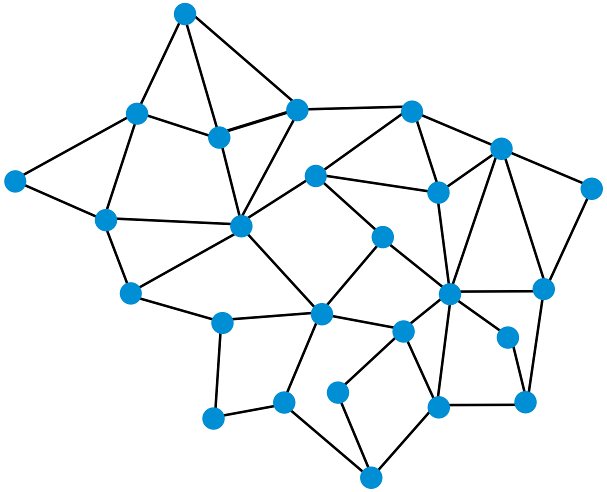
NETWORK EVOLUTION



i) centralized

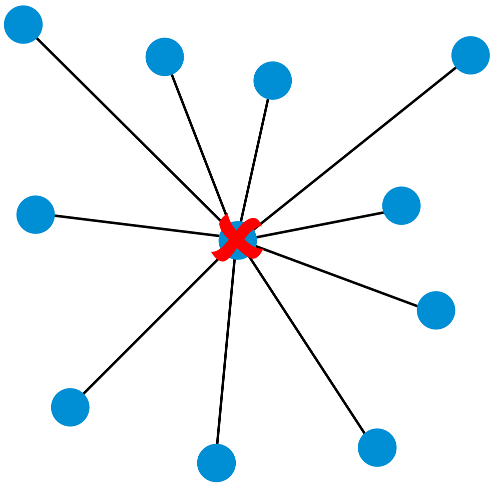


ii) decentralized

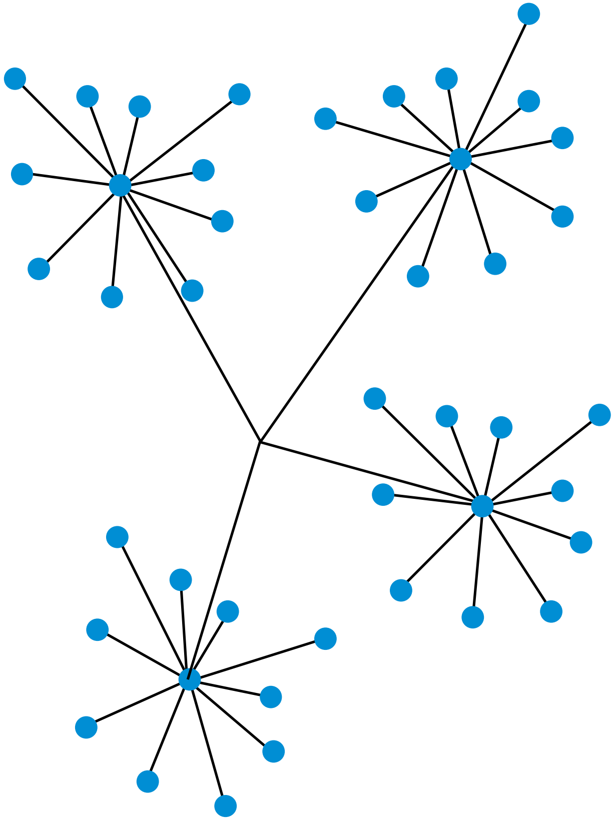


iii) distributed

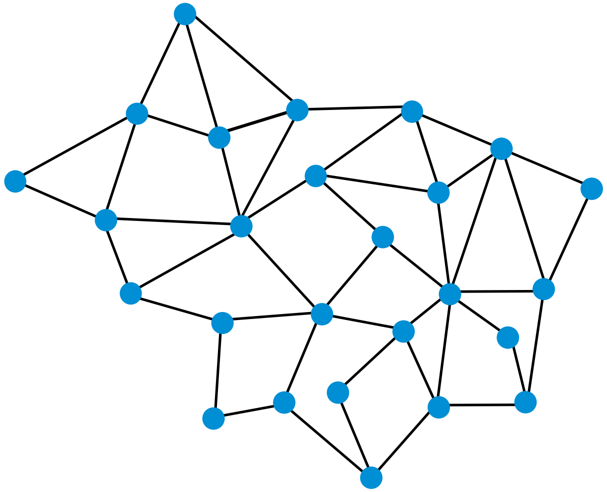
NETWORK EVOLUTION



i) centralized

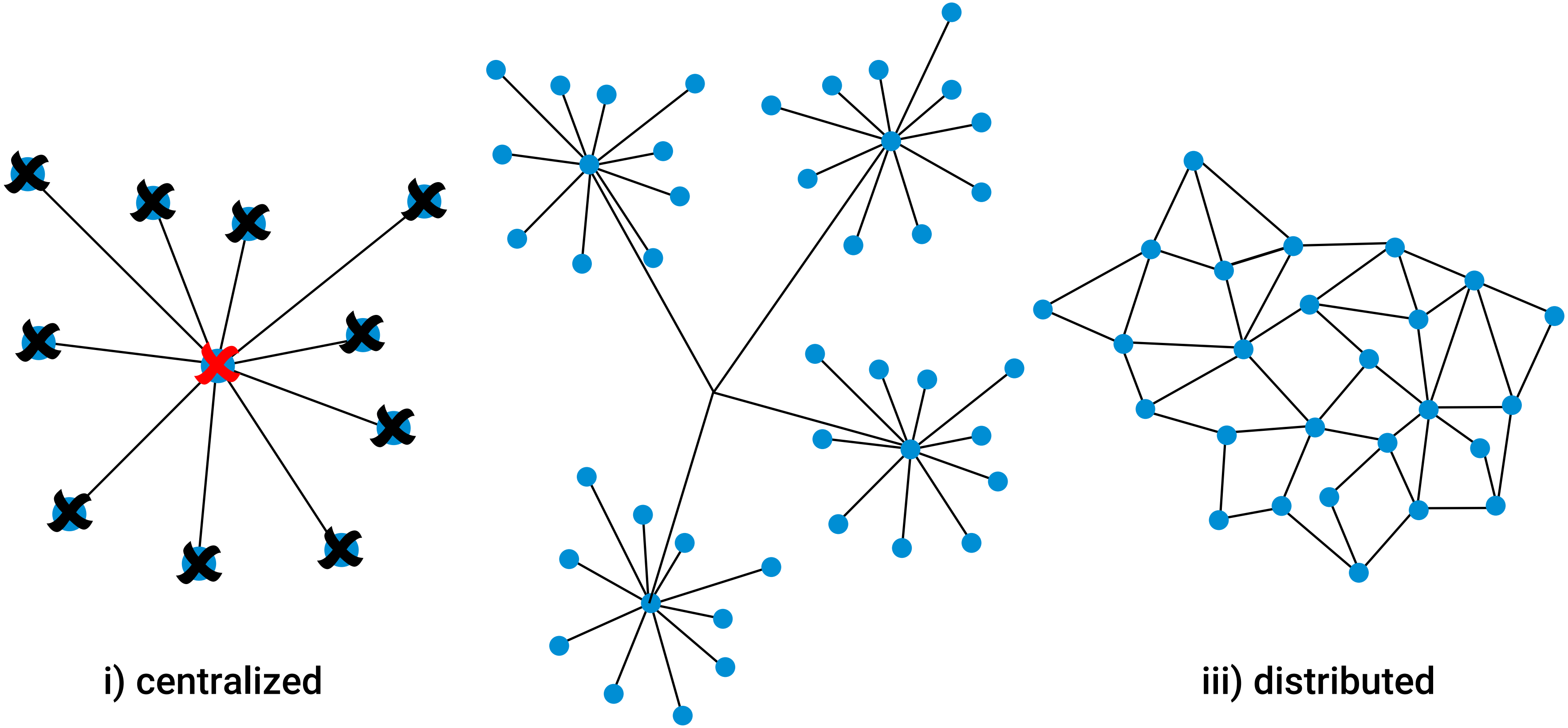


ii) decentralized



iii) distributed

NETWORK EVOLUTION

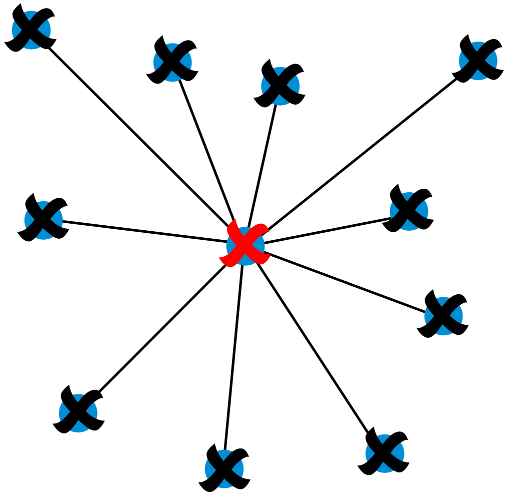


i) centralized

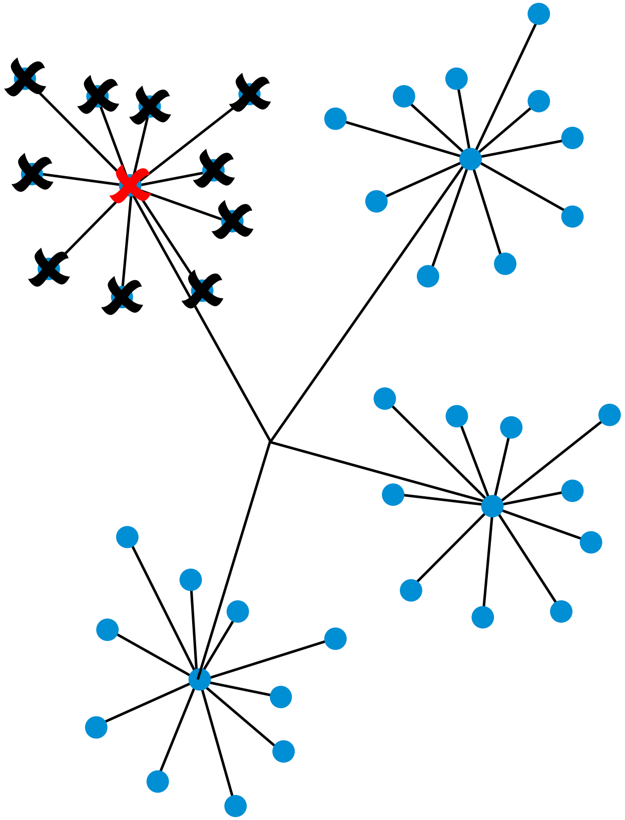
ii) decentralized

iii) distributed

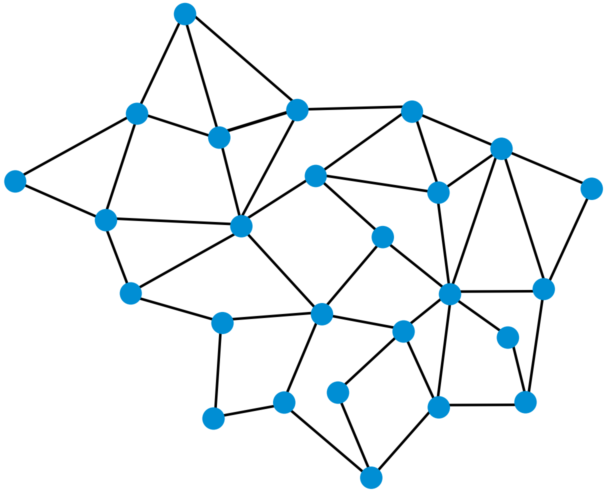
NETWORK EVOLUTION



i) centralized

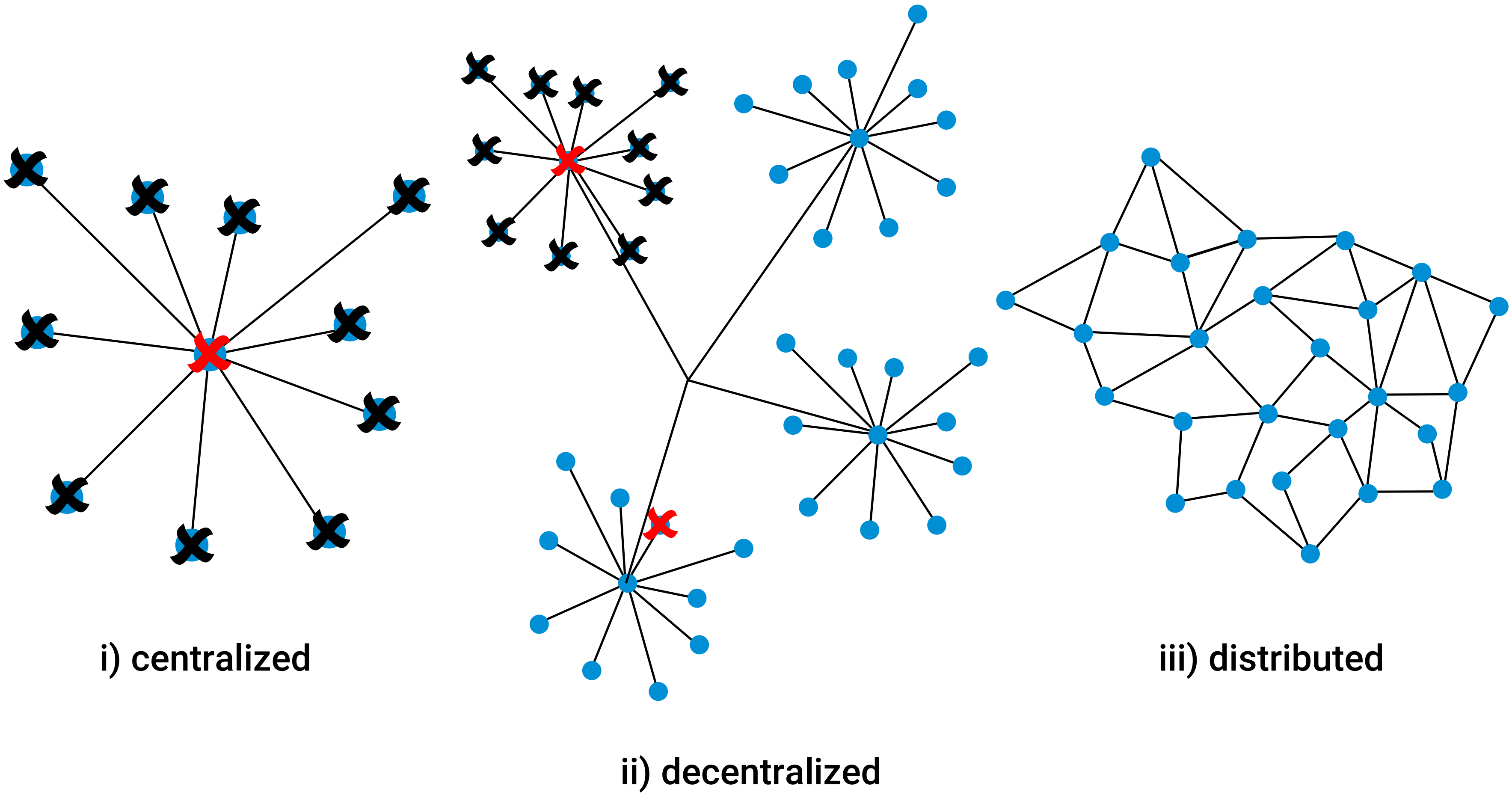


ii) decentralized

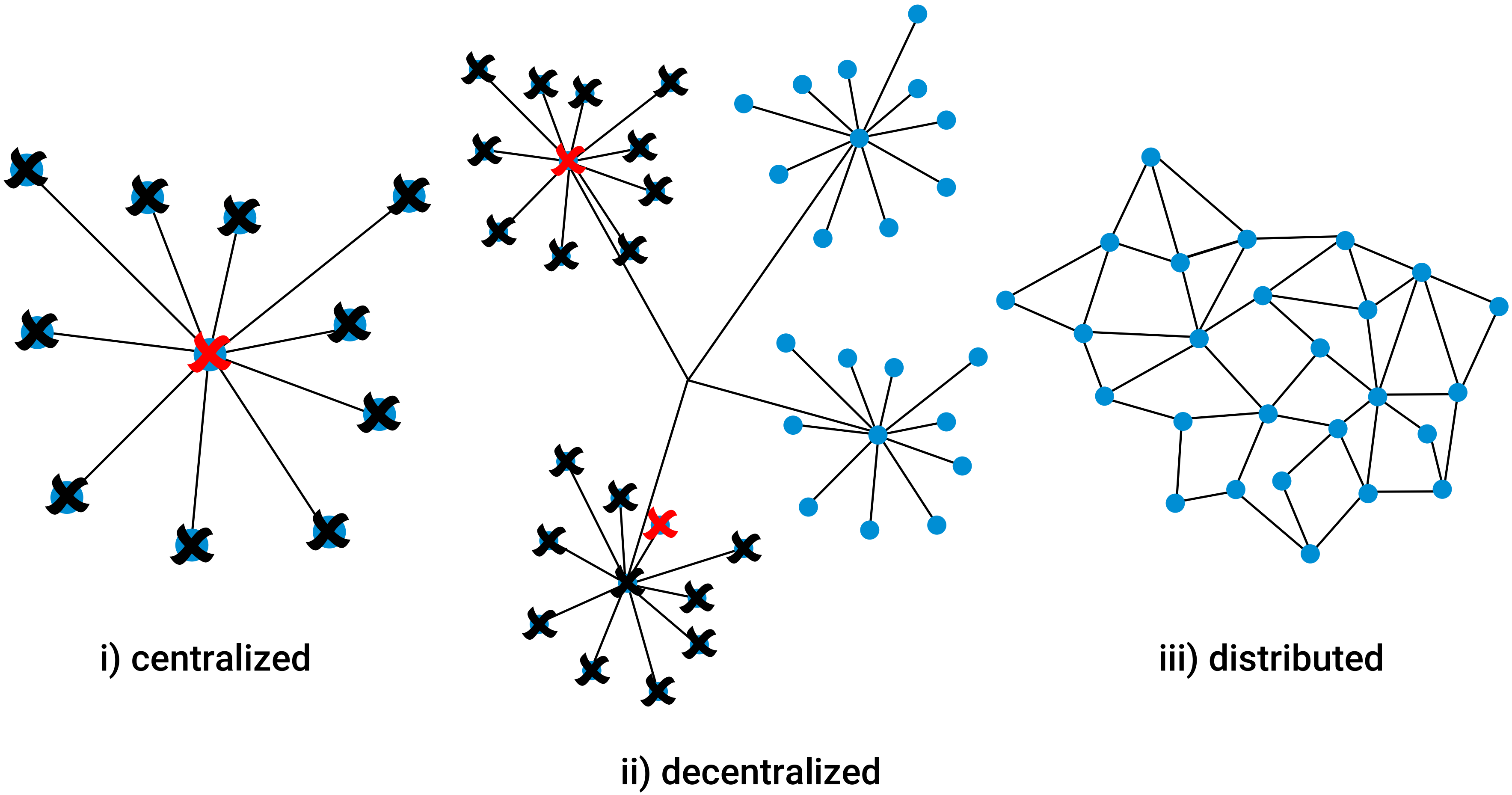


iii) distributed

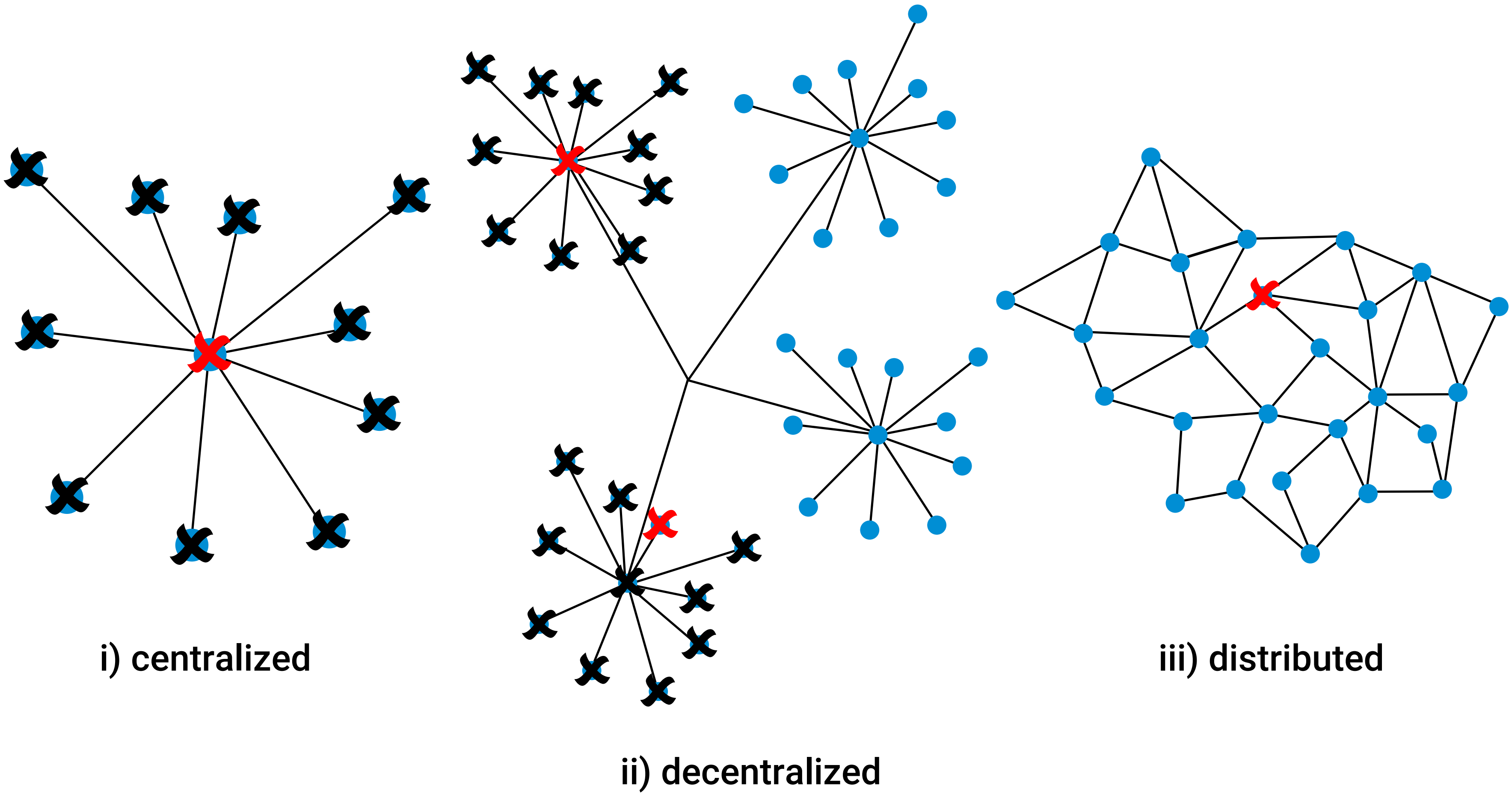
NETWORK EVOLUTION



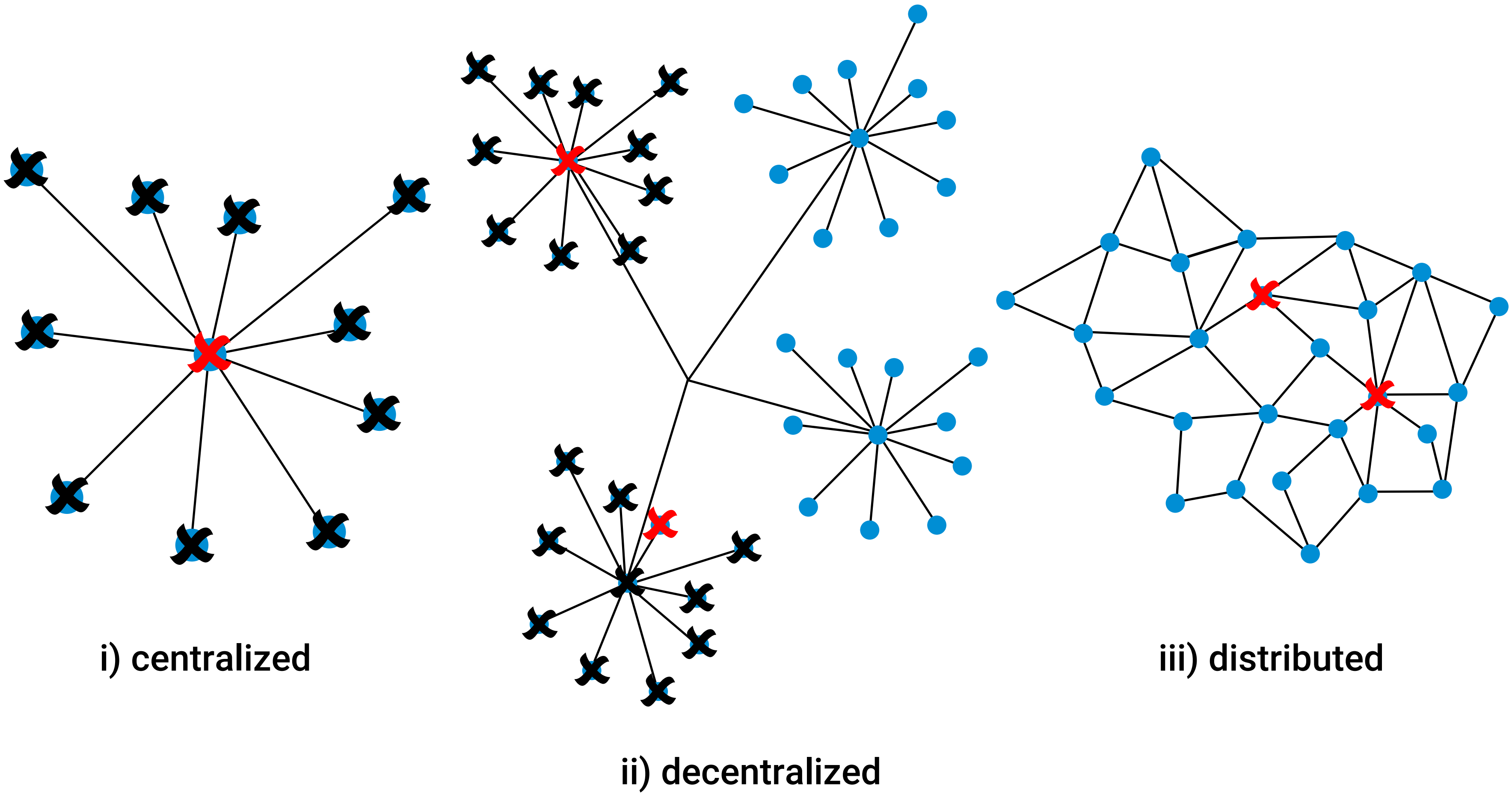
NETWORK EVOLUTION



NETWORK EVOLUTION



NETWORK EVOLUTION

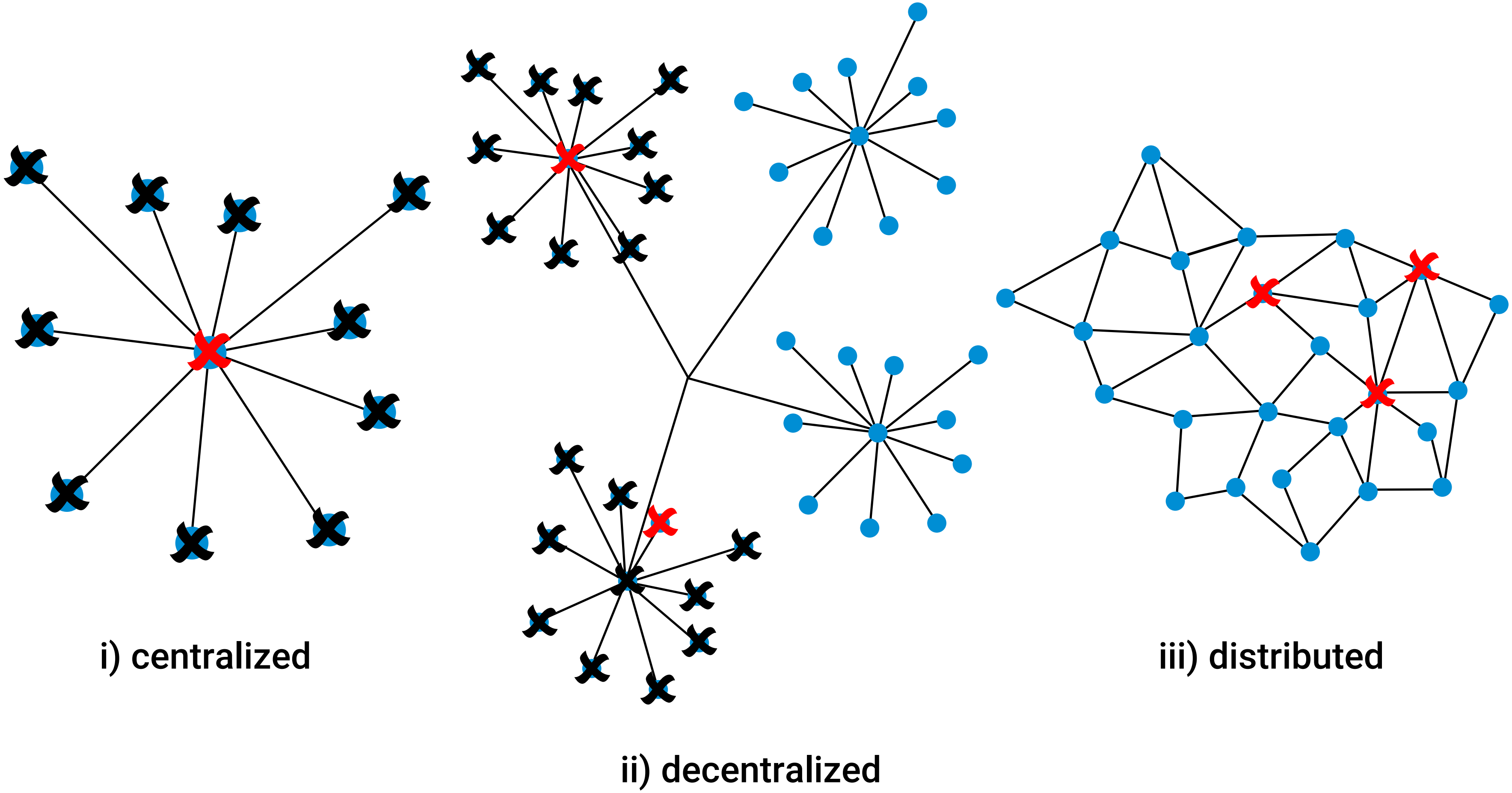


i) centralized

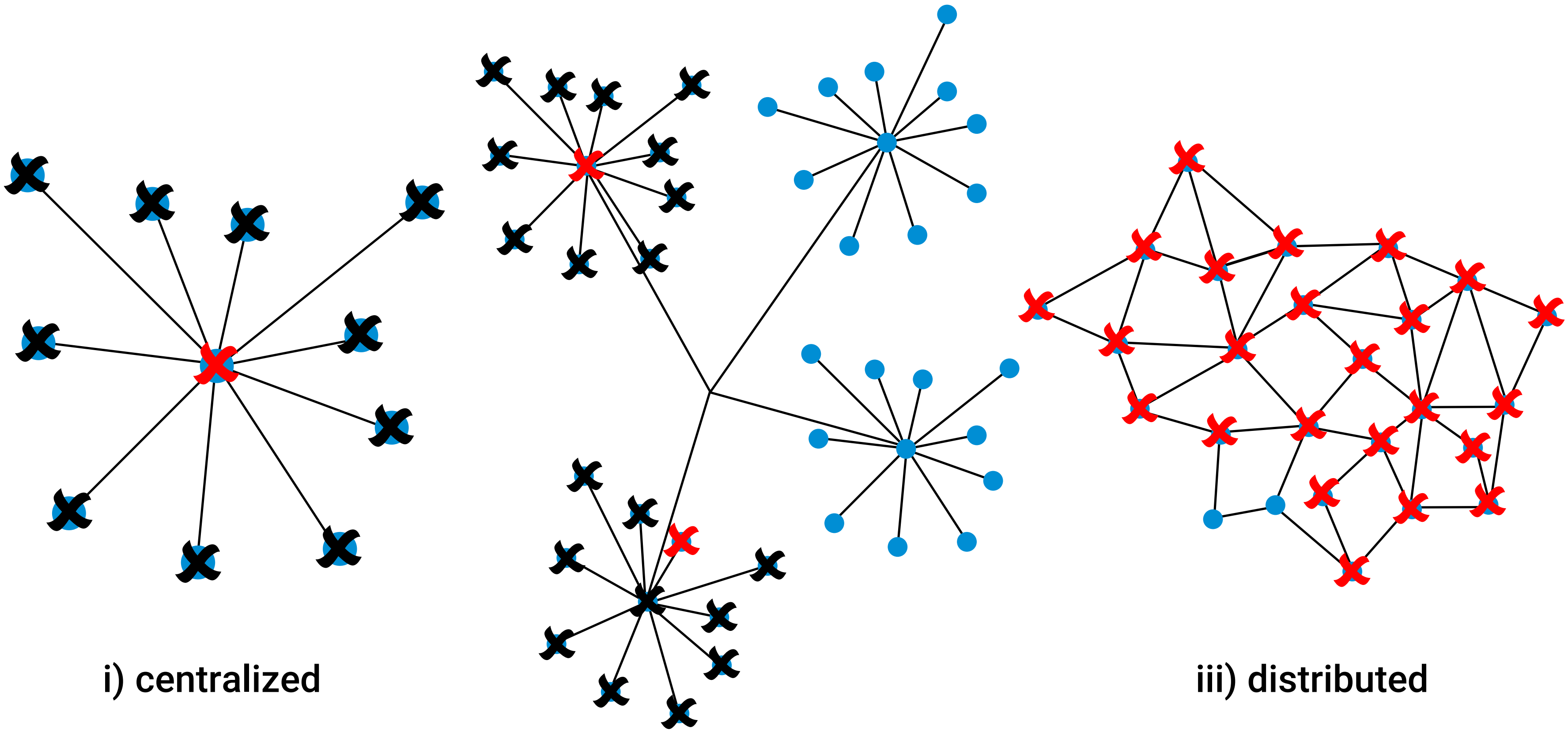
ii) decentralized

iii) distributed

NETWORK EVOLUTION



NETWORK EVOLUTION



i) centralized

ii) decentralized

iii) distributed

DISTRIBUTED NETWORKS

- **Many, equal nodes**
- **Each node has multiple connections to other nodes**
