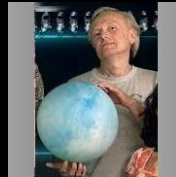

Humankind 2.0: The Technologies of the Future

8. Blockchain and Fintech

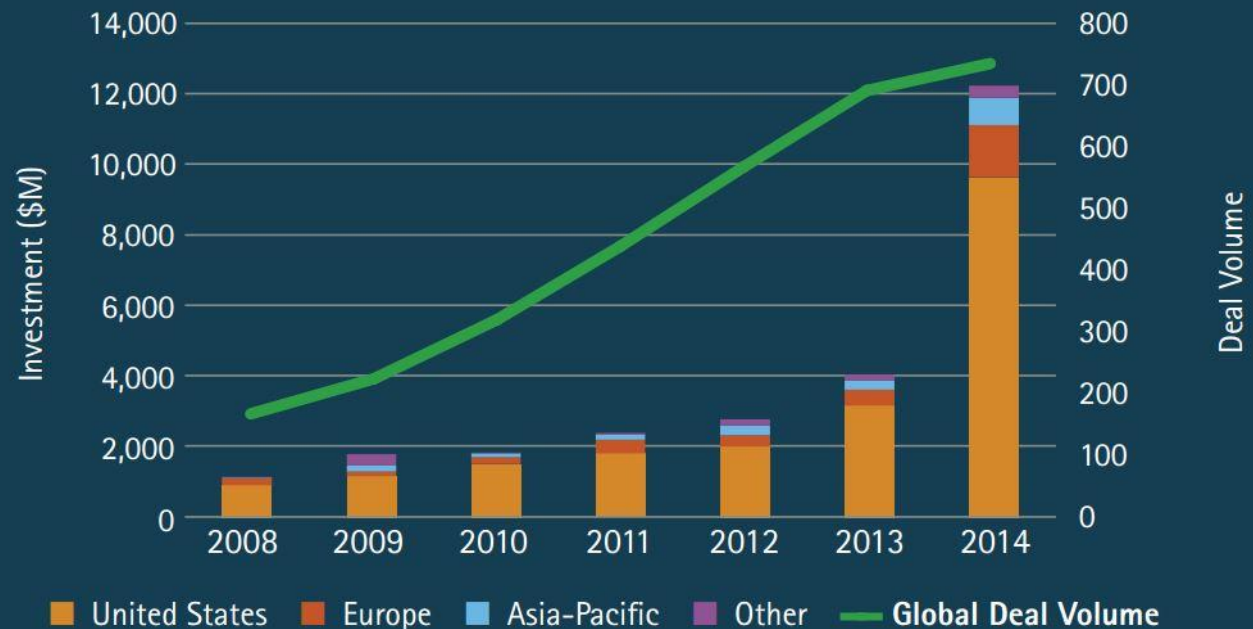
Piero Scaruffi, 2016



FinTech

- Investments in fintech startups doubled between 2014 and 2015, to \$19 billion (KPMG and CB Insights)

Figure 4: Global FinTech Financing Activity

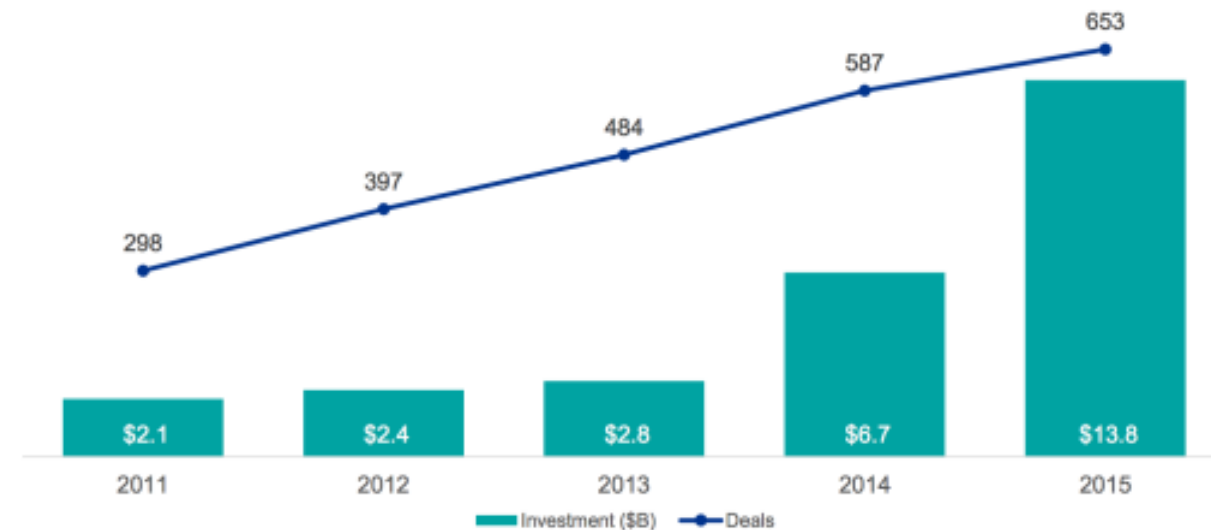


Source: Accenture and CB Insights

FinTech

Annual Global Financing Trends to VC-Backed Fintech Companies

2011 – 2015



Source: The Pulse of Fintech, 2015 in Review, Global Analysis of Fintech Venture Funding, KPMG International and CB Insights (data provided by CB Insights) March 9th, 2016.

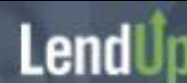
FinTech Origins

- Online stock brokerage
 - E*Trade (1992, Palo Alto)
- Internet banking
 - First Virtual (1994)
 - ING Direct (1996, Canada)
 - Everbank (1998, Florida)
 - Ally Bank (2001, Utah)
- Online payment
 - First Virtual (1994)
 - CyberCash (1994)



eBanking

- OnDeck (New York, 2007): small business lender
- Kabbage (Atlanta, 2009): small business lender
- Funding Circle (London, 2010): small business lender
- Kreditech (Germany, 2012): instant lending to individuals based on credit score
- BankMobile (New York, 2015): no-fee online and mobile bank
- LendUp (San Francisco, 2011): payday loans

The OnDeck logo features the word "OnDeck" in a blue sans-serif font, followed by a blue chevron symbol pointing to the right.The Kabbage logo consists of a stylized green leaf icon to the left of the word "Kabbage" in a green sans-serif font.The Funding Circle logo features a purple circular icon with a white arrow pointing clockwise, followed by the words "Funding Circle" in a black sans-serif font.The Kreditech logo has a blue background with a yellow and orange bar chart icon on the left, followed by the word "Kreditech" in a white sans-serif font.The bankmobile logo features the word "bankmobile" in a lowercase, rounded, grey sans-serif font.The LendUp logo has a dark grey background with the word "LendUp" in a white sans-serif font, where the "Up" is slightly larger and more prominent.

eBanking

- SoFi (Stanford Graduate School of Business, 2011): student loan refinancing



Marketplace Lending

- Fintech + Sharing Economy + P2P
- Zopa (London, 2005)
- Lending Club (San Francisco, 2006)
- Prosper (San Francisco, 2006)
- Upstart (Palo Alto, 2012)



Automated Financial Advisors

Algorithm-based financial advisors

- Betterment (New York, 2008)
- Personal Capital (Redwood City, 2009)
- Nutmeg (London, 2010)
- Wealthfront (Palo Alto, 2011)
- Charles Schwab's Intelligent Portfolios (2014)
- Coincube (New York, 2014): a robo-advising service for Bitcoin

The logo for Betterment, featuring a white icon of a person's head and shoulders inside a blue circle, followed by the word "Betterment" in white sans-serif font.The logo for Personal Capital, featuring a stylized icon of three vertical bars of increasing height, followed by the words "PERSONAL CAPITAL" in white sans-serif font.The logo for Nutmeg, featuring the word "nutmeg" in white lowercase sans-serif font on a green rectangular background.The logo for Wealthfront, featuring a stylized green icon of three curved lines, followed by the word "wealthfront" in white lowercase sans-serif font.The logo for Charles Schwab, featuring the words "charles SCHWAB" in white sans-serif font, with "charles" in a script font and "SCHWAB" in a bold sans-serif font, on a blue rectangular background.The logo for Coincube, featuring the word "COINCUBE" in white uppercase sans-serif font on a blue rectangular background.

Payments

- Currency Cloud (London, 2010): B2B international payments
- AstroPay (London, 2009): international credit card payment
- Tipalti (Palo Alto, 2010): international payments
- Zipmark (New York, 2010): online check payments
- Check (Palo Alto, 2013; acquired by Intuit): mobile bill payment



Trading Brokerage

- RobinHood (Palo Alto, 2013): mobile based commission-free trading brokerage.



Real Estate

- Nestio (New York, 2011): finding residential rentals/ leasing and marketing platform for residential landlords
- Point (Palo Alto, 2014): home equity marketplace



Automotive Retail

- Drive Shift (San Francisco, 2013)
- Beepi (Los Altos, 2013)
- Vroom (New York, 2013)



And more...

