Blockchain, Future of the Web

KORBIT

김진화 | louis@korbit.co.kr

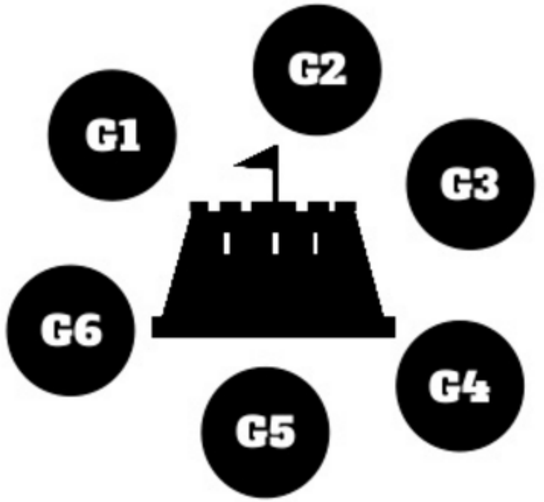
FIN-TECH

what is the difference between

FIN-TECH & e-Finance

Byzantine General Problem

- Byzantium very rich!
- greedy neighbours
- Neighbours wish to invade Byzantium
- non strong enough by itself
- Generals can send unlimited messengers
- Generals can not trust any other general
- How to agree on an attack strategy?

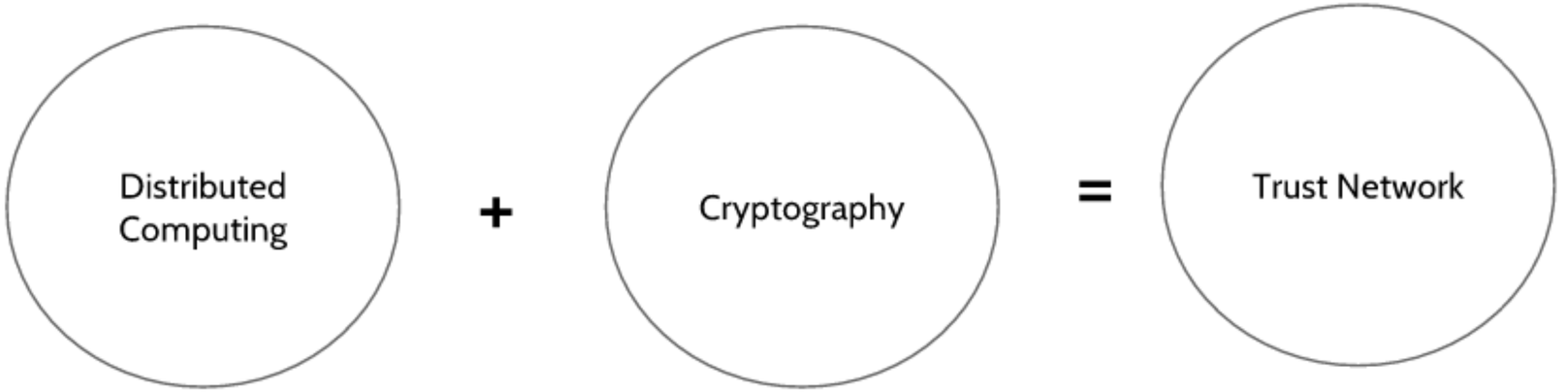


Consensus

Leslie Lamport
Distributed Computing

- Satoshi Nakamoto
  - "Bitcoin: A Peer-to-Peer Electronic Cash System"
    - "Proof of Work"
      - Byzantine General Problem
    - Bitcoin has been running more than 7 years.
      - Attacks from all the fields.
    - He proves it.
  - The creator of "Trust Network"

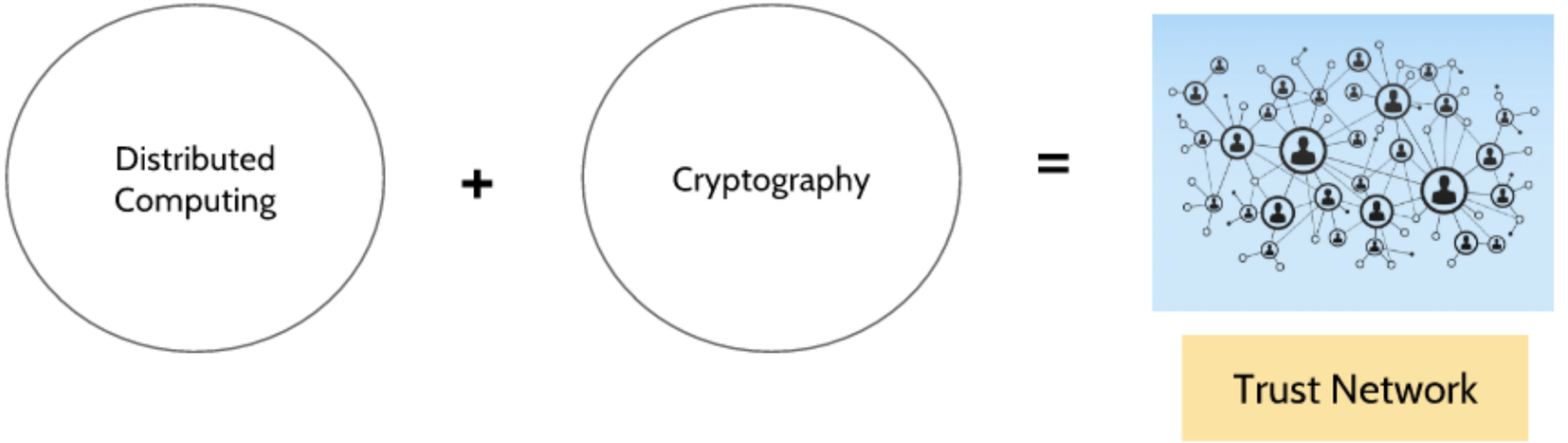
Satoshi Nakamoto



- Bitcoin (Blockchain)
  - "This is **the distributed trust network**

    ... that the Internet always needed and never had."

Marc Andreessen



❑ Byzantine General Problem

1985
"Impossibility of Distributed Consensus with One Faulty Process"

1989
Paxos Consensus Algorithm
(Peer-to-Peer model)
- Leslie Lamport

1995
The Internet

2000
Bittorrent

Oct. 2008
"Bitcoin: A Peer-to-peer electronic cash system"
- Satoshi Nakamoto

2009
Google App Engine
Master/Slave model

2010
Bitcoin

2011
Google App Engine
High Availability Model
(Paxos Consensus Algorithm)

2015
ethereum

Vitalik Buterin

Until Bitcoin, May 2008
- Synchronous Consensus Model: YES
- Asynchronous Consensus Model: NO

The Good side

Google
amazon
facebook

The Evil
(The Darkside)

Microsoft
IBM

2016 The Blockchain Ecosystem

Market Insight • Proposition Development • Customer Engagement • Product Launch

FirstPartner

Introduction

The blockchain combines cryptography & distributed computing to deliver secure, direct peer to peer transactions without the need for a central party. At its heart is the Distributed Ledger. This is a tamper proof, public, network-hosted, record of all consensus verifiedtransactions.