- **Very resilient to failures, attacks**
- **As long as 2 nodes are up, the network is still running**

WHO INVENTED IT?

KEY HISTORICAL DATES

- 2009 first block created
- Satoshi Nakamoto was the pseudonym used
- Early days, it was just him/her/them/it
- Then crypto-geeks, then early technology adopters
- Satoshi disappears December 2010 - date of last post
- Recent years have seen 'professionalism' of the ecosystem

SEEKING SATOSHI

- Not this guy! (probably)
- Not a great coder
- Not a great cryptographer
- Aware of the controversy blockchains create

SEEKING SATOSHI

- While conspiracy theories are fun, it's mostly irrelevant

- Operational design published openly
- Protocol is opensource
- Code is opensource and has mostly been re-written

IS IT MONEY?

Digital cash? Digital gold?

HAS ALL THE SAME CHARACTERISTICS

Durability	-	Safe for long term storage
Portability	-	Easy to move around and spend
Divisibility	-	So you can spend small amounts
Uniformity	-	Each unit of value is equal
Limited supply	-	To preserve value
Acceptability	-	So you can actually spend it

IS IT LEGAL TENDER?

NO!

Legal tender is defined as *"coins or banknotes that must be accepted if offered in payment of a debt."* **Fiat money** is **currency** that a government has declared to be legal tender, but it is not backed by a physical commodity.