- Float (Los Angeles, 2015): 24/7 mobile digital credit
- Cumulus Funding (Chicago, 2011): Income Share Agreements (receive funds in exchange for a small percentage of your income)
- Activehours (Palo Alto, 2012): provide employees with immediate access to accrued wages
- FlexWage (New Jersey, 2009): provide employees with immediate access to accrued wages



Fraud Detection

- BillGuard (New York, 2010; acquired by Prosper)
- Rippleshot (Chicago, 2012)
- Iris Analytics (Germany, 2007, acquired by IBM)



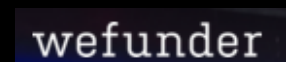
Mortgage

- Planwise (San Mateo, 2011): automatic real estate and mortgage lender
- Quicken's Rocket Mortgage (2015): mortgage/refinance tool



Equity Crowdfunding

- Funding startups with money collected from individuals
- An alternative to banks, angel investors and venture capitalists
- EquityNet (Arizona, 2005): a social network for investors and entrepreneurs
- Legalized in the USA by the JOBS Act (2012)
- Crowdcube (England, 2011)
- Seedrs (England, 2012)
- CircleU (San Francisco, 2011)
- Wefunder (San Francisco, 2011)



P2P Insurance

- Policy holders form individual insurance-networks, thereby lowering their annual insurance premiums
- Friendsurance (Germany, 2010): peer-to-peer personal/casualty insurance
- Guevara (London, 2014): peer-to-peer car insurance
- Lemonade (New York, 2015): peer-to-peer property/casualty insurance



Virtual Insurance Agents

- CoverHound (San Francisco, 2010)
- Insurify (Boston, 2016): Evia (Expert Virtual Insurance Agent) to find the best car insurance

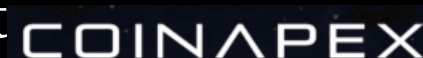


Fintech accelerators

- SixThirty (St Louis, 2013): startup accelerator specializing in fintech



- Coin Apex (New York, 2014): startup incubator specializing in Bitcoin startups



- Mentorship programs:
 - FinTech Innovation Lab Exposes (New York, 2012): mentorship program run by the New York City Investment Fund and Accenture
 - FinTech Sandbox (Boston, 2014): nonprofit six-month program for FinTech startups



Fintech accelerators

- Financial Solutions Lab (CFSI and JPMorgan Chase, 2015): a community of startups, financial services companies and nonprofit organizations building solutions to improve the financial lives of citizens

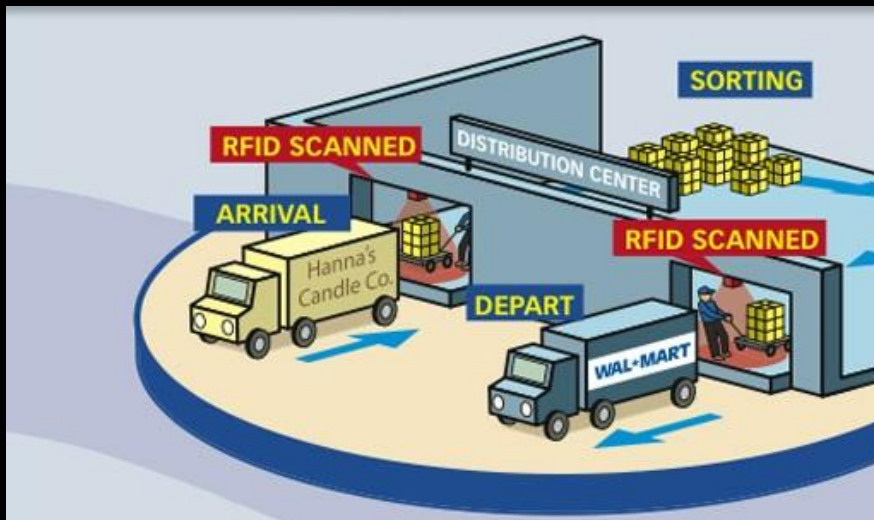


The Electronic Wallet



Electronic Wallet

- The RFID era
 - Sony's FeliCa in Japan (1996)
 - Wal-Mart (2004): RFID mandatory on its suppliers
 - Nokia 5140 (2004): the first GSM phone integrated with RFID reading capability



Electronic Wallet

- Billpoint (1998, backed by eBay, Wells Fargo, Visa): person-to-person payment
- Paypal (2000)
 - Payment by email
 - Compatible with the physical world (bank account and credit cards)
 - No need to share bank account / credit card information with merchants
 - Verification (small-value deposit)
 - Simplicity



Electronic Wallet

- Paypal mafia



Electronic Wallet

- The NFC era
 - Sony and Philips/ NXP (2004): Near Field Communication (NFC), a two-way wireless technology for short-range communications between electronic devices
 - Blaze Mobile (2005, Berkeley): the NFC payment sticker
 - Nokia 6131 (2007): the first NFC phone
 - Bling Nation (2007, Palo Alto): NFC sticker for smartphones to charge purchases to a Paypal account.



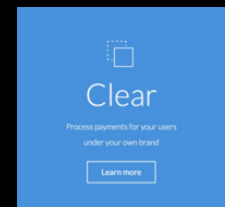
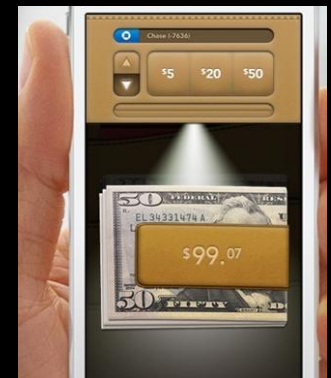
Mobile Payment

- Mobile users carry a computer with them, not just a phone. They even carry a GPS that knows their location.
- Square (2009, Jack Dorsey): a "reader" that allows anybody with a mobile phone to make a payment and anybody with a mobile phone (and a Square-provided "cash register") to accept it (no cash, no credit cards, no RFID, no receipt).
- Stripe (2010, Patrick and John Collison)
 - Supported by Visa and American Express
- Flint (2011): like Square but no hardware - just scanning credit cards

A screenshot of the Stripe payment interface. It features a light blue header with the 'stripe' logo. Below the header, there are input fields for 'Card number:', 'Expires:', 'Name on card:', and 'Card code:'. A blue button at the bottom says 'Pay \$1210.00'.

Mobile Payment

- Paypal Beacon (2013)
 - Bluetooth-based technology that detects Beacon-enabled phones when customers enter a Beacon-enabled store and then automate the purchase of merchandise
- Clinkle (2014, Palo Alto)
 - Compatibility with every merchant
 - Phone-to-phone payments via Aerolink
- WePay Clear (2014, Palo Alto): like Stripe but fraud-free guarantee



Mobile Payment

- Apple's iBeacon (2013)
 - Bluetooth technology to alert devices of the presence of fellow iBeacon devices.
 - Apple Pay (2014) to make online payments as secure as in-store payments
 - Digital wallet incorporated directly into the operating system
 - SIM-independent secure memory chip, an NFC radio, and a fingerprint reader.



Mobile Payment

- Google Wallet (2011, replaced by Android Pay)
- Etc

Chirpify

DWOLLA

icache.com

zipmark



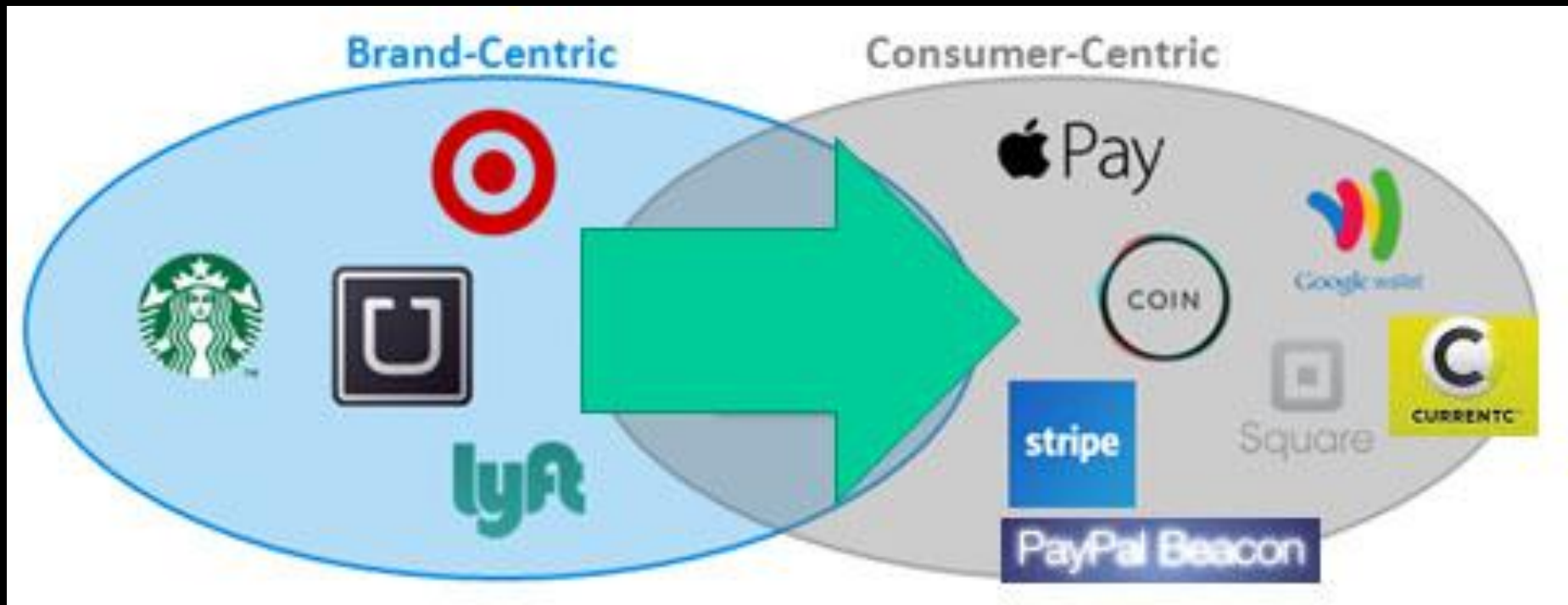
Mobile Payment

- The QR Age
 - AliPay (2004)
 - WeChat Pay
 - LianLian Pay (2016)