Initially realised via Bitcoin & similar "cryptocurrencies", focus & investment is now shifting to the potential of blockchain technology to revolutionise the infrastructure & processes of established Financial Institutions & other enterprises.

This Map summarises the key principles behind the blockchain & the emerging ecosystem addressing payments, banking & other potential use cases.

Blockchain numbers

$921million Cumulative VC investment in Bitcoin & blockchain companies to Oct 2015. $462 million of this in 2015 alone. [1]

$121million Largest cumulative funding total - raised by Bitcoin computer developer 21inc. [1]

805 Number of early stage Bitcoin & blockchain companies identified by Venture Scanner [2]

30+ Banks & Financial Institutions known to be testing, analysing or investing in the blockchain technologies [3]

11m Number of registered Bitcoin wallets in Sept 2015 - up from 6.6m in Sept 2014 [4]

106,000 Number of merchants who accept Bitcoin [4]

$4.9bn Bitcoin capitalisation Nov 2015. Bitcoin accounts for around 90% of the capital value of all cryptocurrencies [5]

$2.7bn value of Bitcoin trading in Sept 2015 [6]

475 Bitcoin ATMs installed worldwide [7]

Sources:
1 CoinDesk & Crunchbase
2 Venturescanner.com reviewed Nov 2015
3 FirstPartner research
4 CoinDesk State of Bitcoin Report Q3 2015
5 Blockchain.info checked 16th Nov 2015
6 Bitcoinity.org
7 Coin ATM Radar checked Oct 2015

Author | Richard Warren
rwarren@firstpartner.net

Like what you see?
Contact us for in-depth insight into your target markets!

Contacts | hello@firstpartner.net
+44 (0) 870 874 8700
@firstpartner
www.firstpartner.net

Payment Use Cases

Retailing | Person 2 Person | Remittances | Financial Inclusion | Interbank Clearing | Forex | Resilience | Trading & Markets

The Cryptocurrency Ecosystem

Specialist companies facilitating transaction validation, currency exchange, storage & payment on existing cryptocurrency newtworks (primarily Bitcoin)

Users

Wallets: Blockchain, Xapo, Armory, bitreserve, case

Bitcoin Debit Cards: WageCan, ANXPRO

BitCoin ATM: LAMASSU, genesiscoin, BITACCESS

International Remittance: ABRA, BitPesa, R3BIT

Merchants

Merchant Payment Processing: Bitcoin PoS (PEY, DC POS)

Bitcoin Processing: Bitnet, GOCOIN, bitpay

Risk & Fraud Management: vogogo

PSPs Supporting Bitcoin: PayPal, adyen, Braintree, stripe

Exchanges: Bitfinex, kraken, LocalBitcoins.com, BITSTAMP, HUOBI.com, BTC

Multiservice Companies (Mining, Exchange, Wallet, Processing): coinbase, CIRCLE, BITX, BTCC, PAYMIUM

Mining

Mining Technology & Commercial Operations: 21 INC, KnCMiner, BitFury, spondooliestech, HASHRABBIT, BTCS

Mining Pools: - Ghash.io, - F2Pool, - AntPool, - Slush'spool

Established Financial Ecosystem

Regulated financial instutions & platform vendors exploring blockchain technology as an alternative to centralised & correspondent payment processing

Money Transfer Operators: Western Union

Market Makers

Securities Markets: Nasdaq

Retail & Commercial Banks: Barclays, Deutsche Bank, Bank of America, BNP Paribas, fidor BANK, BBVA, citi, HSBC, ING, J.P.Morgan, UBS, RBS, Santander

Central Banks & Initiatives

Liquidity Provision | National Clearing | Compliance | Policy

The following major central banks have undertaken assesments or issued statements on regulation, potential risks to financial systems and/or benefits but none yet has a definitive policy stance.

- Bank of England
- Banque de France
- Deutsche Bundesbank
- European Central Bank
- The Federal Reserve
- Monetary Authority of Singapore
- People's Bank of China
- Reserve Bank of India

Card Schemes: VISA, MasterCard, American Express

Interbank Networks: SWIFT, earthport

Enabling the Financial Services Blockchain

Commercial platforms & services targeting Financial Institutions

Securities & Derivatives & Asset Trading Platforms: Smart contracts & blockchain for transparent trading & post trade settlement — Mirror, symbiont, clearmatics, HEDGY, SETL

The R3 Consortium: Technology led initiative of 30+ banks to design & apply distributed ledger technology to global financial markets

Institutional Investment: TradeBlock, itBit, SolidX

Financial Infrastructure & APIs: Enable implementation of private Blockchains/ sidechains &/or the development & securing of financial applications — BLOCKCYPHER, eris INDUSTRIES, Gem, ripple, Digital Asset Holdings, Chain, Blockstack.io

Bitcoin Based Cryptocurrencies

Open Protocols for Institutions

The Distributed Ledger

Anatomy of a Transaction

1 Initiation: sender — Transaction Instruction: -prior transaction(s) -recipient address -value & conditions -digital signature

2 Verification: nodes or miners: -propogate -group into "candidate blocks" -validate signatures -verify through "consensus" — the network

3 Completion: recipient — "Value" — Verified Block — Blockchain

Protocol Components

The Currency

The medium for transaction settlement within the newtork & rewarding miners. Cryptographically generated, protocol rules determine issuance & destruction. May be tradeable "off the newtork" (e.g. Bitcoin) or only exist on network (e.g. XRP)

The Ledger

AKA the Blockchain. A Public record of all transactions - stored across a distributed P2P network of servers. Verified transactions are added in "blocks" and the history provides proof of value or assets "owned".

Consensus

Prevents "double spend" or validation of fraudulent transactions:

Proof of work: miners compete to validate blocks by solving highly processor/RAM intensive cryptographic problems for reward

Distributed consensus: majority validation by trusted subnetworks of peer nodes within the network. Used by Ripple & Stellar

Proof of stake: achieves distributed consensus by network users proving their ownership of currency. Used by Peercoin & Bitshares

Blockchain — Distributed P2P Networks

Bitcoin
Created as an alternative to central bank controlled fiat currencies, Bitcoin was the first working Cryptocurrency. It remains dominant but lack of scalability and other inherent flaws will likely prevent mass adoption.
Validation: Proof of Work
Latency: 10 minutes
Currency: BTC - on and off-network
Issuance: Mining Reward. 21M Limit

Litecoin
Consensus: Proof of Work
Latency: 2.5 minutes
Currency: LTC - on and off-network
Issuance: Mining Reward. 84M Limit

Dogecoin
Consensus: Proof of Work
Latency: 1 minute
Currency: Doge - on & off-network
Issuance: Mining Reward. Unlimited

Ripple
Consensus based protocol designed specifically for existing financial institutions. Supplementing existing processes & directly supporting fiat currencies, lead use cases are international paymemts & inter Financial Institution settlement
Validation: Distributed consensus
Latency: 3 seconds
Currency: XRP on-network only
Issuance: At inception -100 BN units created.

Ethereum
Smart contract & distributed app focus
Validation: Proof of Work
Latency: 12 seconds
Currency: ETH on-network only
Issuance: Mining Reward.