Cryptocurrencies aren't regulated by any central bank.

SO WHAT?

Lots of things aren’t legal tender but still have value:

- **Gold**
- **Diamonds**
- **Rolex watch**
- **US$ (outside the US)**

WORLDS MOST EXPENSIVE PIZZA?

22nd May 2010 is Bitcoin Pizza day – bitcoins first real world transaction

- **Laszlo Hanyecz offered 10,000 BTC for 2 pizzas**
- **Someone in the UK phoned through the order using their credit card**
- **Then worth US ~$24**
- **Currently worth US ~$2.4m**

ECOSYSTEM DEVELOPMENTS

One of the fasting moving in tech

PARALLELS TO THE INTERNET

Blockchains today have been likened to the Internet in 90s.

- **Similar investment levels**
- **Similar excitement levels**
- **Similar visions of potential uses**

History doesn’t repeat, but it rhymes: We expect similar...

- **Similar path to maturity – people, tools, process**
- **Similar adoption curve (perhaps faster)**
- **Evolution of protocol/services built on blockchains (perhaps faster)**

PARALLELS TO THE INTERNET

Just as the internet revolutionised access to information, blockchains will do the same to multiple industrial verticals:

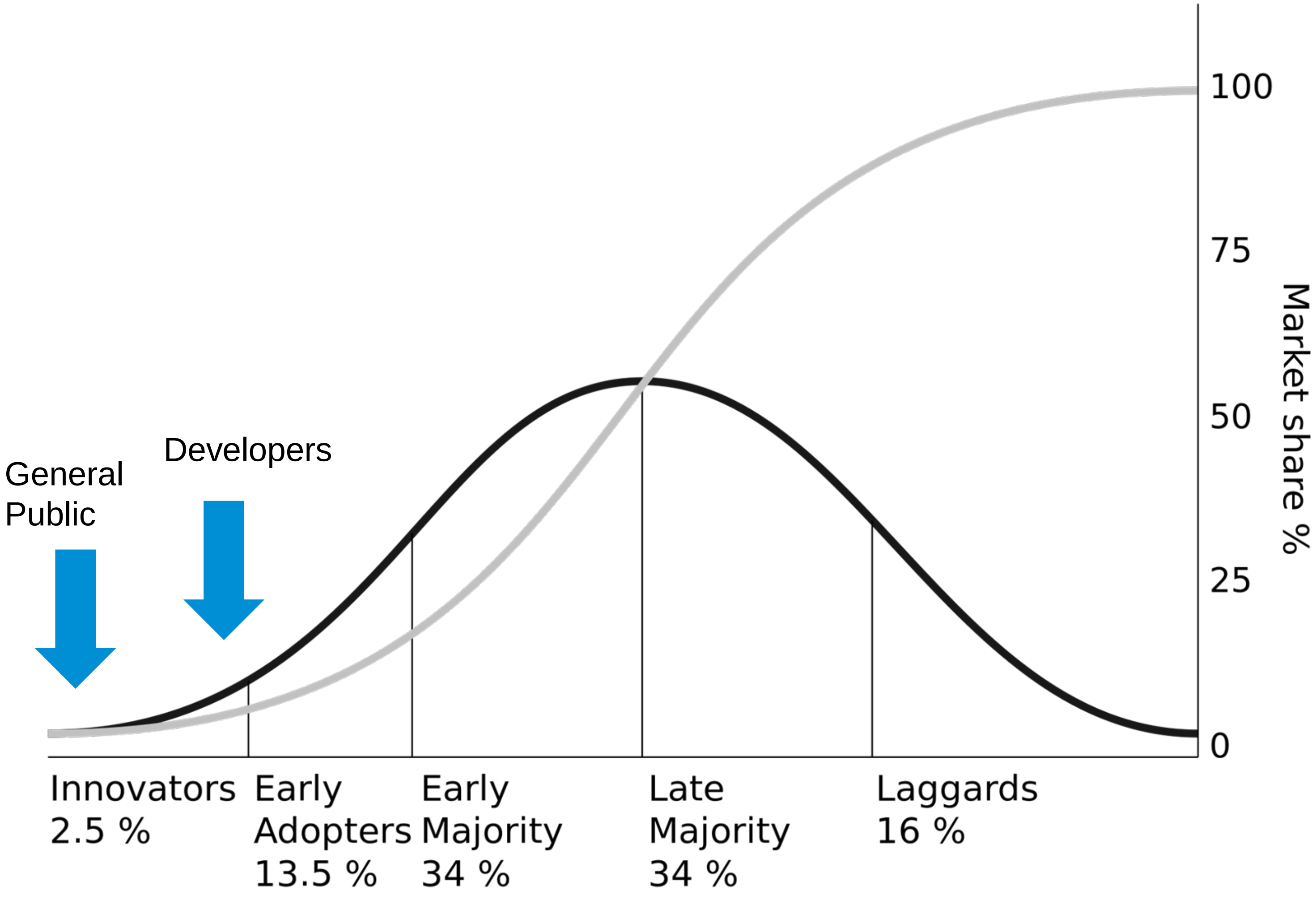
- Finance first
  - It's what blockchains were built to do
  - It's where the money is

Non finance uses

- Specialist blockchains dedicated to one task
- Generalist blockchains to be used as a 'platform‘

Brave new world/wild west – still lots of learn and build

WHERE ARE WE NOW?



INVESTMENT INTO THE SECTOR

- **Reid Hoffman (LinkedIn) Invested US$20M in Blockstream Personally**
- **Sir Richard Branson backed BitPay (Exchange) in a US$30 Million Round**
- **Circle (Exchange) raised US$50 Million - led by Goldman Sachs**
- **NYSE led a US$75 Million Investment in Coinbase (Exchange)**
- **US$1 Billion from VC funding is expected in 2015**
- **Although this is a small cross section,**
- **the importance is the names, not the numbers!**

EVOLUTION OF THE NETWORKS

1st generation networks transfer value - bitcoin, litecoin, dogecoin

Blockchain 1.5 technologies build upon existing blockchains by offering additional dependent layers and protocols allowing for unique offerings:

- **NameCoin provides distributed DNS**
- **ColoredCoin, Counterparty and Omni can tag and track digital assets**
- **FileCoin and StorJ provide distributed CDN (content delivery network) with proof of bandwidth**