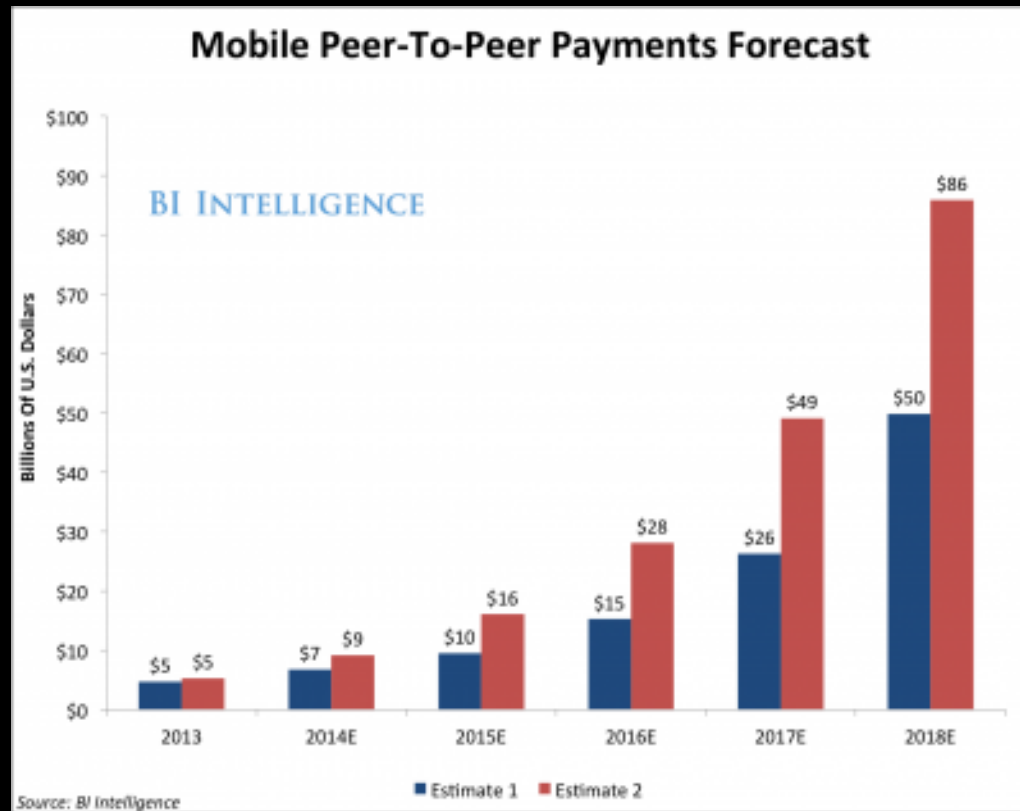
Mobile Payment

- Transition from brand-centric to consumer-centric



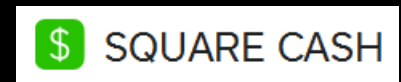
Mobile Payment

- Peer-to-peer payment



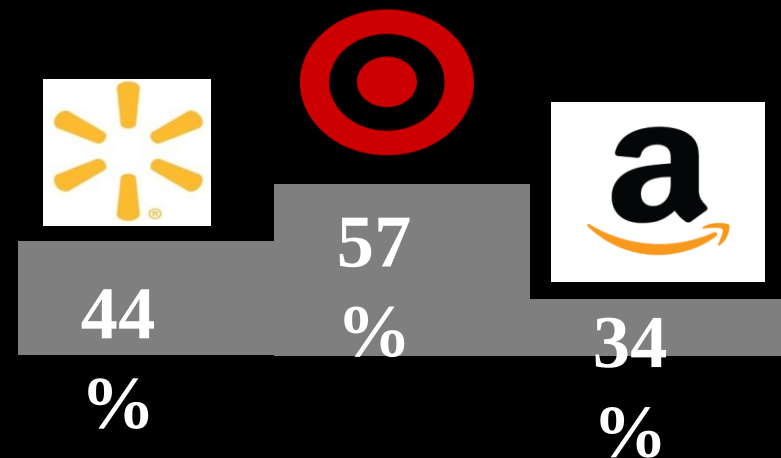
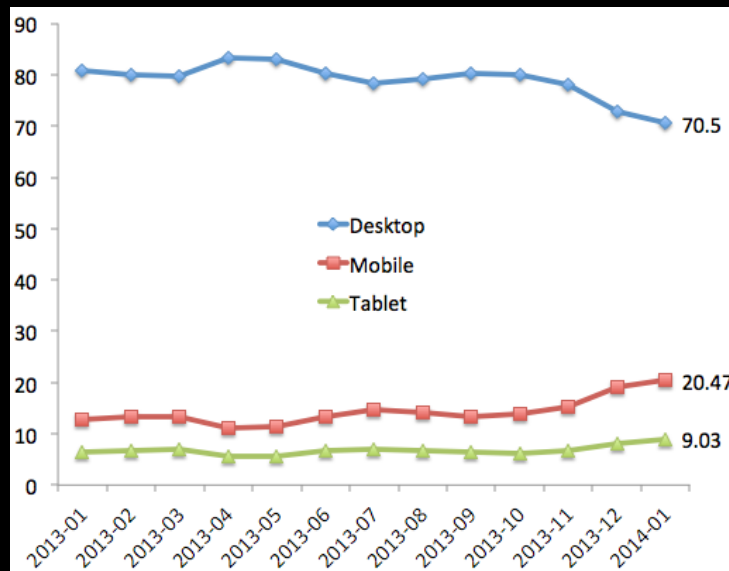
Mobile Payment

- Peer-to-peer payment
 - WePay (Boston, 2008)
 - Venmo (New York, 2009)
 - GoCardless (London, 2011)
 - nTrust (Canada, 2011)
 - Square Cash (2013)
 - SnapChat 's SnapCash (2014, based on Square Cash)
 - Google's new Wallet (plans to link Google Wallet to Gmail but only on Android)



Mobile Payment

- Thanksgiving 2014: mobile devices outpace personal-computers for online browsing
- 2015: 30% of all eCommerce traffic in the USA comes from smartphones and tablets



Mobile Payment

- 2016: Google Hands Free connects the customer's phone with a point of sales system so that the customer can pay without pulling out the smartphone (same idea that Square had)

China

Examples of Internet finance in China

Company	Product/service	Brand name	Description
Alibaba	Payments, settlement, remittances	Alipay	Established in 2004 as a third-party payment platform to resolve Alibaba's Taobao C2C site's payment difficulties. Can be used to pay utility and credit card bills and transfer funds to participating banks. Has also started to extend credit to consumers based on their repayment histories.
	Lending	Ali Microfinance	Microfinance company that extends credit to merchants of Alibaba B2B site, Taobao C2C site and Tmall B2C site. Also securitizes loans to microenterprises.
	Fund management	Yu'E Bao	See main text
		Taobao wealth management	First online third-party fund sales platform (November 2013). Provides sales support to fund distributors.
Alibaba, China Ping An Insurance & Tencent	Insurance sales	Zhong An Online Property Insurance	Sells insurance and settles insurance claims online without bricks-and-mortar branches (November 2013).
Tencent	Payments	Tenpay	Payment service similar to Alipay
	Fund management	WeChat	WeChat is a messaging app like Line. WeChat wealth management products were launched in January 2014 (see main text).
Renrendai	P2P lending		Established in May 2010
Demohour	Crowd funding		Established in May 2011
China Construction Bank	E-commerce, financial services	Shanrong	B2B and B2C e-commerce platform (June 2012). Industrial and Commercial Bank of China's Rong-e-Gou (B2C) platform went live in January 2014. Bank of China, Bank of Communications, et al. also have similar platforms.

Source: NRI, based on company disclosures and media reports

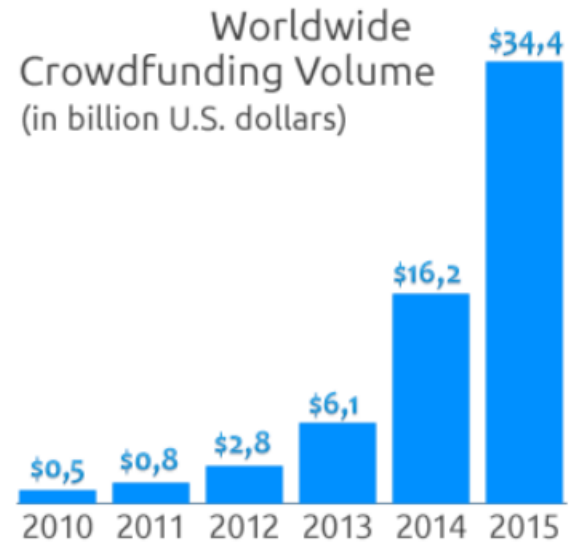
Crowdfunding

“Crowdfunding will surpass VC as a funding source in 2016” (Forbes)

Kickstarter (2008, San Francisco)

Indiegogo (2008, New York)

GoFundMe (2010, San Diego)



Crowdfunding Site	2014 Volume
gofundme	\$470M
KICKSTARTER	\$444M
indiegogo	???