Stellar
Ripple derivative. Financial focus
Validation: Distributed consensus
Latency: 2-5 seconds
Currency: Lumens on-network only
Issuance: 100 BN then 1% issued PA

Crypto 2.0 - Building on the Bockchain

Smart Contracts

Encode & validate "conditions" for a transaction between parties. Potentially facilitate legally binding transactions over the blockchain

CLEARINGHOUSE, consensys, Counterparty, CODIUS

Colored Coins & Open Assets

Bitcoins altered to represent an asset. Exchanged via the Open Assets Protocol. Allows trading of physical & other assets

coin, ChromaWay, Omni, coinprism

Core Blockchain Protocols

bitcoin, stellar, ripple, DASH, ethereum, Peercoin, VIACOIN

Enabling Layers
Protocols, platforms & SDKs that build on top of core blockchain protocols to enable additional transaction types & services

Ripple: facilitating multiple Financial Institutions focussing on payment solutions

Protocol Commercialisation
Consensys: building an Ethereum based ecosystem & partnered with Microsoft for Ethereum Blockchain as a Service

Other Use Cases

IoT — Registering and validating connected devices
FILAMENT, IBM, SAMSUNG

Data — Distributed storage of and access to business data
factom, MaidSafe, STORJ.IO

e-Identity — Registering and validating individual identity
ShoCard

Legal — Executing smart legal contracts
stampery, Bitproof.io

Crowd Funding — Raising finance & distributing equity
lighthouse, OpenBazaar

Market Places — Trading & sharing of physical & digital assets & services
La'Zooz, BLOCKPARTI, ALEXANDRIA, BISANTYUM

Publishing — Digital asset rights management, distribution & payment

Proof of Ownership — Tamper proof registration & "stamping" of physical & digital assets

Data & Analytics

COINALYTICS, BLOCKCORP, blockr, KAIKO, bitcoin charts

Key Security/HSMs

gemalto, THALES

Balancingthe Benefits

Blockchain Benefits
- Ecosystem simplification
- Faster interbank clearing & settlement
- Lower transaction costs
- Reduced counterparty risk
- Transaparency & auditability
- Ease of software development/integration

Vs.

Risks
- Unproven technology
- Untested capacity/scalability
- Low transaction speed
- Possible concensus protrotcol flaws
- Cryptocurrency price volatility
- Uncertain regulatory status

Investors

ANDREESSEN HOROWITZ, BLOCKCHAIN CAPITAL, overstock, Google ventures, LIGHTSPEED VENTURE PARTNERS, AME CLOUD VENTURES, DIGITAL CURRENCY GROUP, PANTERA

Blockchain

What is Blockchain?

Tamper-evident distributed data-structure

위변조 검출이 가능한 분산 데이터 구조

What is it for?

Reach consensus about data chronology

데이터 내역에 대한 의견일치를 위해 사용

Blockchain

In its purest form – as used by Bitcoin to create and track units of the crypto-currency – **blockchain is a shared digital ledger** of transactions recorded and verified across a network of participants **in a tamper-proof chain** that is visible to all. Permissioned or private variations add a layer of privileging to determine who can participate in the chain – and we expect the majority of commercial applications to use some form of permissioned model.

Goldman Sachs Global Investment Research, May 24, 2016

BLOCKCHAIN IS:

A database (with copies of the database replicated across multiple locations or nodes)

of transactions (between two or more parties)

split into blocks (with each block containing details of the transaction such as the seller, the buyer, the price, the contract terms, and other relevant details)

which are validated by the entire network via encryption by combining the common transaction details with the unique signatures of two or more parties. The transaction is valid if the result of the encoding is the same for all nodes.

and added to the chain of prior transactions (as long as the block is validated). If the block is invalid, a “consensus” of nodes will correct the result in the non-conforming node.

Blockchain benefits

Security

모든 데이터베이스를 한 곳에 보관/관리 한다면 해커들이 단 하나의 데이터베이스만 침입하는 것으로 치명적인 피해를 유발할 수 있다. 하지만 블록체인처럼 분산된 데이터 구조에 침입하는 것은 현실적으로 매우 어렵다.

Auditability

모든 참여자들이 장부를 공유하고 있기 때문에 기본적으로 모든 거래기록이 투명하게 공개된다.

Standardization

여러 기관이 참여하는 경우에도 시스템 통합에 따른 복잡한 프로세스와 그에 수반하는 고비용 구조를 줄일 수 있다.

Blockchain benefits for capital markets (McKinsey & Co)

Faster clearing and settlement

Leads to reduced costs, and lower counterparty settlement risk and fraud

Ledger consolidation & audit trail

Could address regulatory requirements for the consolidation of proprietary ledgers into a single data model for reporting purposes.

Reduction in systemic risk

Distributed ledgers virtually eliminate credit and liquidity risk by requiring pre-funding prior to trading.

Operational improvements

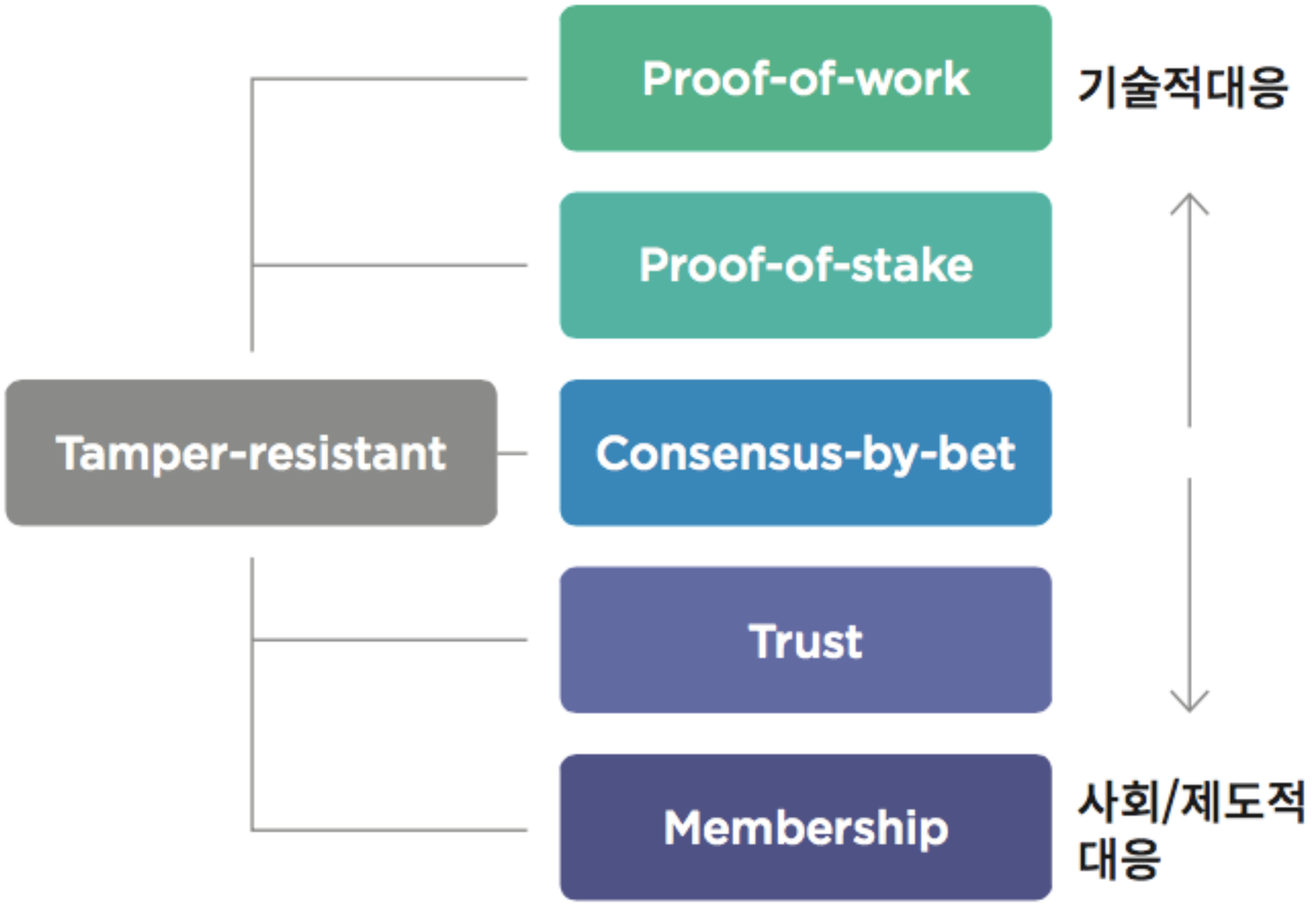
Instrument standardization and alignment of terms in advance of blockchain trading would eliminate a number of middle- and back-office processes.