EVOLUTION OF THE NETWORKS

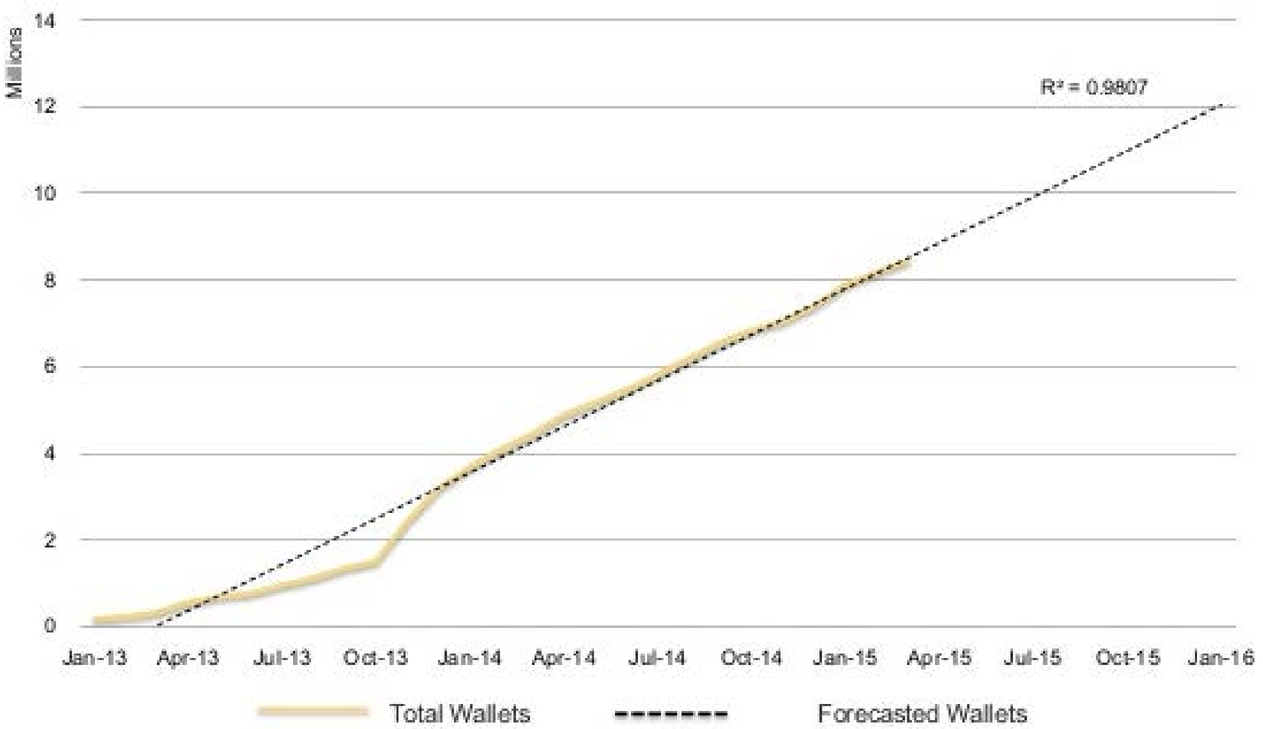
Blockchain 2.0 is currently in a mostly theoretical or pre-alpha state but involves starting from scratch and introducing turing-complete functionality

- **Ethetherum and Codius introduce autonomous applications (recently used by IBM at the core of their new IoT platform - ADEPT)**

Curated blockchains, Private access/Hybrid blockchains, entry/exit points are known & regulated

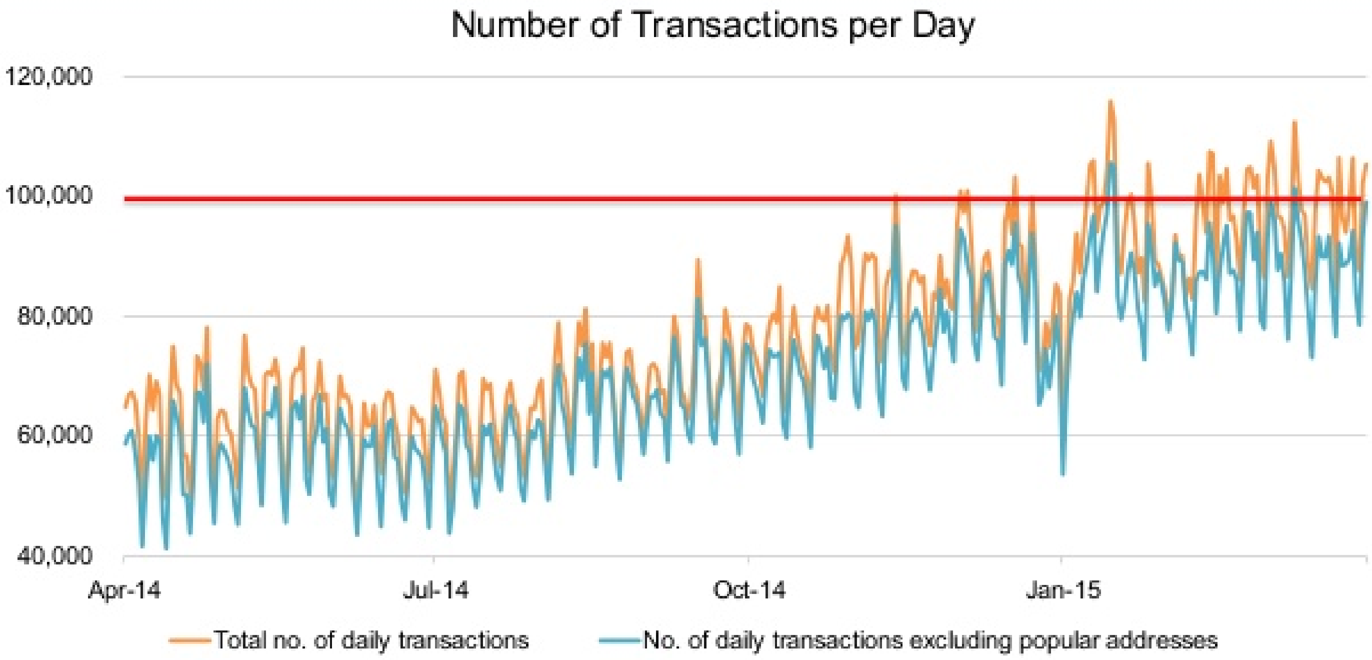
- **Ripple**
- **Tembusu**

FORECAST FOR TOTAL BITCOIN WALLETS BY END OF 2015 MAINTAINED AT 12 MILLION



Data Sources and notes: total wallets based on data from Blockchain.info, MultiBit, Coinbase, Andreas Schildbach (Android Bitcoin Wallet developer). Historical Coinbase data provided by BitcoinPulse.

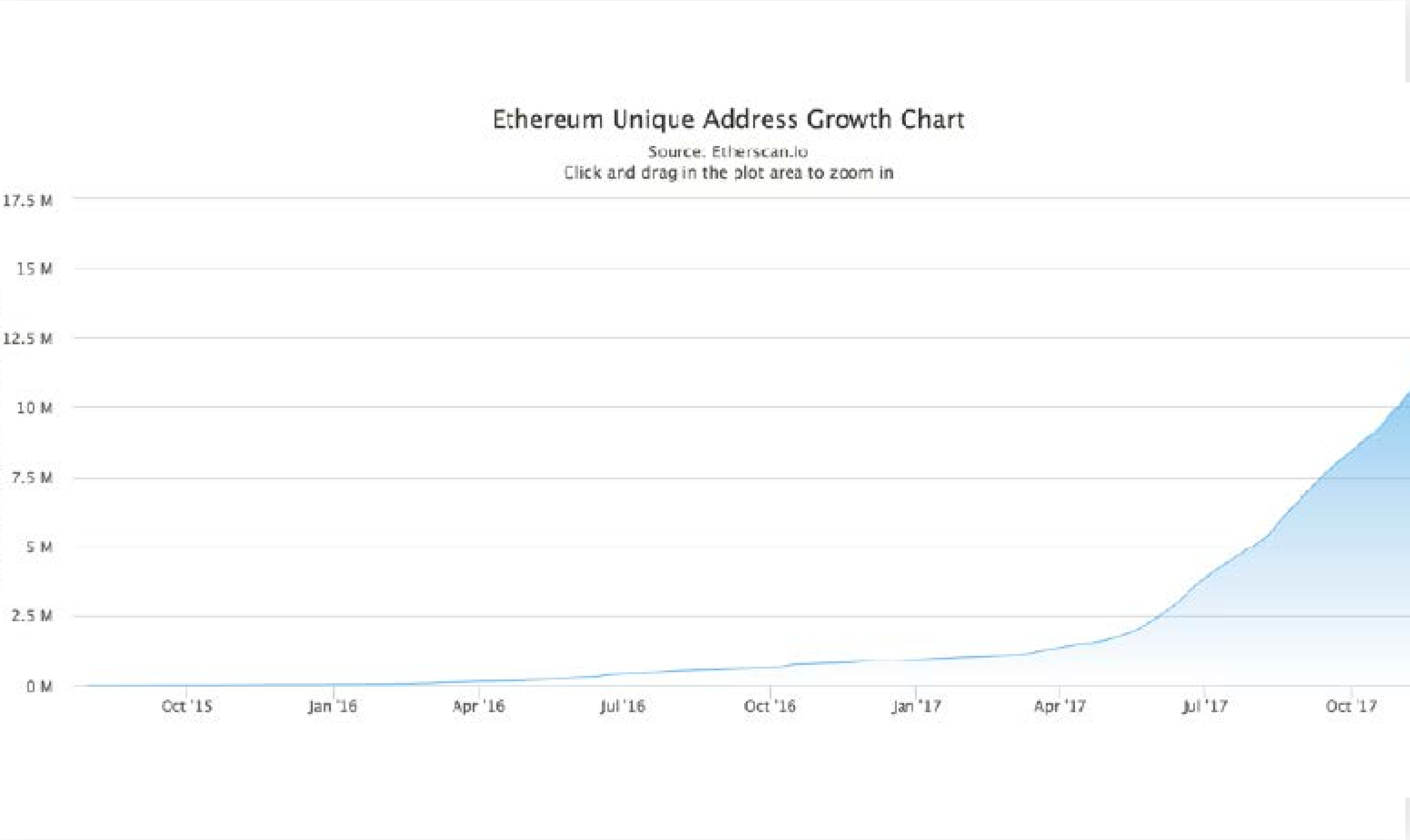
BITCOIN TRANSACTIONS HAVE BEEN RISING; AVERAGE OF 10,000 DAILY TRANSACTIONS BY POPULAR ADDRESSES*