Cryptography

- Post-quantum cryptography
- Zero-knowledge proofs
- Indistinguishability obfuscation
- Secure multi-party computation
- Bitcoin blockchain

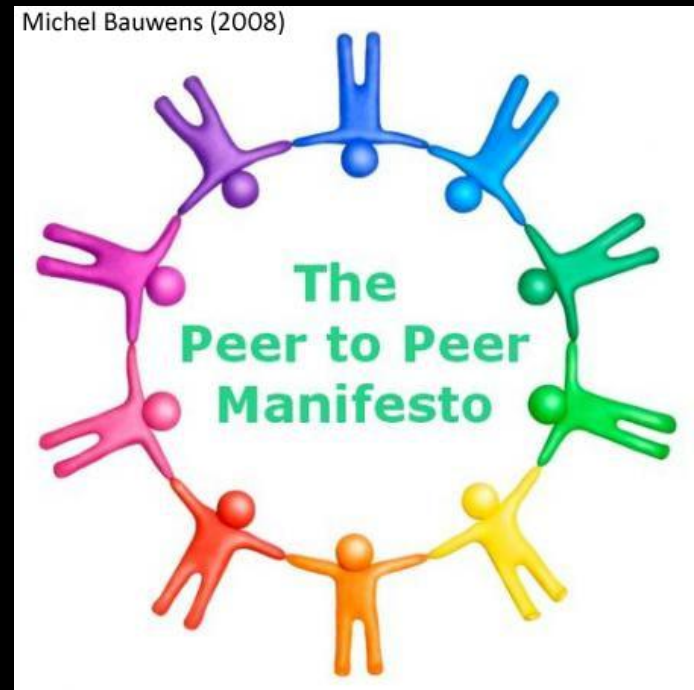


Makart Steg in Salzburg
With thousands of love padlocks

The Peer-to-peer World

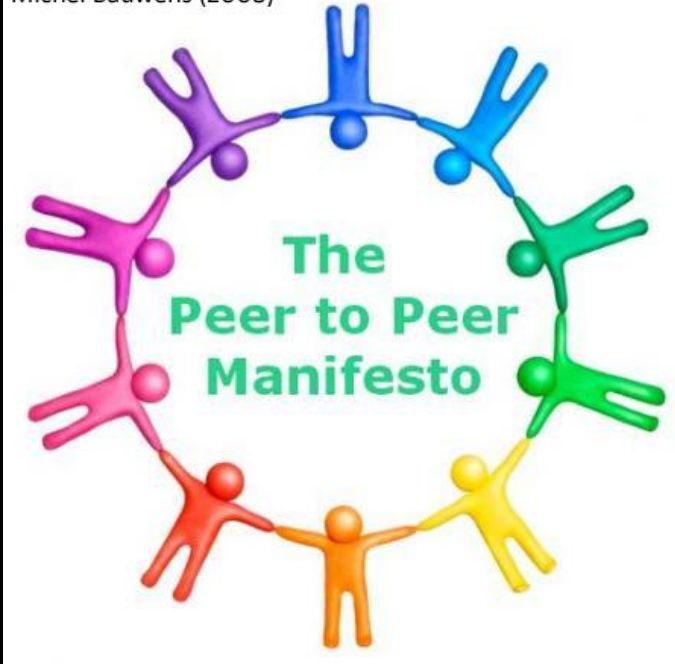


The Peer-to-peer World



The Peer-to-peer World

Michel Bauwens (2008)



Silk Road (2013)



Cybercurrency

- DigiCash (David Chaum, 1990)
- E-gold (Douglas Jackson, 1996): 5 million users by 2009 - shut down by the USA
- WebMoney (Russia, 1998)
- Tencent's qq coins (China, 2005) - shut down by China
- Liberty Reserve (Costa Rica, 2006) - shut down by the USA
- Perfect Money (Andrew Draper, Switzerland, 2007)
- Bitcoin (2009) - decentralized!



Cybercurrency

- 402 error code never implemented

Error

- 401 Unauthorized
- 402 Payment Required
- 403 Forbidden
- 404 Not Found
- 405 Method Not Allowed
- 409 Conflict
- 410 Gone

Cybercurrency

- Cynthia Dwork (1992): punish spammers with computational processing, i.e. computational processing is a cost
- Adam Back (1997): hashcash (cryptographic hash functions on a network, no need for central authority)
- Nick Szabo (1997): a distributed trust model



Cybercurrency

- Bitcoin

The Crypto Anarchist Manifesto

[Timothy C. May](mailto:tcmay@netcom.com) <tcmay@netcom.com>



cypherpunk



Martti Malmi www.weidai.com
Wei Dai



Craig Wright **Dave Kleiman**



Hal Finney **Nick Szabo**



Cybercurrency

- Bitcoin (2009)
 - The first successful currency not to be printed by a government
 - A system capable of creating copies that cannot be copied
 - Peer-to-peer
- Bitcoin's distributed blockchain mechanism makes central authorities of trust obsolete
- Virtually invulnerable to hacking (unlike government databases)



Cybercurrency

- Jan 2017: Bitcoin surges past \$1000 for the first time in 3 years
- Dec 2017: Bitcoin surges past \$10,000 for the first time



How does Bitcoin work?