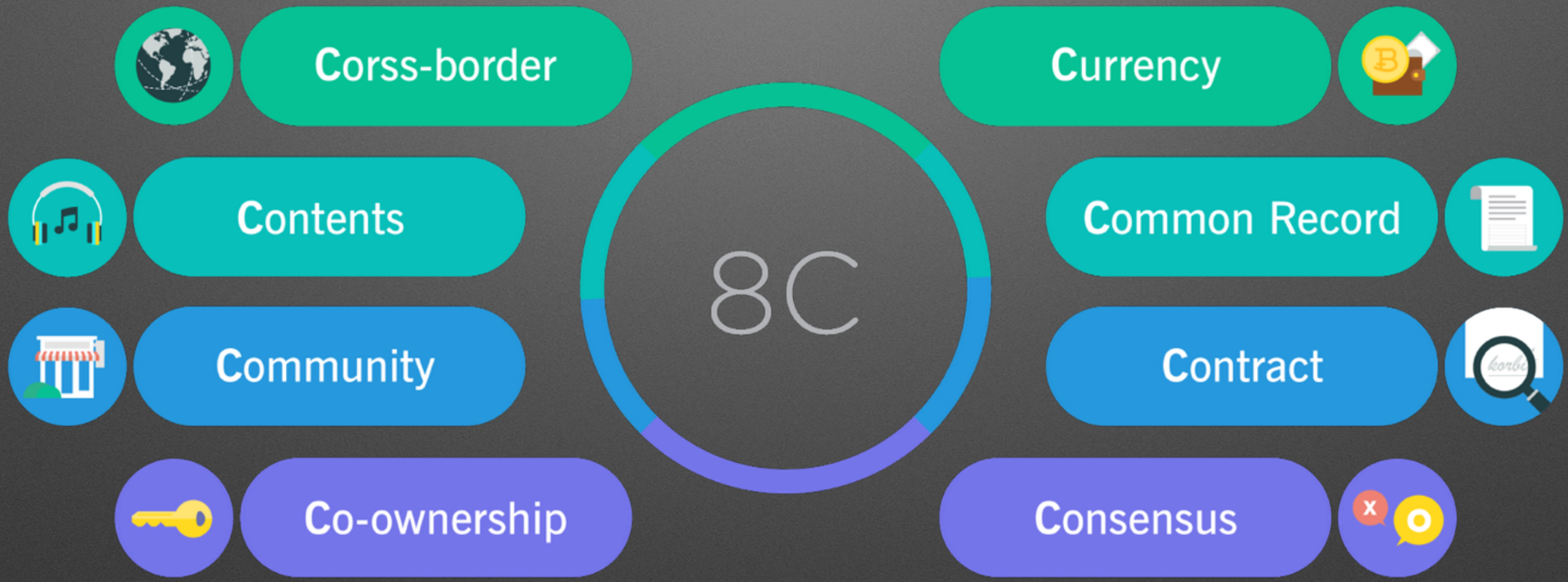
Source: McKinsey & Company, “Beyond the Hype: Blockchains in Capital Markets” (2016)

Blockchain types

	No Native Currency	Native Currency
Closed Membership	**공유 장부:** **데이터 관리 최적화** (은행간 블록체인)	혼합 시스템 (리플, 사이드체인...)
Open Membership	불가능?	**암호화 화폐:** **결제 최적화** **(비트코인, 이더리움...)**

그림1. 위변조에 대응하는 블록체인 메커니즘 분류





김진화, <동아비즈니스리뷰> 블록체인 스페셜 리포트 2015. 10

Creating New Markets

The Sharing Economy: Lodging

$3-9bn increase in US booking fees through 2020

What blockchain can do

Ease identity and reputation management. Blockchain can securely store and integrate users' online transaction and review history with identification and payment credentials—making it easier to establish trust between parties. This information can be used to streamline transactions and enhance review quality.

Select enablers

Airbnb, HomeAway, FlipKey, OneFineStay

Incumbents at risk

Hotel industry

Redistributing Markets with "Creative Destruction"

Smart grid

$2.5-7bn new US market for distributed power

What blockchain can do

Enable transactions in a decentralized power market. Blockchain can connect local power generators (think: neighbors with solar panels) to consumers in their area, enabling distributed, real-time power markets. A blockchain-enabled market could also increase grid security and spur adoption of smart grid technologies.

Select enablers

TransActive Grid; Grid Singularity

Incumbents at risk

Utility companies

Streamlining Existing Markets

Real estate title insurance

$2-4bn annual US cost savings

What blockchain can do

Improve efficiency and reduce risk. By recording property records in a blockchain, title insurers would have easier access to the information they need to clear a title. The fact that the ledger is tamper-proof could help lower real estate fraud in emerging markets.

Select enablers

BitFury, Factom / Epigraph

Incumbents at risk

Title insurers

Cash securities (equities, repo, leveraged loans)

$11-12bn annual global cost savings

What blockchain can do

Cut settlement times and reconciliation costs. Using a blockchain-based system can significantly shorten trade settlement time, in some cases from days to just hours. It also helps lower capital requirements, OpEx and custody fees in the process.

Additional savings could be achieved if blockchain is applied in other capital markets such as FX, OTC derivatives and commodities

Select enablers

Digital Asset Holdings, R3CEV, Chain.com, Australian Securities Exchange, itBit, Axoni, Ripple

Incumbents at risk

Custody banks and clearing houses

Anti-money laundering compliance

$3-5bn annual global cost savings

What blockchain can do

Increase transparency and efficiency. Storing account and payment information with blockchain could improve data quality and reduce the number of falsely identified "suspicious" transactions.