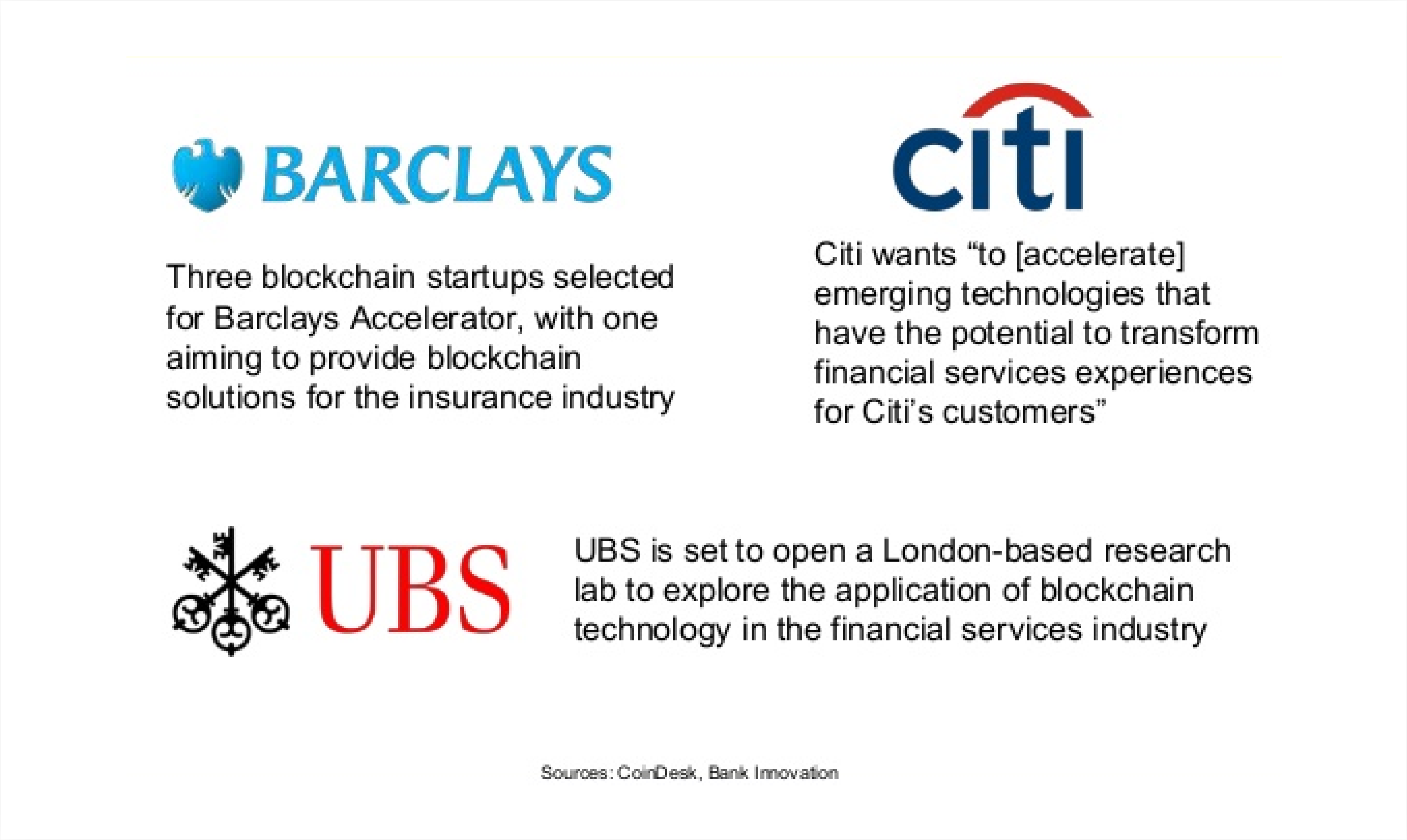
- The milestone of 100,000 daily transactions by 'addresses excluding popular ones' was reached in February, which is two months later than total transactions

Source and note: Blockchain.info, * 100 most popular addresses.

Growth in CryptoAddresses



WALL STREET INTEREST IN BITCOIN IS GROWING



BARCLAYS
citi
UBS

Three blockchain startups selected for Barclays Accelerator, with one aiming to provide blockchain solutions for the insurance industry

Citi wants "to [accelerate] emerging technologies that have the potential to transform financial services experiences for Citi's customers"

UBS is set to open a London-based research lab to explore the application of blockchain technology in the financial services industry

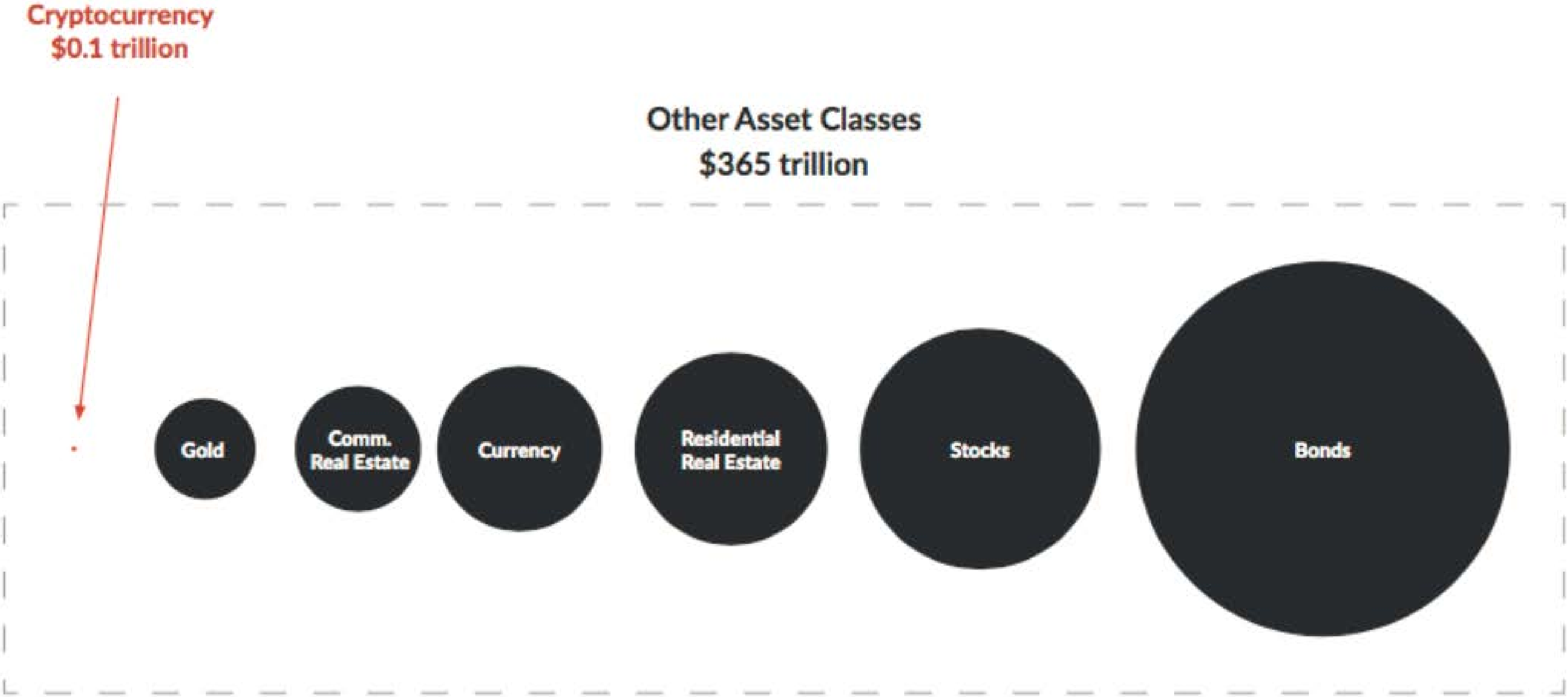
Sources: CoinDesk, Bank Innovation

BLOCKCHAIN ECONOMICS

Rethinking Economics with Computer Science Principles and Network Models

Blockchain Investing

Cryptographic Asset Class

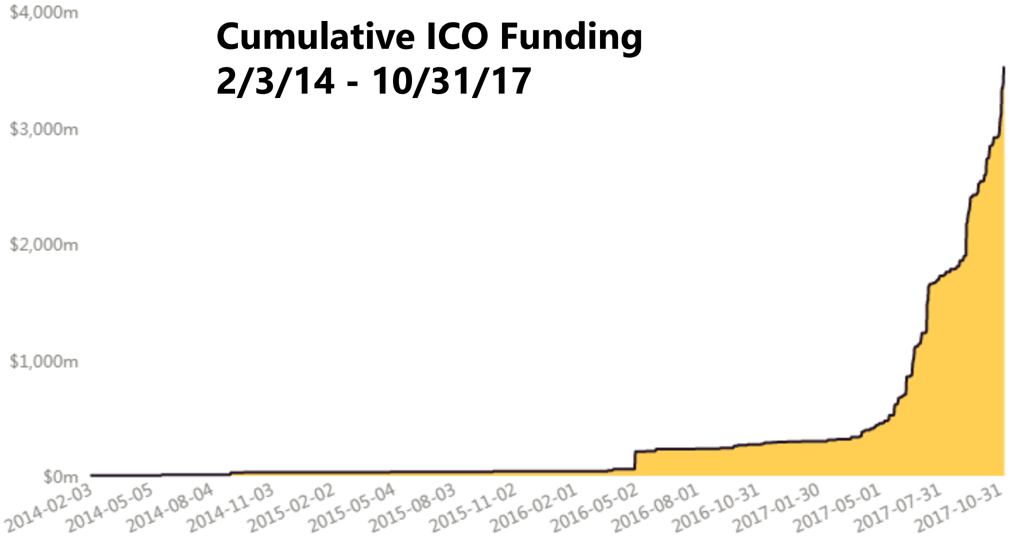


https://www.slideshare.net/SebastianCochinescu/vlad-andrei-tokens-deep-dive-presentation

ICOs = “crypto-daytrading”?

- $3.5 bn cumulative ICO funding (Coindesk)
  - ICOs surpass VC funding (PitchBook)
    - ICOs: $3.5 bn, VC funding: $2.7 bn (2/14-10/17)
- Tokens: many functions beyond fundraising
  - Voting, dividends, access, participation, notification

coindesk
ICO TRACKER



Cumulative ICO Funding
2/3/14 - 10/31/17

Source: https://www.coindesk.com/ico-tracker, https://pitchbook.com/news/reports/3q-2017-fintech-analyst-note-blockchain