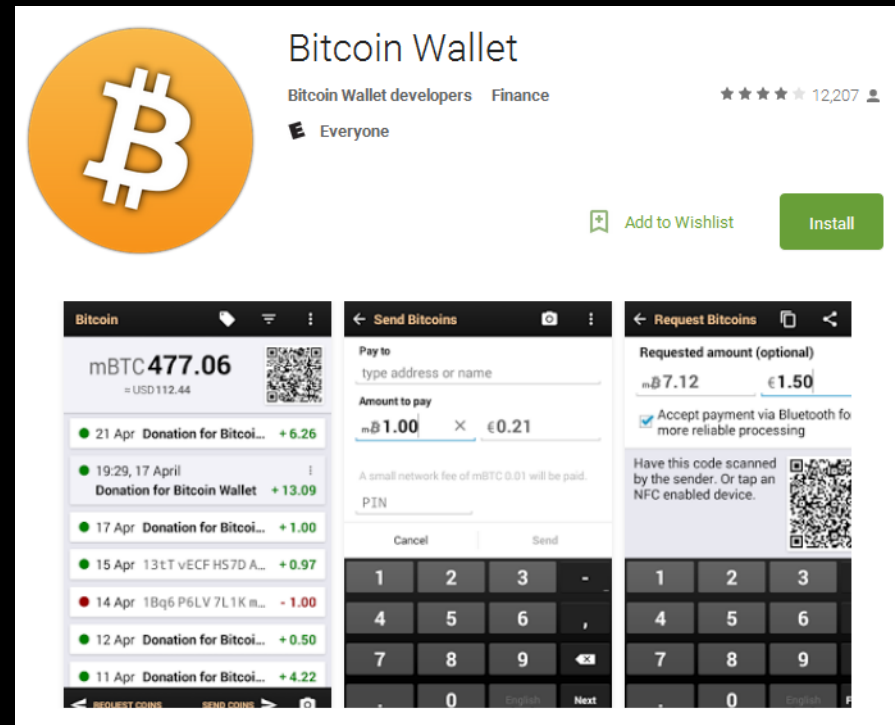
1. Download a software wallet app



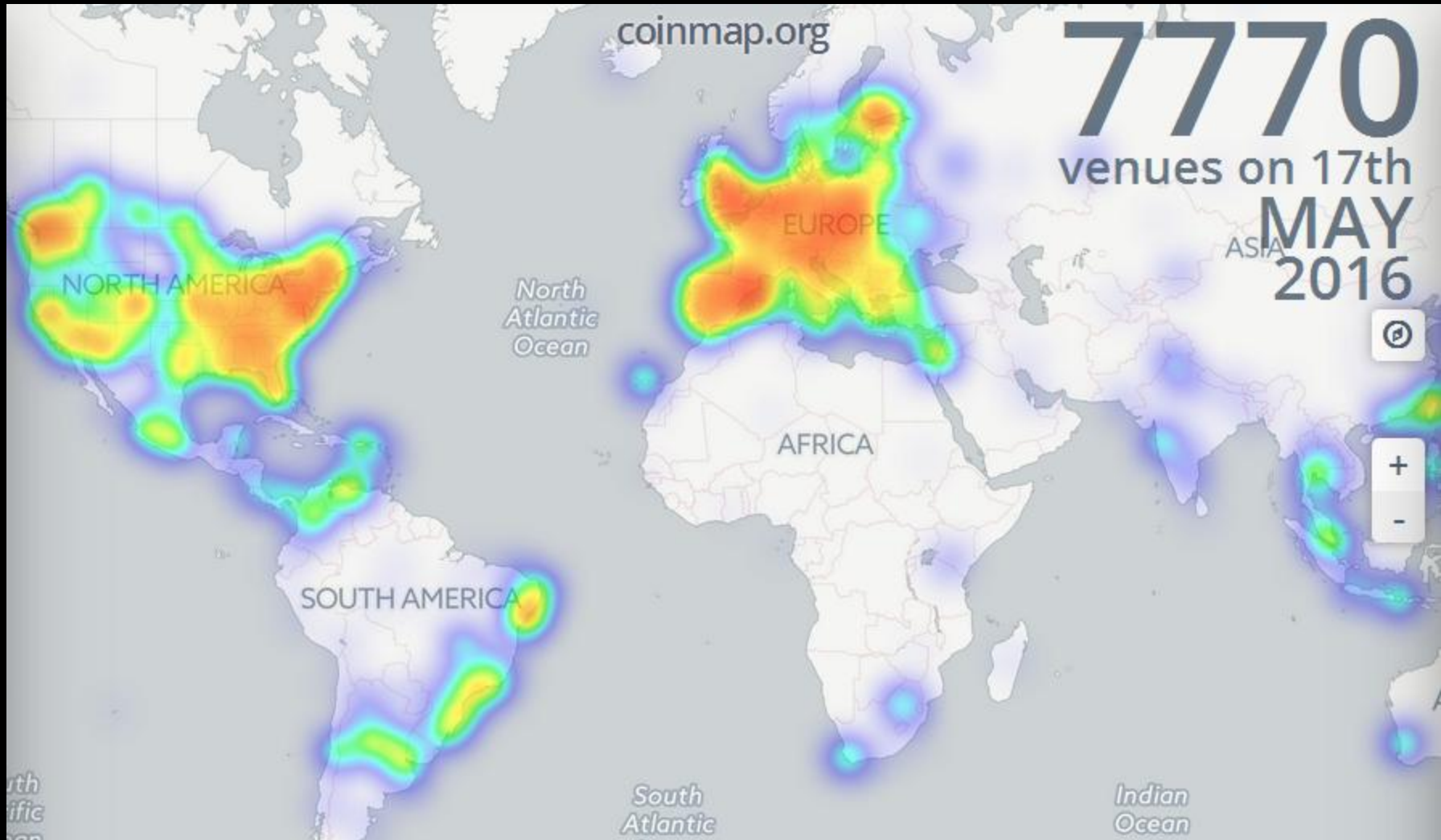
2. Buy bitcoins



3. Spend bitcoins

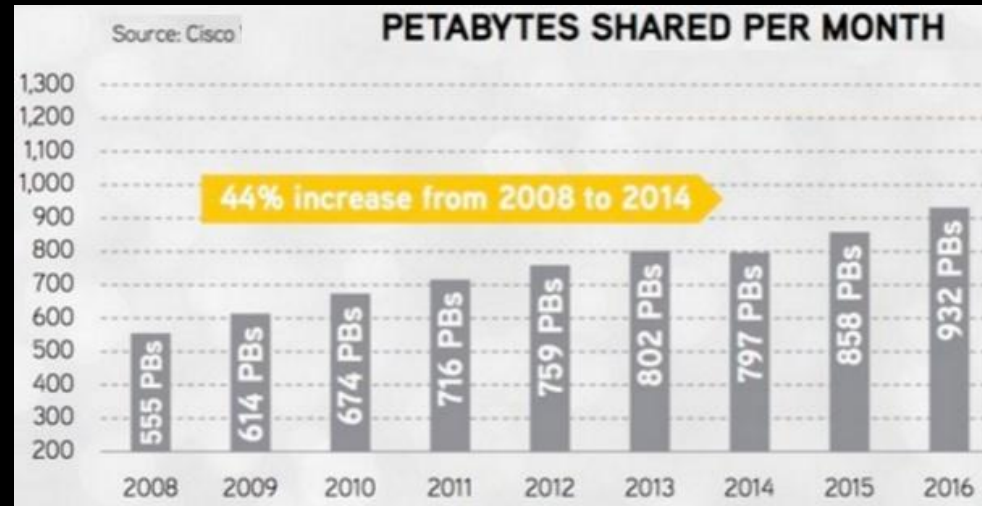


Where can I use Bitcoin?

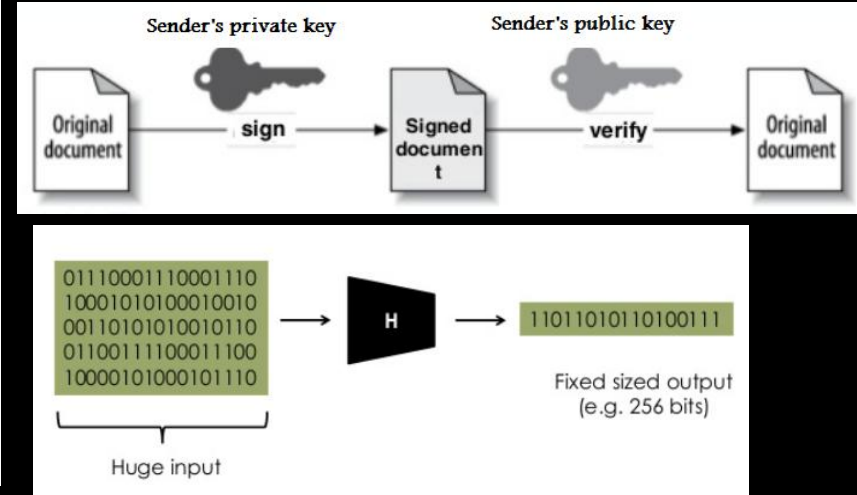
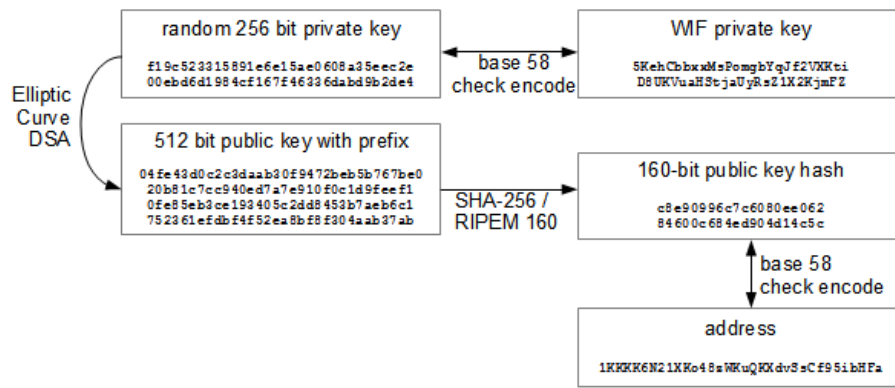


Bitcoin

- Enabling technologies:
 - distributed file sharing,
 - digital signature,
 - hashing,
 - and... blockchain



Bitcoin Keys

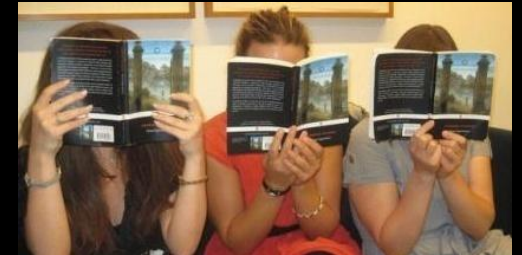


Blockchain

- The missing disruption
- The world runs on three processes: storage, computation, and communication.
- The personal computer disrupted computation.
- The Internet disrupted communications.
- Blockchain disrupts storage.

Bitcoin

- The blockchain is the main innovation of Bitcoin
- A blockchain contains every transaction ever executed in the currency
- The network shares a transaction book (or public ledger)
- Double-spending of bitcoins impossible
- In order to add a new block to the Bitcoin blockchain, a Bitcoin “miner” must include a “proof of work”



Bitcoin

- The stack:
 - Blockchain (blocks maintained and replicated by thousands of nodes)
 - Protocol (designed and maintained by the open-source Bitcoin community or Ethereum or other community)
 - Token (what are you exchanging? money? cars? houses?)
 - Applications (wallets, services, etc)

Bitcoin issues

- A world currency administered not by a central bank but by
 - Developers, whose software determines how the currency is created and used
 - Miners, whose computers mint the currency

Bitcoin issues

- Bitcoin transactions take an average of ten minutes to be confirmed
- Scalability: capable of processing only seven transactions per second.
- Bitcoin runs on open source software

**MIT
Technology
Review**

Business

Bitcoin Transactions Get Stranded as Cryptocurrency Maxes Out

Bitcoin hit a capacity limit that could hamper dreams of it becoming widely used.

by Tom Simonite March 3, 2016

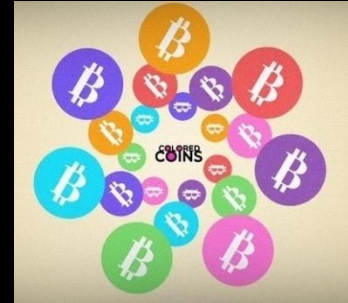
Bitcoin issues

- Solution: increase the block size - the Bitcoin XT fork (Mike Hearn and Gavin Andresen, 2014)... but all the computers on the bitcoin network must install a new version at the same time!
- Solution: SegWit optimization (Pieter Wuille, 2015, adopted 2016) that increases the volume of transactions fitting into a block without increasing the block size (1 Mbyte)
- Solution: 2 Mbyte block size (up from the original 1 Mbyte) + "segregated witness" code optimization – the Segwit2x fork (Jeff Garzik, 2017)



Alternative Cryptocurrencies

- “Colored” currencies: user-issued currencies running on the bitcoin protocol
- More than 70 in 2015
- Cryptsy, the largest altcoin exchange, lists hundreds of cryptocurrencies
- Omni/Mastercoin (JR Willett, 2013) uses the same blockchain as Bitcoin



Cryptsy Markets		
24 Hour Volume		
Display Markets: All BTC LTC		
Market	24hr Vol BTC	Price
LTC/BTC	243.59198824	0.01074350
DOGE/BTC	116.54566712	0.00000035
DASH/BTC	90.21066788	0.00601221
BTC/USD	79.00119318	413.53126891
ETH/BTC	61.66069621	0.00195472
LTC/USD	50.60971200	4.44000000
XRP/BTC	24.85799690	0.00001250
EAC/BTC	22.81309278	0.00000011
DGB/BTC	17.62607422	0.00000106

Alternative Cryptocurrencies

- Different “proof of work” algorithms than Bitcoin’s SHA-256 (hence do not use Bitcoin’s blockchain):
 - Litecoin (former Google engineer Charles Lee, 2011, second for market capitalization in 2015)
 - PPCoin/Peercoin (“Sunny King”, 2012) to replace mining with a less costly (“green”) alternative, which evolved into Primecoin (“Sunny King”, 2013)



Mining

- The process of adding transaction records to the public ledger
- “Proof of work”: a computing task that is costly to execute but easy to verify (SHA-256 computations)
- Bitcoin mining implements a distributed consensus system
- Custom-built supercomputers are needed for parallel processing



Mining

- Avalon (China, 2012): the first ASIC mining chip
- BitFury (San Francisco, 2011): 16nm “green” ASIC chip that can deliver 100 gigahash per second (2015)
- **21** (San Francisco, 2013): embeddable bitcoin mining chip (2013) and the first computer with native hardware and software support for Bitcoin (2015)



Mining

- 'Green' mining projects
 - Primecoin
 - Foldingcoin
 - Gridcoin
 - Zennet
- Cloud-based mining: Genesis



Bitcoin Banking

- Cook Investment Firm (Andrew Cook, Chile, 2011): world's largest bitcoin investment fund (he founded it when he was 20)
- Epiphyte (San Francisco, 2013): banking with crypto-currencies
- NextBank (2015): the first all-bitcoin institution



Bitcoin Payment

- Coinbase (San Francisco, 2012): bitcoin wallet
- Circle (Ireland, 2013): sending bitcoins to friends and family
- Quickcoin (San Francisco, 2014): a Facebook-Integrated bitcoin wallet to send bitcoins as messages

The Coinbase logo, featuring the word "coinbase" in white lowercase letters on a blue rectangular background.The QuickCoin logo, featuring a stylized "Q" icon inside a blue circle, followed by the word "QuickCoin" in white text on a blue rectangular background.