Select enablers

SWIFT and others

Incumbents at risk

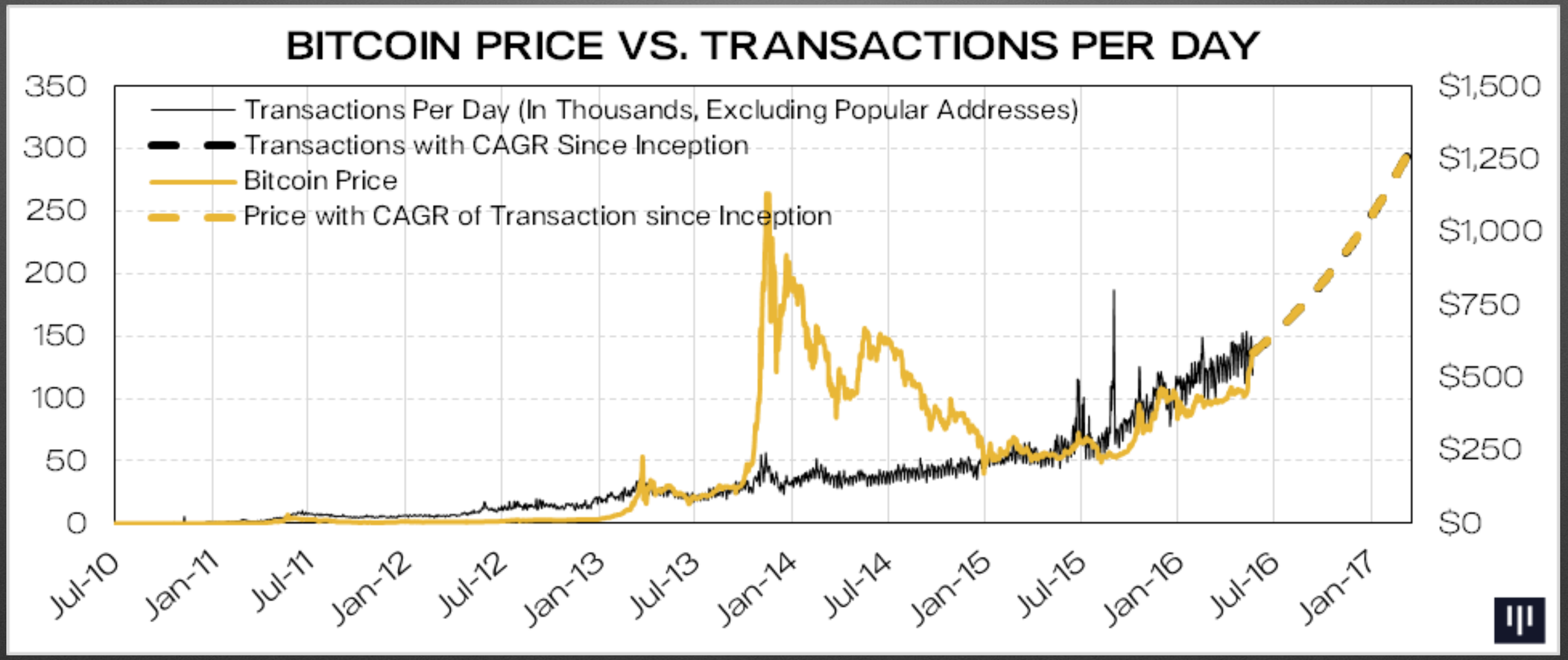
Specialty compliance software vendors

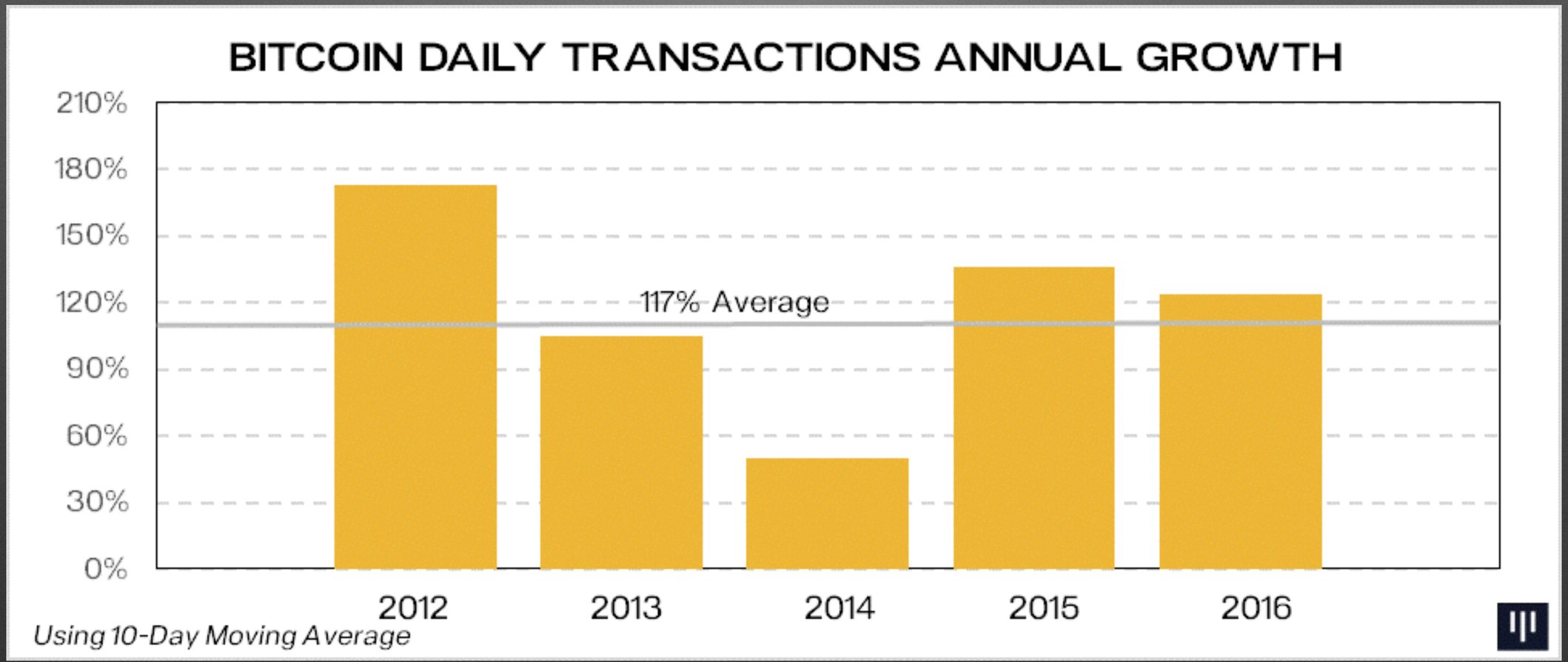
Our beliefs

Bitcoin is not consumer currency.
Bitcoin is a settlement instrument.

Private blockchains for data exchange.
Public blockchains for value exchange.

The blockchain ecosystem will consist of
domestic champions and global connectors.