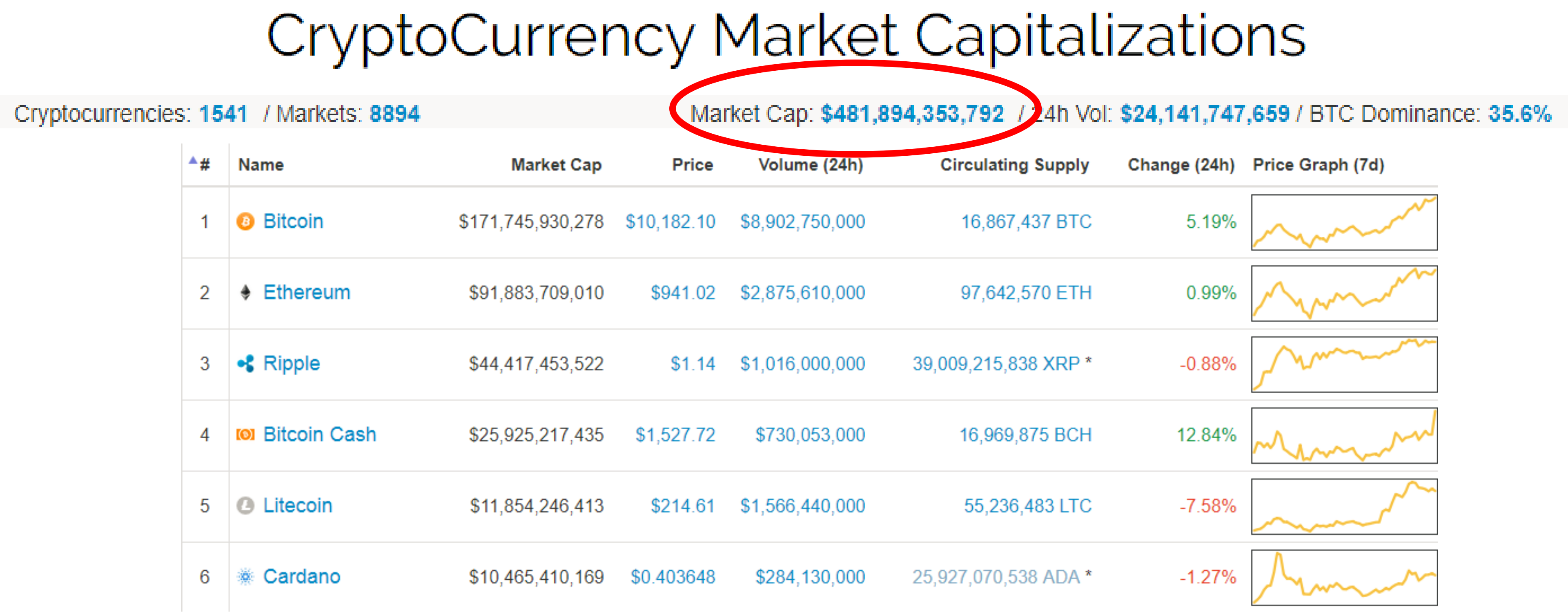
ICO Regulatory Stance

- US: investor protection; regulated (Jul 2017)
  - ICOs and exchanges; what about smart contracts?
  - ICOs vs token sales (network utility) vs crowdfunding
  - Howey Test: is it a security?
    1. Investment of money
    2. Expectation of profits from the investment
    3. The investment of money is in a common enterprise
    4. Any profit comes from the efforts of a promoter or third party
- International Climate
  - Singapore MAS: ICOs may be securities per Singapore's Securities and Futures Act (SFA) and the Financial Advisers Act
  - UK: caveat emptor; safer if regulated, not regulated
  - China: banned, exchanges ordered to close (Sep 2017)
  - Russia: regulation expected by end 2017 (Sep 2017)
  - Reg Arb: Gibraltar DLT Regulated Entities (2018e)

Source: https://www.coindesk.com/ico-tracker, https://www.coindesk.com/china-outlaws-icos-financial-regulators-order-halt-token-trading/

Cryptocurrency Market Capitalizations (2/18)

- S&P 500: $22.2 tn; US GDP $18.8 tn
- Crypto market cap: $481 bn (≃ top 50th of 200 countries)



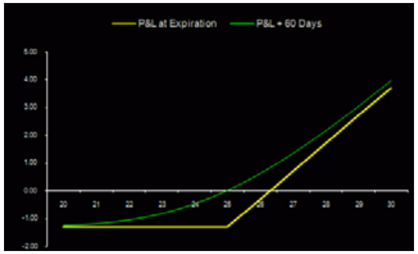
CryptoCurrency Market Capitalizations

Cryptocurrencies: **1541** / Markets: **8894** Market Cap: **$481,894,353,792** / 24h Vol: **$24,141,747,659** / BTC Dominance: **35.6%**

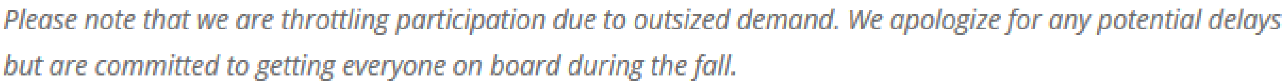
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$171,745,930,278	$10,182.10	$8,902,750,000	16,867,437 BTC	5.19%	
2	Ethereum	$91,883,709,010	$941.02	$2,875,610,000	97,642,570 ETH	0.99%	
3	Ripple	$44,417,453,522	$1.14	$1,016,000,000	39,009,215,838 XRP *	-0.88%	
4	Bitcoin Cash	$25,925,217,435	$1,527.72	$730,053,000	16,969,875 BCH	12.84%	
5	Litecoin	$11,854,246,413	$214.61	$1,566,440,000	55,236,483 LTC	-7.58%	
6	Cardano	$10,465,410,169	$0.403648	$284,130,000	25,927,070,538 ADA *	-1.27%	

Regulated Futures & Options

1. LedgerX Options
   - Cleared $1m (week 1), $2m (week 2)
   - NY-based CFTC-regulated Swap Execution Facility (SEF) and Derivatives Clearing Organization (DCO)
   - Swap execution facility, clearing Bitcoin options
   - Sep 2017 began providing physically-settled put and call options and day-ahead swaps trading
     - Private trading for large customers



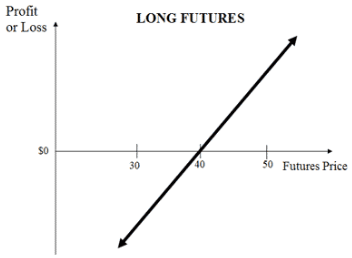
LedgerX



Please note that we are throttling participation due to outsized demand. We apologize for any potential delays but are committed to getting everyone on board during the fall.

Regulated Futures & Options

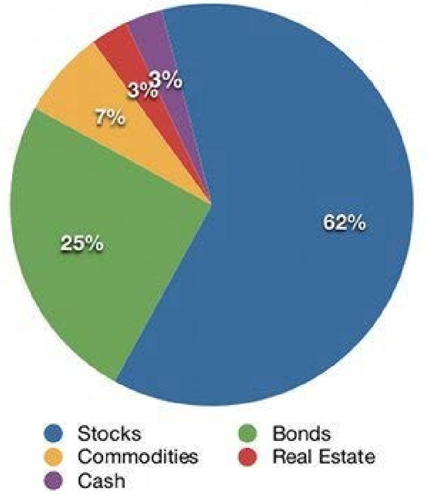
2. CBOE Bitcoin futures contracts – 12/10/17
   - Cash-settled, pending CFTC review
   - Settlement based on Gemini Trust data
3. CME Bitcoin futures contracts – 12/18/17
   - Cash-settled
   - Settlement based on CME CF Bitcoin Reference Rate (BRR), launched in November 2016 with London-based Crypto Facilities trading platform



- Significance: cryptocurrency exposure in an institutional product, demand could be large

Institutional Markets

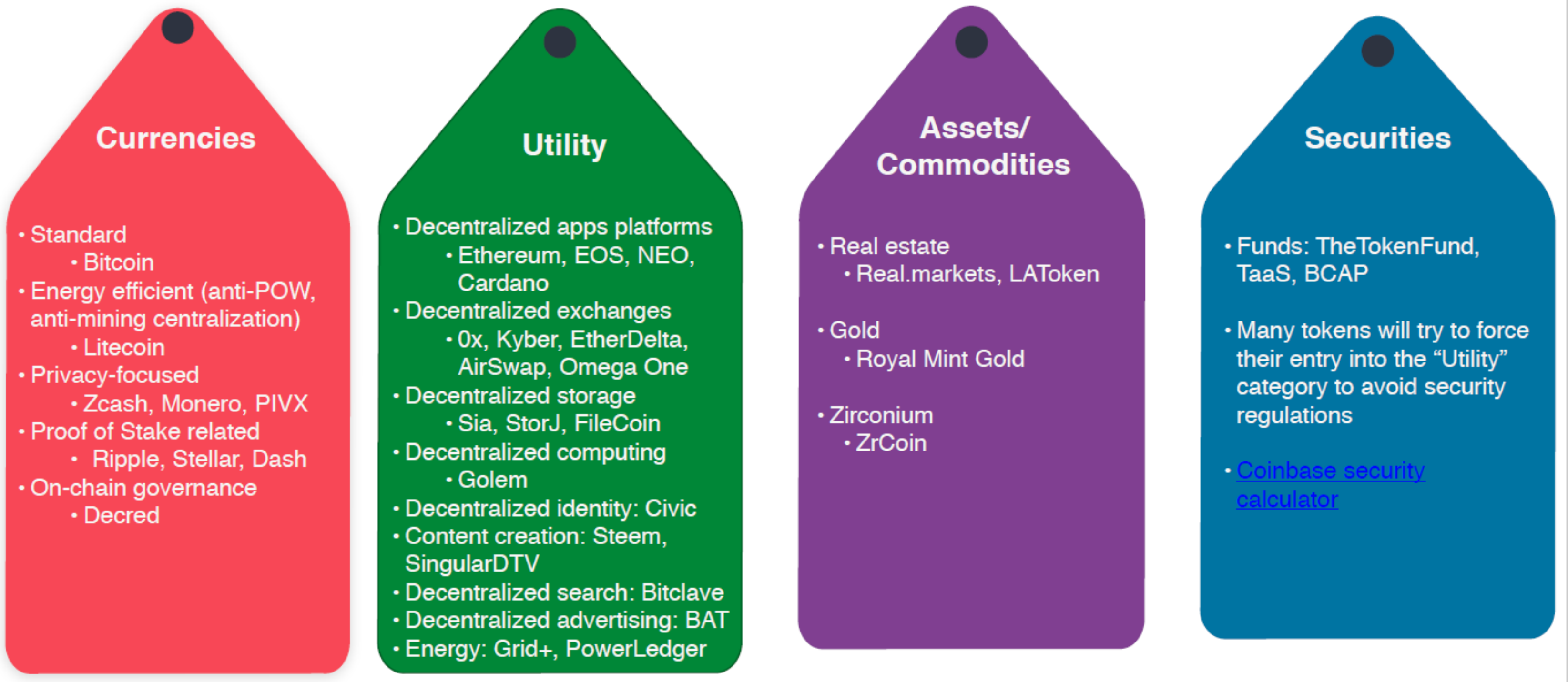
- Exposure to cryptographic assets
  - Asset class current value: $200 billion
  - Estimated value in 10 years: $2 trillion
- Demand for regulated products
  - Dark pools (institutional exchanges for Contracts-for-Difference, private trading, block trades; $20m+)
    - Genesis Trading, Cumberland Mining, Circle, Gemini Exchange, Project Omni
  - Regulated Futures and Options
    - LedgerX, CME, CBOE
  - Regulated ICOs



Asset Tokenization

Tokenization: process of turning an asset, right, or digital good into an interchangeable unit to power an ecosystem

Token: a more complicated and feature-rich form of money



Currencies

- Standard
  - Bitcoin
- Energy efficient (anti-POW, anti-mining centralization)
  - Litecoin
- Privacy-focused
  - Zcash, Monero, PIVX
- Proof of Stake related
  - Ripple, Stellar, Dash
- On-chain governance
  - Decred