Bitcoin BTM

- CoinCloud (Menlo Park, 2014): trading bitcoins for cash



Life in the Bitcoin world

- Exchange dollars for bitcoins and viceversa: Coinbase (San Francisco), Gemini (New York)
- Personal wallet: software or hardware
- Software (“hot” wallet): Mycelium, Breadwallet, Copay.io and Jaxx.io
- Hardware: Keepkey, Trezor, Ledger
- Spend bitcoins, e.g. Purse.io that allows to buy Amazon goods



Blockchain Banking

- BitShares/ Invictus Innovations (Daniel Larimer, Virginia, 2013): financial services (including exchange and banking)
 - Based on blockchain but not the bitcoin blockchain



Blockchain goes mainstream

- 2017: Mastercard adopts blockchain technology for cross-border payments (no cryptocurrency though)
- 2017: IBM cross-border payments in the South Pacific (using Stellar's cryptocurrency Lumens)



Blockchain Non-Banking Applications

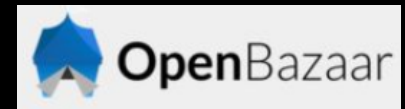
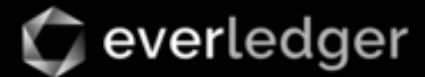
- Decentralised social messenger
Gems (Daniel Peled, Israel, 2014)
on bitcoin blockchain
- Supply chain finance app Skuchain
(Mountain View, 2014)



Blockchain applications

- Smart Property

- *Everledger* ledger tracks diamonds
- *Provenance.org* tracks supply chain authenticity
- *OpenBazaar* decentralized Craigslist exchange
- *Factom-HealthNautica* securing medical bills and claims



Blockchain applications

- Government
 - Identification documents
 - National ids
 - Visas
 - Voting registration
- Sidekik
 - On-demand tele-attorney
 - Private police
- Namecoin: decentralized DNS



Blockchain applications

- Physical and intellectual property can be registered and transacted via blockchains as *smart property*
- Nick Szabo (1997): any contract (even governance) can be implemented as self-executing *smart contracts*

Smart property = property whose ownership is controlled via the Bitcoin blockchain

Smart Contract = a program stored on the blockchain that can automatically execute the terms of a contract (Ripple Lab's Codius and Ethereum)

Smart Contracts

- Agreements between parties posted to the blockchain for automated execution
- Every contract in human societies can be reduced to a math problem
- Smart contracts model patterns of interaction in society



The world's first Blockchain marriage:
David Mondrus and Joyce Bayo (
October 5, 2014, Disney World)

Smart Contracts

- Notary Service to register documents
 - Proof of Existence (2014)
 - Factom (Texas, 2014)
 - Empowered Law (Chicago, 2015)

Proof of Existence



Smart Contracts

- Register and transact IP (intellectual property): Monegraph, Ascribe, ...
- Helping artists and writers protect their work from copyright infringement
- Easier than registering a work with the Library of Congress



Smart Contracts

- Music Industry
 - Blockchain can usher in a new era of digital rights management (DRM)
 - Blockchain can reinvent the music and media industry
 - No more piracy
 - Liberate musicians from music labels and streaming services



Smart Contracts

- Music Industry
 - PeerTracks: an “artist equity trading system”
 - Bittunes: an “independent music market”
 - Ujo Music: global royalty distribution and licensing



Smart Contracts

- Medical records
 - MedVault (2015): to record medical information on the bitcoin blockchain
 - Factom's partnership with medical services provider HealthNautica (2015)

**Medical Records Project
Wins Top Prize at Blockchain
Hackathon**

November 10, 2015

2015-04-23

**Factom's Latest
Partnership Takes on
US Healthcare**

Smart Contracts

- Medical records

Verifiable Data Audit

DeepMind's New Blockchain-Style System Will Track Health-Care Records

March 9, 2017

Alphabet's artificial intelligence outfit, DeepMind, plans to build a blockchain-style system that will carefully track how every shred of patient data is used.

Bitcoin 2.0

- Applications beyond fintech all the way to governance
- Any kind of peer-to-peer contract can be implemented as a secure and unbreakable blockchain application
- Computer algorithms can maintain order and trust without the need for a government



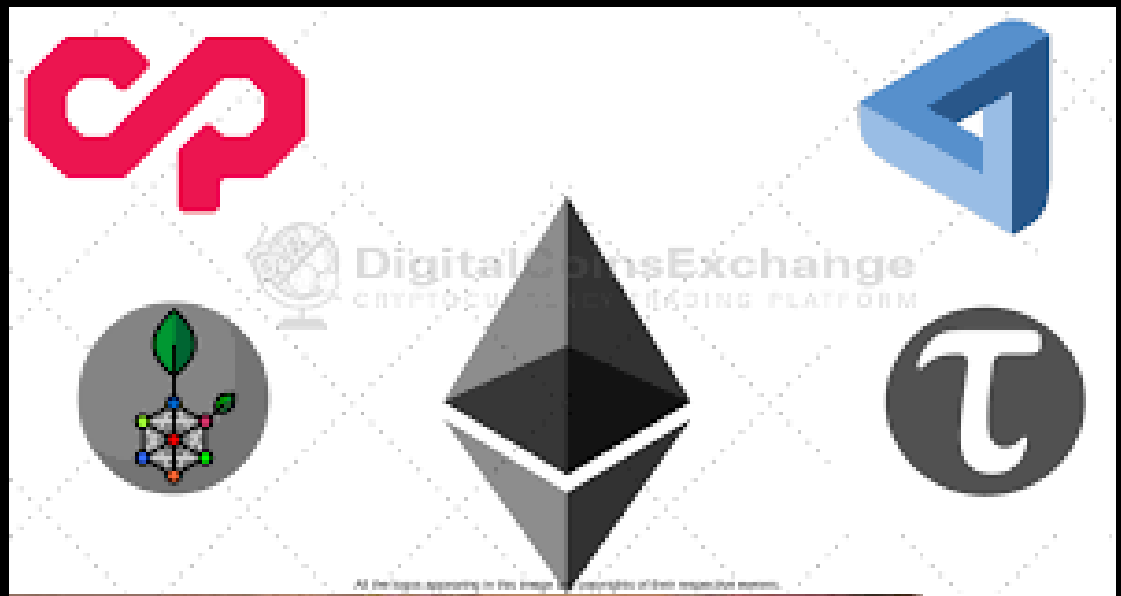
Bitcoin 2.0

- Filecoin (Juan Benet, 2017): earn filecoins for hosting files on your computer, e.g. for offering storage to those who need it



Bitcoin 2.0

- Bitcoin 2.0 technologies for developing decentralized applications (“app coins”):
 - Counterparty
 - Maidsafe
 - Ethereum
 - ...
 - Rootstock
 - Tauchain
 - ...





Bitcoin 2.0

- Ethereum (Vitalik Buterin, 2013)
 - A platform to develop Bitcoin-like "currencies"
 - A platform to develop secure digital contracts
 - A platform to develop decentralized applications
 - Optimized version of the blockchain to save storage space





Bitcoin 2.0

- Ethereum
 - Ethereum doesn't store massive data within the blockchain itself
 - It uses an additional component (originally Swarm, later cancelled, now IPFS)
 - Ethereum = Contracts (decentralized logic) + Swarm/IPFS (decentralized storage) + Whisper (decentralized messaging, under development)

Bitcoin 2.0



- Ethereum
 - InterPlanetary File System/IPFS (Juan Benet, 2015) for decentralized storage (not Swarm)
 - All data on IPFS are perpetually recorded online via P2P distribution
 - An encrypted address for each piece of information
 - A piece of information in IPFS cannot be manipulated
 - IPFS protocol replaces HTTP