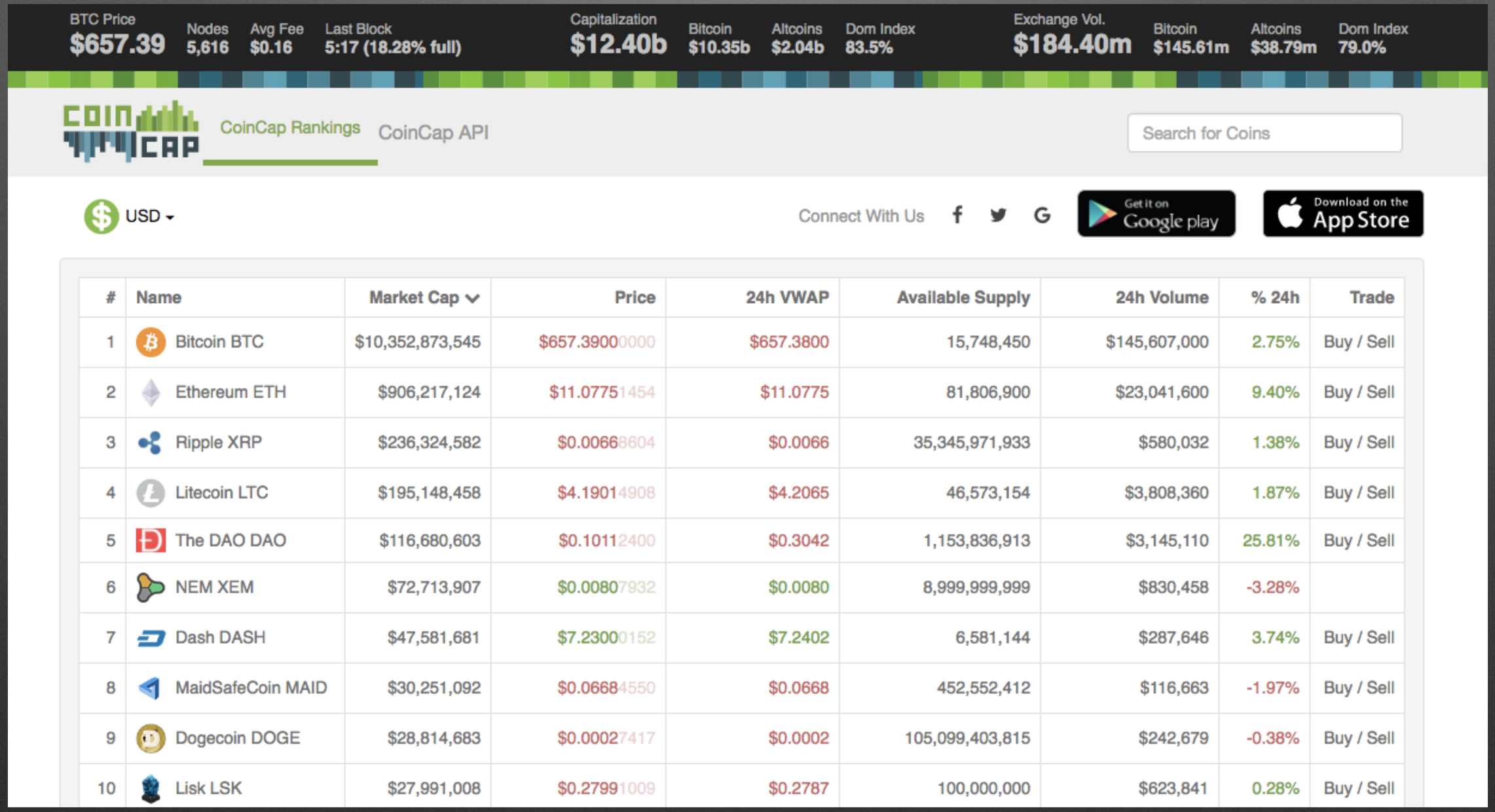

BITCOIN PRICE VS. TRANSACTIONS PER DAY
Transactions Per Day (In Thousands, Excluding Popular Addresses)
Transactions with CAGR Since Inception
Bitcoin Price
Price with CAGR of Transaction since Inception
350
300
250
200
150
100
50
0
$1,500
$1,250
$1,000
$750
$500
$250
$0
Jul-10
Jan-11
Jul-11
Jan-12
Jul-12
Jan-13
Jul-13
Jan-14
Jul-14
Jan-15
Jul-15
Jan-16
Jul-16
Jan-17


BITCOIN DAILY TRANSACTIONS ANNUAL GROWTH
210%
180%
150%
120%
90%
60%
30%
0%
117% Average
2012
2013
2014
2015
2016
Using 10-Day Moving Average

Public Crowdsale,
July and August 2014

31,529 BTC = $18.5m
Ether: 60,102,216 판매

올해들어 2,000% 성장



#	Name	Market Cap	Price	24h VWAP	Available Supply	24h Volume	% 24h	Trade
1	Bitcoin BTC	$10,352,873,545	$657.39000000	$657.3800	15,748,450	$145,607,000	2.75%	Buy / Sell
2	Ethereum ETH	$906,217,124	$11.07751454	$11.0775	81,806,900	$23,041,600	9.40%	Buy / Sell
3	Ripple XRP	$236,324,582	$0.00668604	$0.0066	35,345,971,933	$580,032	1.38%	Buy / Sell
4	Litecoin LTC	$195,148,458	$4.19014908	$4.2065	46,573,154	$3,808,360	1.87%	Buy / Sell
5	The DAO DAO	$116,680,603	$0.10112400	$0.3042	1,153,836,913	$3,145,110	25.81%	Buy / Sell
6	NEM XEM	$72,713,907	$0.00807932	$0.0080	8,999,999,999	$830,458	-3.28%	
7	Dash DASH	$47,581,681	$7.23000152	$7.2402	6,581,144	$287,646	3.74%	Buy / Sell
8	MaidSafeCoin MAID	$30,251,092	$0.06684550	$0.0668	452,552,412	$116,663	-1.97%	Buy / Sell
9	Dogecoin DOGE	$28,814,683	$0.00027417	$0.0002	105,099,403,815	$242,679	-0.38%	Buy / Sell
10	Lisk LSK	$27,991,008	$0.27991009	$0.2787	100,000,000	$623,841	0.28%	Buy / Sell

DAO

Distributed Autonomous Organization

The Mother of all DAOs

Created Once. Endless opportunities.

DAOs will be at the center of many economies going forward and intend to be at the forefront of supporting innovative and promising projects, products and services in order to become 'The DAO': A flexible decentralized autonomous organization leveraging the wisdom of the crowds to benefit the DAO Token Holders.