Utility

- Decentralized apps platforms
  - Ethereum, EOS, NEO, Cardano
- Decentralized exchanges
  - 0x, Kyber, EtherDelta, AirSwap, Omega One
- Decentralized storage
  - Sia, StorJ, FileCoin
- Decentralized computing
  - Golem
- Decentralized identity: Civic
- Content creation: Steem, SingularDTV
- Decentralized search: Bitclave
- Decentralized advertising: BAT
- Energy: Grid+, PowerLedger

Assets/ Commodities

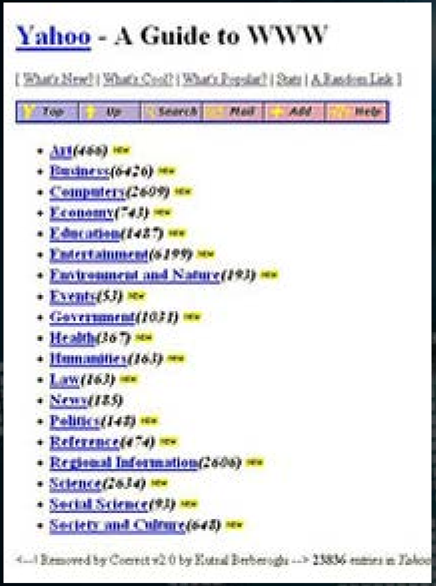
- Real estate
  - Real.markets, LAToken
- Gold
  - Royal Mint Gold
- Zirconium
  - ZrCoin

Securities

- Funds: TheTokenFund, TaaS, BCAP
- Many tokens will try to force their entry into the “Utility” category to avoid security regulations
- Coinbase security calculator

https://www.slideshare.net/SebastianCochinescu/vlad-andrei-tokens-deep-dive-presentation

information internet: static information



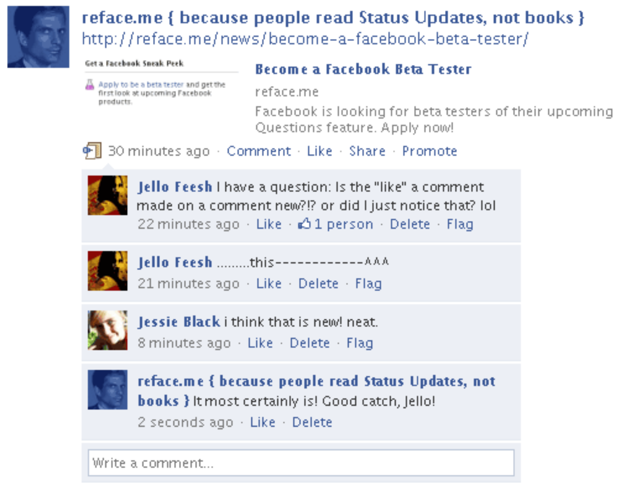
Yahoo - A Guide to WWW

[What's New? | What's Cool? | What's Popular? | Stats | A Random Link]

- Art(466) new
- Business(6426) new
- Computers(2609) new
- Economy(743) new
- Education(1487) new
- Entertainment(6199) new
- Environment and Nature(193) new
- Events(53) new
- Government(1031) new
- Health(367) new
- Humanities(163) new
- Law(163) new
- News(185)
- Politics(148) new
- Reference(474) new
- Regional Information(2606) new
- Science(2634) new
- Social Science(93) new
- Society and Culture(648) new

<--! Removed by Correct v2.0 by Kutnal Berberoglu --> 23836 entries in Yahoo

social internet: engage with content



reface.me { because people read Status Updates, not books }
http://reface.me/news/become-a-facebook-beta-tester/

Get a Facebook Sneak Peek

Apply to be a beta tester and get the first look at upcoming Facebook products.

Become a Facebook Beta Tester

reface.me

Facebook is looking for beta testers of their upcoming Questions feature. Apply now!

30 minutes ago · Comment · Like · Share · Promote

Jello Feesh I have a question: Is the "like" a comment made on a comment new?!? or did I just notice that? lol
22 minutes ago · Like · 1 person · Delete · Flag

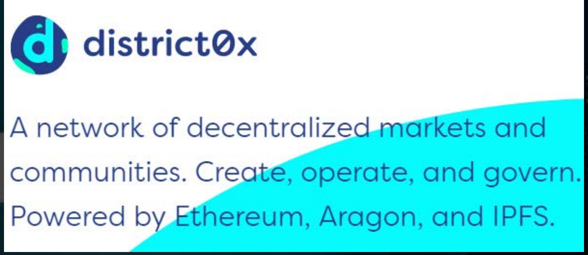
Jello Feesh ....this-------------AAA
21 minutes ago · Like · Delete · Flag

Jessie Black i think that is new! neat.
8 minutes ago · Like · Delete · Flag

reface.me { because people read Status Updates, not books } It most certainly is! Good catch, Jello!
2 seconds ago · Like · Delete

Write a comment...

token internet: participate in the community economy



district0x

A network of decentralized markets and communities. Create, operate, and govern. Powered by Ethereum, Aragon, and IPFS.

2018
VOTE
VOTE FOR THE NEXT DISTRICTS
CREATE, OPERATE, & GOVERN
Vote For the Next Districts

participation

TECHNOLOGY SUMMARY

Building blocks

SOME BUILDING BLOCKS

- Blockchain terminology
- Hash functions
- Merkle trees
- Encoding schemes
- Public/Private key crypto
- Digital Signatures

TERMINOLOGY

- **Address: The 'account number' of the person you are sending coins to. Can be used just once or multiple times. You can have many addresses**
- **Transaction: The transfer of value/coins from one address to another address**
- **Block/Blockchain: The record of transactions**
- **Wallet: Software that manages your addresses and keeps track of transactions and balances**

HASHING FUNCTIONS

‘A hash function is any function that can be used to map digital data of arbitrary size to digital data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or hashes.’

There are many types, but Bitcoin uses SHA256; output is 256bits of data, or 64 hexadecimal characters

HASHING PROPERTIES

- **Any size of data always results in the same length hash**

- **Slight changes of input data gives totally different hashes**
  - **‘Hello World’ = a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e**
  - **‘Hello World!’ = 7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d9069**

- **The same input always produces the same output**

- **Hashes are ‘one way’**

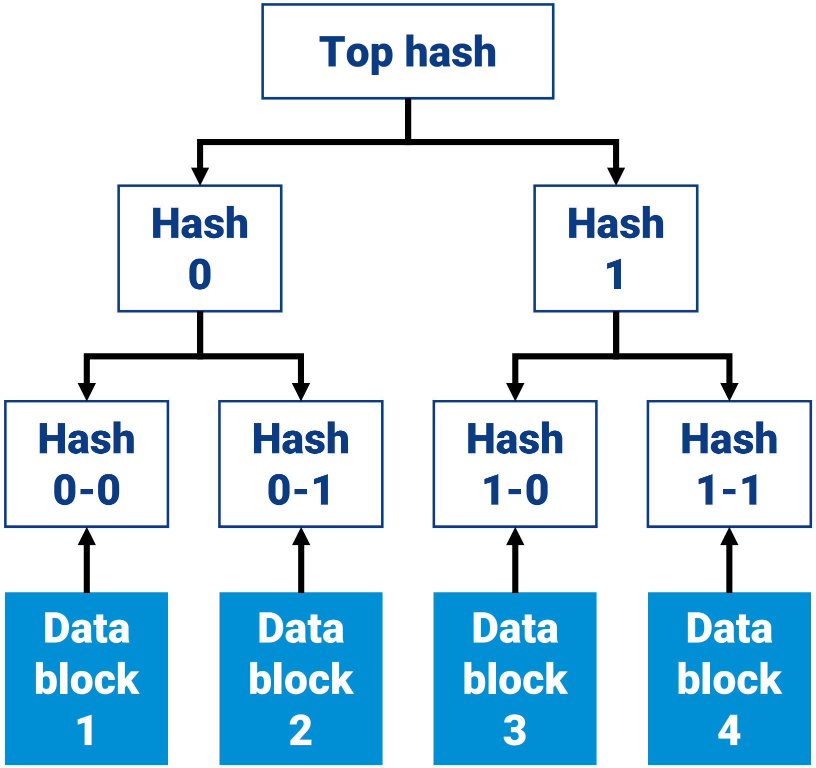
HASHING USAGES

- To record a value while hiding the original value (e.g. a password)
- To verify the integrity of some data (store the hash, to check the data, hash it again and compare the values; should be the same hash value)
- To prove you've done calculations (generating hashes takes computing power)

MERKLE TREE - HASH OF HASHES

- **Multiple blocks of data, in a certain order, into a single hash**

- **Allows you to work out which block has changed**



A BLOCKCHAIN IS AN IMPLEMENTATION OF A LEDGER

- **Take some data, encode it for a specific purpose (e.g. easier to transmit, easier to read, easier to convert between formats)**

- **Two way, you can encode and decode and end up with the same data**

- **Bitcoin uses base 58 - easier to read
(misses out 0 I O l as they all look like zeros and ones)**

‘1234567890’ = 2t6V2H

PUBLIC/PRIVATE KEY CRYPTO

- **2 uniquely related cryptographic keys**
- **Data encrypted with the public key can only decrypted with the private one (and vice versa)**
- **The maths behind it is very complex**
- **Main aim is confidentiality (in messaging)**
- **Also used for digital signatures (the bit we're interested in)**

DIGITAL SIGNATURES

- **Verify the messages came from the correct person**
- **Verify the messages hasn’t been changed or tampered with**
- **Can be used to prove that you have the private key**
- **Main aim is confidence in identity (in messaging)**

WAYS TO DEVELOP

Nodes vs APIs

FUNCTIONAL CATEGORIES

Getting blockchain data:

- **Blocks**
- **Transactions**
- **Sending Transactions (known as relaying)**

Cryptocurrency functions:

- **Generating Private/Public keys, Hashing, Address Encoding etc**
- **Creating transactions**
- **Signing transactions**
- **Support functions**

OPTIONS

Run your own node:

- No dependencies on external service
- Lots of RPC functions you can use to
- No data on addresses you don’t control (apart from BTC)
- No metadata
- Uptime challenge – more chains = more nodes

API:

- Several available
- Address tracking & metadata available
- Advanced functions like multi-sig/exchange functions
- External dependency

HYBRID APPROACH

Run your own node for experimentation

- Start on the testnet
- Send initial transactions to seed your application
- Watch how the transaction/data is represented through the API of your choice
- Simulate external users

API

- Used by your main application/server/scripts

Framework used for cryptocurrency functions

- This stuff is hard, no need to reinvent the wheel

USE CASES

- Background checks: education credentials, criminal records
- Secure document storage: home deed, auto title
- Birth registries
- Land registries
- Financial services: securities clearing, syndicated loans
- Global supply chain: automotive recalls and counterfeit airbags
- Healthcare: EMRs, insurance claims, genome research
- Airlines: registration, re-booking, vouchers, loyalty
- Tokenized economy: Tech Coworking space 1 token = 1 seat
- Payment channels: Starbucks or for bandwidth consumption

Questions?

THANK YOU

●●●