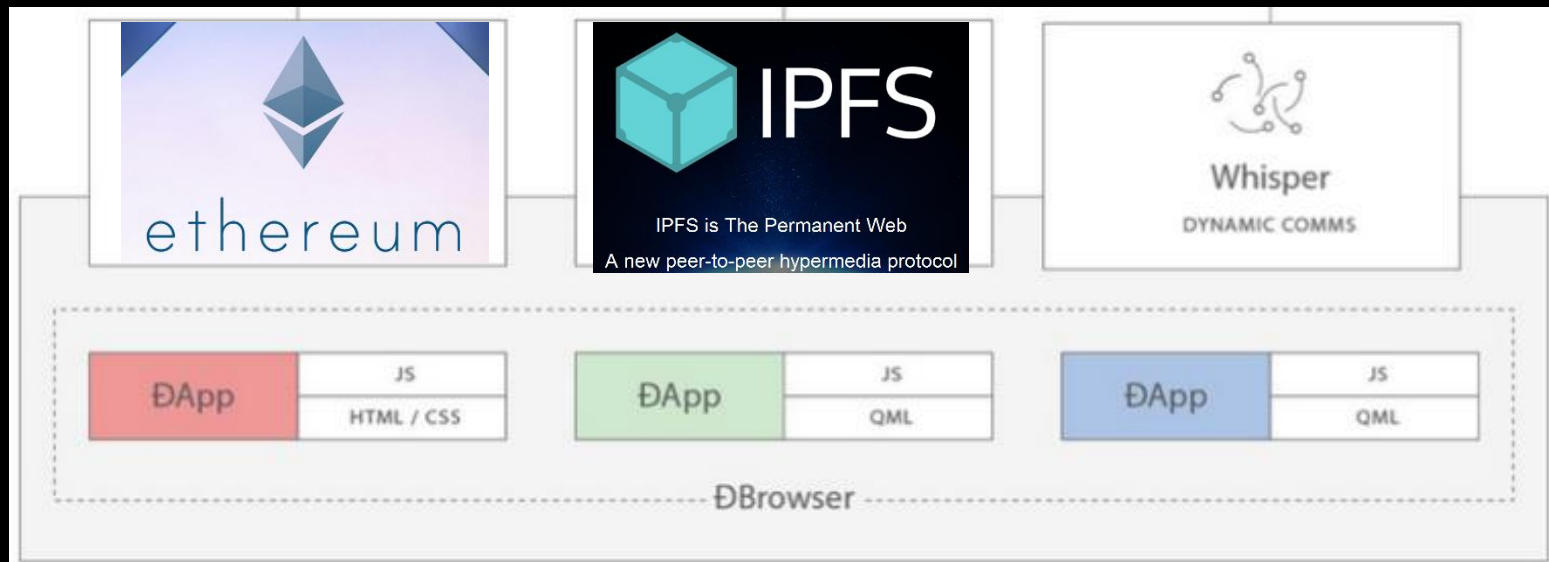


IPFS is The Permanent Web
A new peer-to-peer hypermedia protocol

Bitcoin 2.0



- Ethereum
 - Whisper (201?) for messaging



Bitcoin 2.0

- Ethereum
 - Ethereum is “Turing-complete” (it can implement any program)
 - Vision of Ethereum as the "world computer"
 - Most vulnerable to Ethereum: the intermediaries (Amazon, Uber, Airbnb...)



Bitcoin 2.0

Ethereum

- Criticism:
 - Ethereum not designed for distributed computing
 - Ethereum designed for consensus
 - The blockchain was designed to avoid cheating: it was not designed to be the backend of a distributed system

THE VERGE

Cryptocurrency faces political fight to clean up \$53 million theft

By [Russell Brandom](#) on June 21, 2016 07:53 am

Bitcoin 2.0

Ethereum

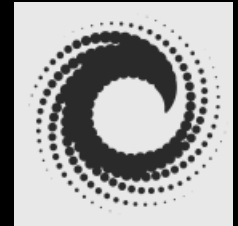
- United Nations helps refugees in Jordan with Ethereum (2017)



Bitcoin 2.0



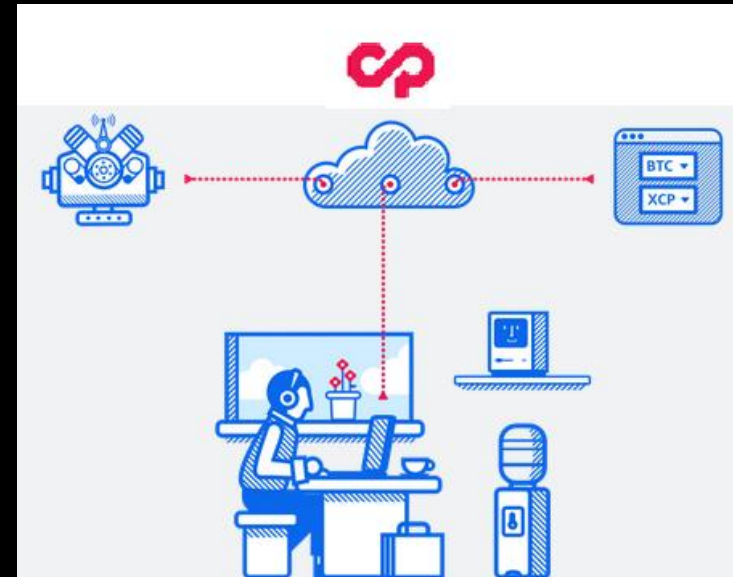
- Consensus Systems/ ConsenSys (Martin Koeppelmann and Joseph Lubin, New York, 2014)
 - Custom “decentralized applications” (dapps) for blockchain ecosystems on top of Ethereum
- Spritzle/HitFin (Nathalie & Patrick Salami, San Mateo, 2015)
 - Ethereum-based platform for trading derivatives



Bitcoin 2.0



- Counterparty (Chris DeRose, 2014)
 - A platform to foster the creation of P2P financial apps on the blockchain
 - E.g., users can create their own currency and set up exchanges of digital currencies
 - Adds information to blockchain transactions



Bitcoin 2.0

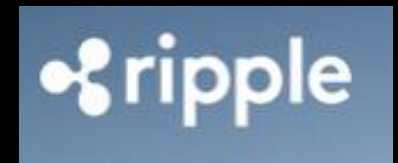


- Swarm (Joel Dietz, Palo Alto, 2014): an incubator of Counterparty projects; a platform for launching Counterparty projects and the initial mentorship and funding; a crowdfunding platform for creating decentralized apps
- Storj (Shawn Wilkinson, Georgia, 2014), a distributed peer-to-peer encrypted cloud storage (similar to Dropbox but distributed, like Swarm/IPFS but running on Counterparty instead of Ethereum)



Bitcoin 2.0

- Counterpart uses the bitcoin blockchain
- Ethereum uses a non-bitcoin blockchain
- Non-blockchain consensus: Ripple
- Ripple (2013): secure and instant global financial transactions with no chargebacks (2016: third-largest cryptocurrency by market capitalization after bitcoin and ethereum) - based on a trust graph, not a blockchain



Bitcoin 2.0

- Other platforms for easy decentralization of applications:
- Eris (New York, 2014)
 - Founded by two lawyers, Preston Byrne & Casey Kuhlman
 - A universal blockchain platform
 - It can clone Ethereum, Bitcoin and many other blockchains
 - A blockchain is a database, and each user should have its own
 - Uses IPFS for storage



Bitcoin 2.0

- Other platforms for easy decentralization of applications:
 - Ripple's Codius (San Francisco, 2013)
 - non blockchain
 - Etherparty (Los Angeles, 2015): cloud-based, no programming required (runs on Ethereum)



DLTs

- Beyond the Bitcoin blockchain
- Beyond the blockchain

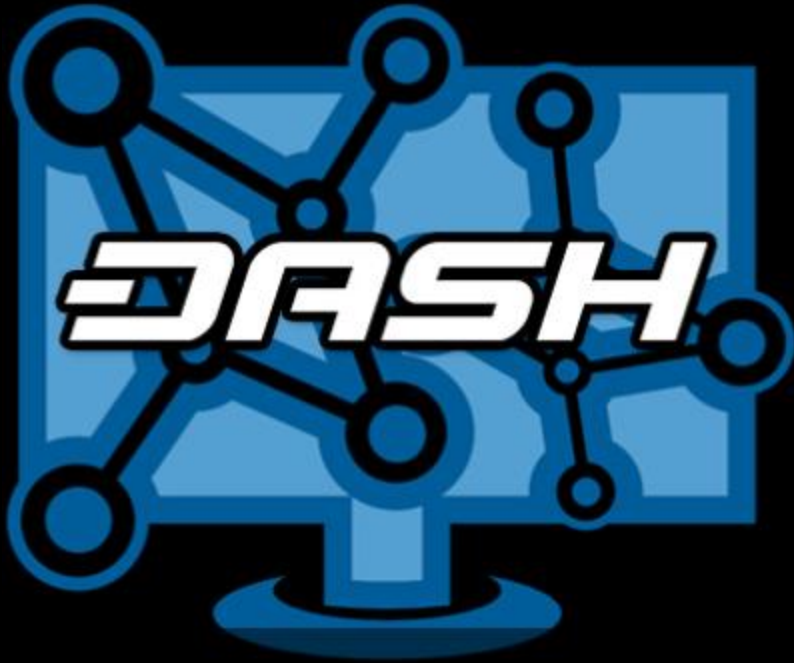
DLTs

- 2014: Evan Duffield's Xcoin/Dash
- faster than Bitcoin and has lower fees than Bitcoin
- built-in governance via a second-tier network ("masternodes")
- 2015: the first decentralized governance system, the Dash Budget System



Dash Announces New Blockchain Research Lab at Arizona State University

Posted by Joël Valenzuela | Aug 18, 2017 | News | ★★★★★



DLTs

- 2013: BCNNext's NXT
 - "proof of stake" method instead of the "proof of work" method
 - no mining
 - a platform to build financial applications
-
- 2015: NEM
 - "proof of importance" method (PhD thesis of Makoto Takemiya)
 - Eigentrust reputation system (Sep Kamvar, Mario Schlosser & Hector Garcia-Molina at Stanford)



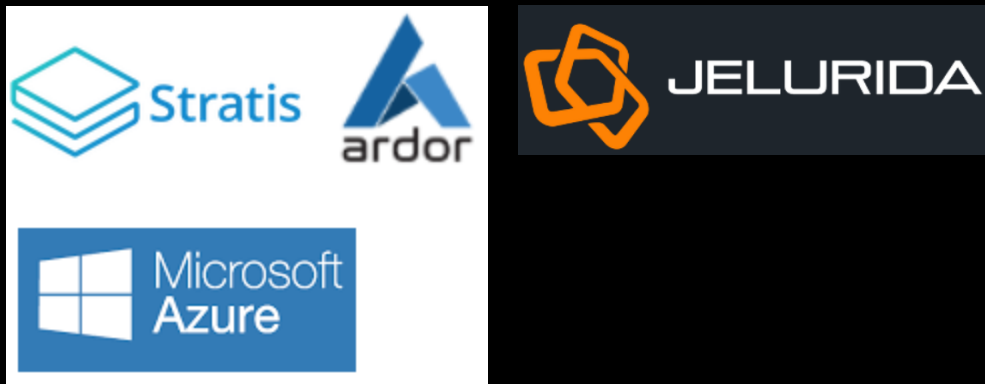
DLTs

- 2017: Arthur & Kathleen Breitman's Tezos
- Democracy on the blockchain: each token is a vote
- "proof of stake" method but even that can be subject to a democratic vote



Blockchain-as-a-service

- Azure by Microsoft
- Ardor by Jelurida, founded by Petko Petkov (a core developer of NXT) and Lior Yaffe
- Stratis, founded in 2016 in Philadelphia.