SEE THE PROPOSALS

The DAO

CREATION PROPOSALS MANIFESTO CURATOR PRINCIPLES VOTING FORUMS TERMS SUPPORT BLOG

The time has come to breathe life into The DAO

A One Time Only Event

1097.53 M
DAO TOKENS CREATED

11.02 M
TOTAL ETH

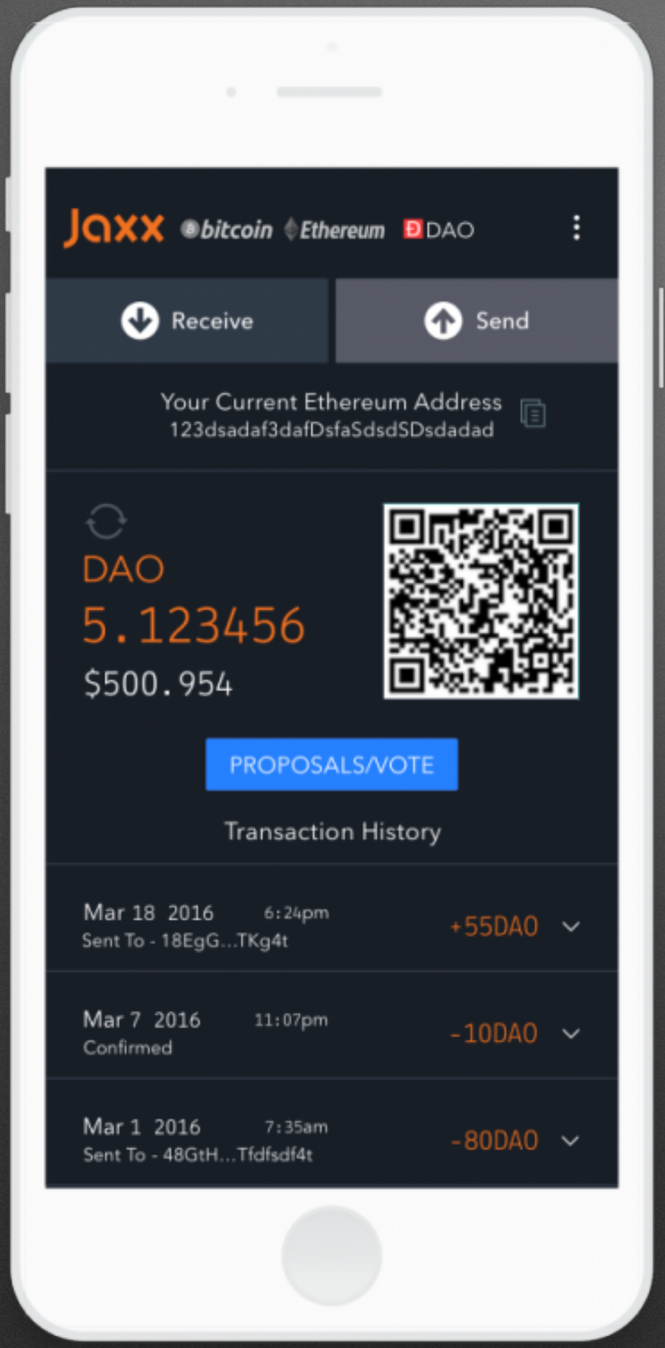
146.60 M
USD EQUIVALENT

1.20
CURRENT RATE
ETH / 100 DAO TOKENS

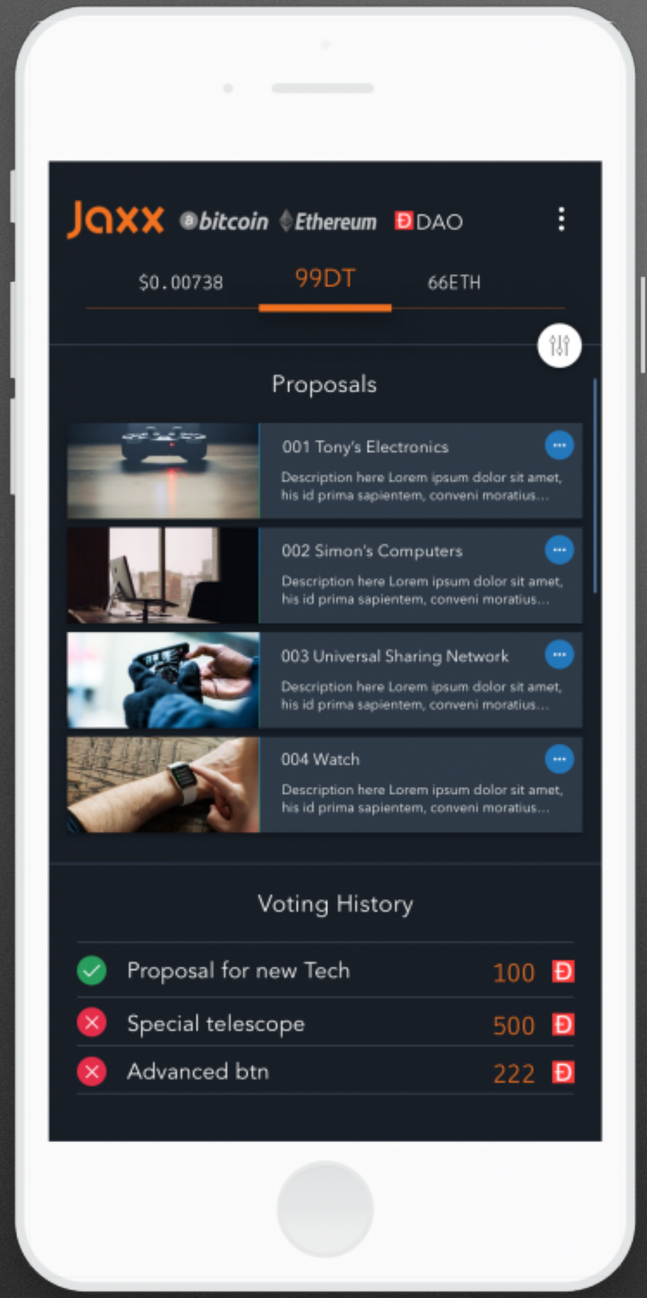
23 hours
NEXT PRICE PHASE

9 days
LEFT
ENDS 28 MAY 09:00 GMT

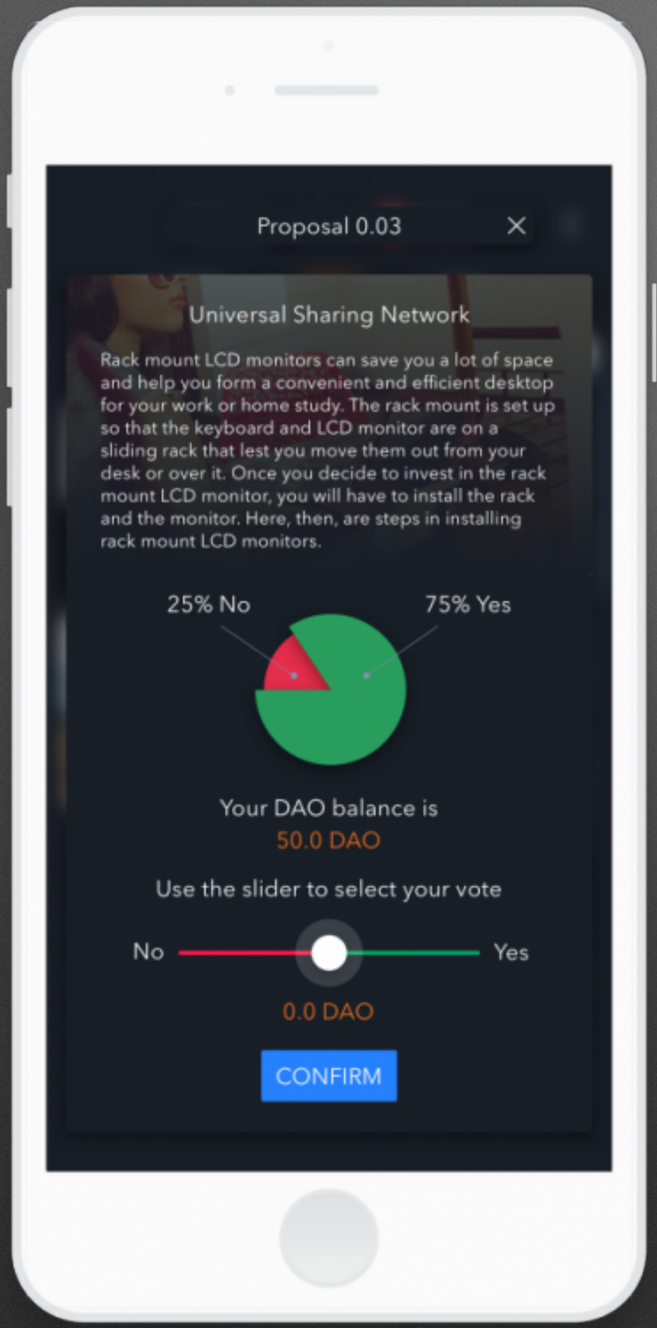
To obtain DAO tokens, follow the wizard below or send ETH from your **Ethereum Wallet** (NOT an exchange) to The DAO's address below. Note that sending ETH to the DAO's address signifies your acceptance of the **Terms**



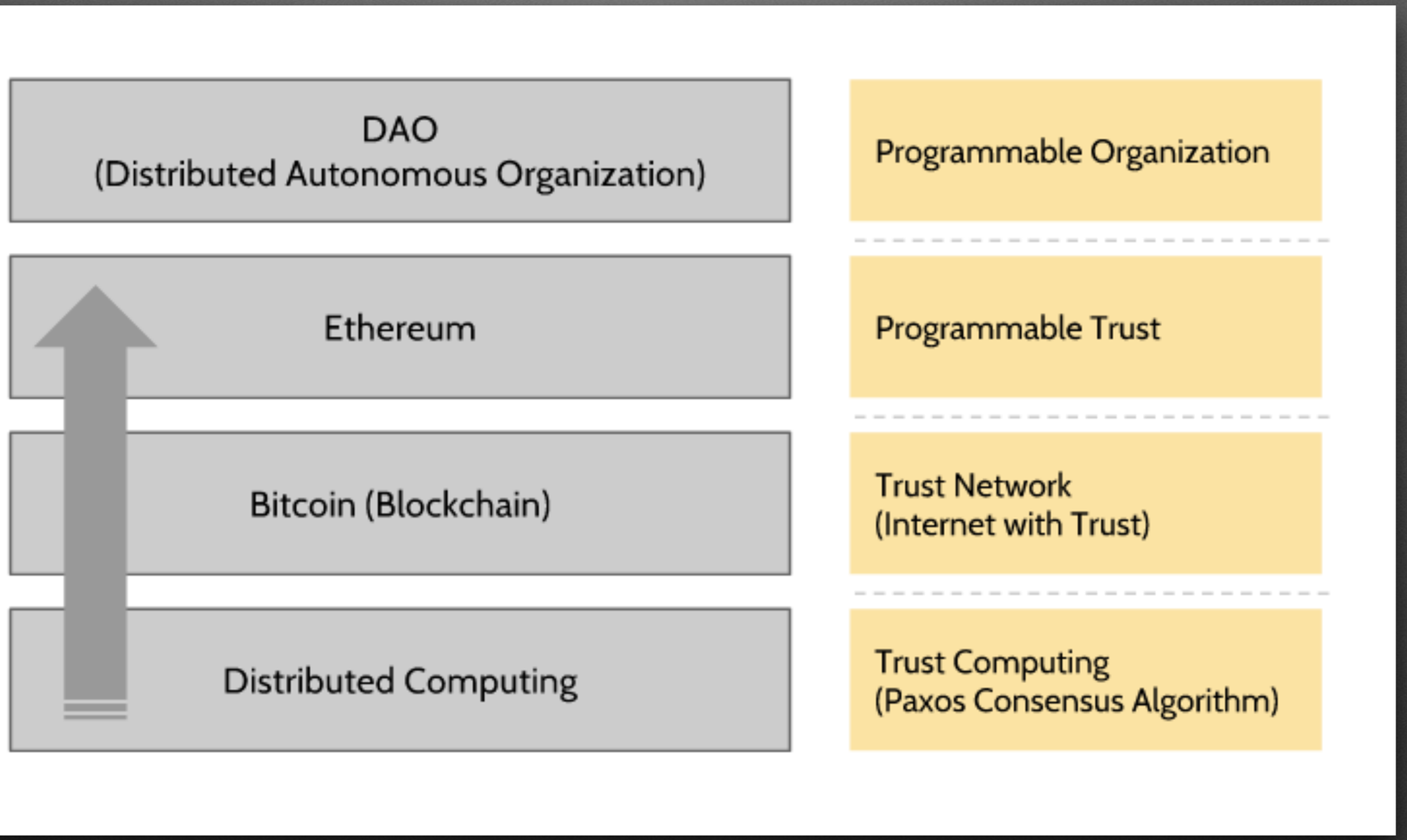
The initial DAO screen,
for viewing your token balance and
transferring tokens
between accounts.



The proposals screen,
which displays current DAO proposals
and your voting history.



When you select a proposal, you can read its description, as well as view the current For/Against breakdown for members who have voted so far.
A slider will let you select your vote and the level of token commitment you're making.


DAO
(Distributed Autonomous Organization)
Ethereum
Bitcoin (Blockchain)
Distributed Computing
Programmable Organization
Programmable Trust
Trust Network
(Internet with Trust)
Trust Computing
(Paxos Consensus Algorithm)

- Fedex


WEFT
DEPOSCO
postmaster
uShip
HAVEN
FLEXPORT
TRANSFIX
FedEx
Ship
Track
Manage
Learn
FedEx Office
CB INSIGHTS
shipstr
KEYCHAIN
ROADIE
Shipwire
boxc
Package, Envelope, or Express Freight
FedEx Express or FedEx Ground
Create Shipment
Get Rates & Transit Times
Find FedEx Locations
Schedule and Manage Pickups
Order Shipping Supplies
Pack Shipment
Access International Services
Freight Shipments
FedEx Freight
Generate Bill of Lading
Get Rates and Transit Times
Schedule and Manage Pickups
View Transit Maps
Find FedEx Locations
Go to Shipping Desk
International Services
U.S. Offshore Services
Expedited/Extra-care Handling
FedEx Custom Critical
Ship
Fast Ship
Get Rates & Transit Times
Temperature Control
Secure Services
Truckload Solutions
Air/Ocean Freight Forwarding
FedEx Trade Networks
Get Forms
My Forms
Importer Security Filing
eManifest
DROPSHIP
RICKSHAW
MATTERNET
Doorman
shyp
shippo
ShipBob
pivot
cargomatic
UBER
deliv
zipments

44 Startups Attacking Apple's Core Apps and Services

CB INSIGHTS

www.cbinsights.com

- A Bank becomes “Another Dumb Pipe”.

Blockchain Could be
'Economic Layer'
for the Web