DLTs

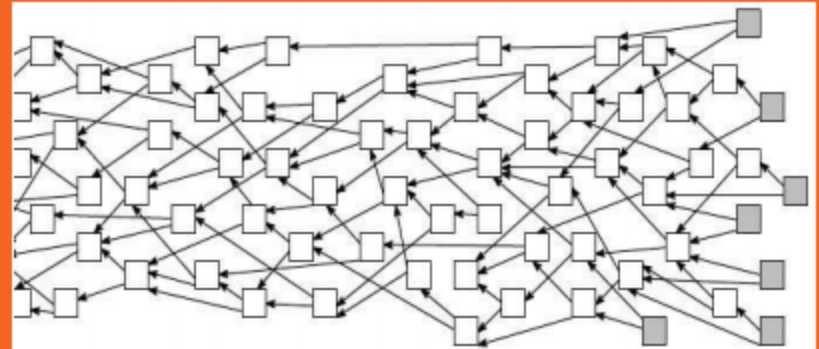
- Blockchain vs DAG

DISTRIBUTED LEDGERS

BLOCKCHAIN



DAG



DLTs

- Iota, designed for micro-transactions (Serguei Popov et al)
- A "directed acyclic graph" (or DAG), known as a "tangle", instead of a blockchain
-
- 2015: Sergio Demian Lerner's DagCoin
- replaces blocks with DAGs
- each user that transacts becomes automatically a miner



The tangle

Serguei Popov*, for Jinn Labs

April 3, 2016. Version 0.6



DAGCOIN®

DLT development

Most important ready-to-go DLTs cores

	Bitcoin Core	Graphene	Scorex	Tendermint	Ripple / Stellar
Language	C/C++	C++	Scala	Go	C++
Consensus	PoW	dPoS	PoW, 2x PoS	PoS	
Blockchains	Bitcoin, Dash, Litecoin, ...	BitShares, Steem, Golos	– (Waves experiments)	Cosmos (under dev)	Ripple, Stellar, Infra (e-Auction)
“+”	Most proved	Blazingly fast	Modular	PoS	Fast & proved
“_”	Hard to understand	Complex model	Limited functionality, no real-world impl	Immature	Complex model

DLT development

- Meta-languages for smart contracts
 - Solidity
 - Serpent
 - Viper

Dapps

- The smart contract is the simplest form of decentralized automation
- Decentralized Application: a smart contract with an unlimited number of participants (e.g., Tor, BitTorrent, MaidSafe)
- Decentralized Applications are smart contracts
- No server: the blockchain serves as the "backend"
- No centralized intermediary



Beyond the Internet

- MaidSafe (David Irvine, Britain, 2006)
 - To decentralize the Internet leveraging the enormous amount of unused hard-disk space that exists around the world combined with peer-to-peer protocols and encryption
 - No central servers, no central databases



- MaidSafe
 - MAID (Massive Array of Independent Disks)
SAFE (Secure Access For Everyone)
 - Data are shredded and heavily encrypted, and the encrypted chunks are randomly distributed around the world
 - Only the owner can reassemble and decrypt these chunks
 - No blockchain: not a "proof of work" ("mining") algorithm but a "proof of resource" mechanism
 - Transactions are not stored in a blockchain: no traces of that transaction exist except with the two parties involved

Beyond the Internet



- MaidSafe
 - MaidSafe rewrites the Internet
 - SafeNet: a Tor-like platform that decentralizes all the services currently available on the Internet (messaging, email, social networks, data storage, video conferencing, etc); i.e. it makes them work without any need for servers and databases
 - The final solution to the problems of identity theft and surveillance

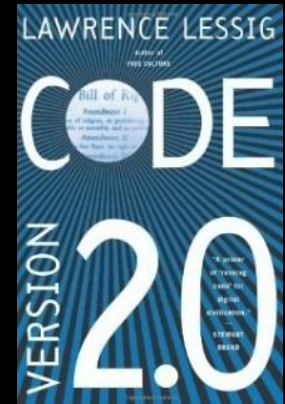
Beyond the Internet



- MaidSafe
 - A P2P-based system for storage and routing
 - Decentralized storage a` la Storj: "farmers" offer spare storage to the network
 - A crowd-sourced Internet
 - A browser that lets people browse HTML pages securely and anonymously
 - The user can log into any computer of the network and the computer becomes "her" computer: her data, her applications, her profile.
 - When she logs out, no trace of her work is left behind.

Smart Law

- The traditional world: legally-binding
 - Flexible interpretation of the law, rhetorical power of attorneys
- The blockchain world: technologically-binding
 - Software inexorably executes the contract no matter what
- Auto-executing code replaces lawyers, courtrooms, judges and prisons
- No need for a legal system if the world moves to smart contracts



Initial Coin Offerings

- 2014: First ICO (Karmacoin)
- 2017: Filecoin's record ICO
- 2017: China bans ICOs



\$257 Million: Filecoin Breaks All-Time Record for ICO Funding

Sep 7, 2017 at 20:45 UTC by Stan Higgins

Bloomberg Technology

Bitcoin Tumbles as PBOC Declares Initial Coin Offerings Illegal

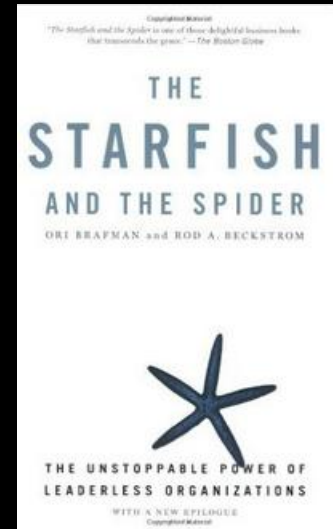
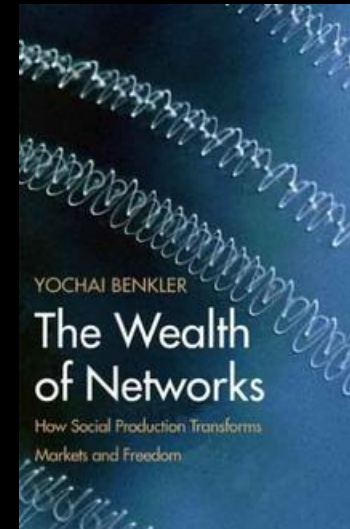
By Lulu Yilun Chen and Justina Lee

September 4, 2017, 12:17 AM PDT

China PBOC says all ICOs must be stopped and refunds provided

Governance 2.0

- DAOs (Decentralized Autonomous Organizations)
 - An unmanned organization under the control of an incorruptible algorithm
 - The algorithm is, in turn, a publicly auditable open-source software
 - DAOs are autonomous
 - DAOs are self-enforcing
 - DAOs have no central control



Governance 2.0

- Bitnation (Susanne Tarkowski Tempelhof, 2014)
 - a platform to create DAOs
 - *"Create Your Own Nation In 140 Lines Of Code"*
 - does not involve central authorities
 - a collaborative platform for DIY government
 - provides the same services that traditional governments provide, but in a decentralized way



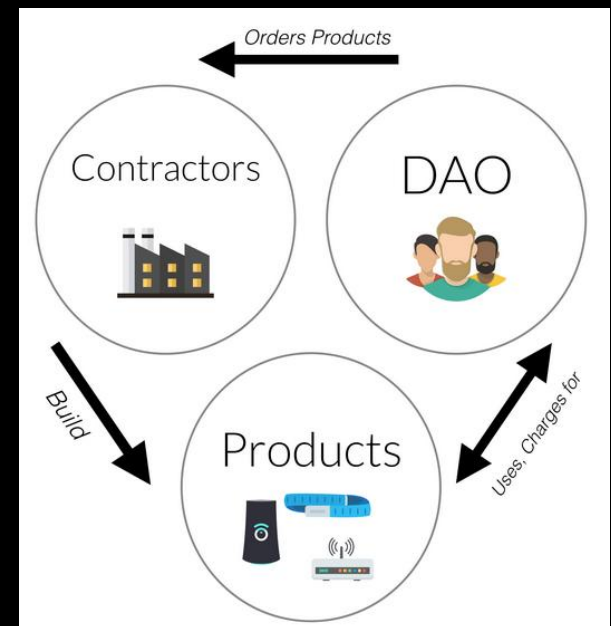
<https://bitnation.co>

CREATE YOUR OWN NATION IN 140 LINES OF CODE

Governance 2.0

- DAO (Slock.it, 2016)
 - the DAO raises the equivalent of \$150m to invest in startups
 - 14% of all ether ever issued on Ethereum
 - Largest crowdfunding project of all times

Slock.it



Governance 2.0

- Distributed Collaborative Organizations
 - 2014: Primavera De Filippi (Harvard Univ) and Housman Shadab (New York Law of School) invented an LLC-like organization for blockchain organizations
 - Integration of blockchain-based distributed organizations (DAOs) with the existing legal system



Governance 2.0

Blockchain Is Helping to Build a New Kind of Energy Grid

Using the technology behind Bitcoin, participants in the Brooklyn Microgrid are buying and selling locally generated renewable energy over a peer-to-peer network.

April 19, 2017



BROOKLYN
MICROGRID

How Blockchain Can Bring Financial Services to the Poor

A project from the Bill & Melinda Gates Foundation aims to use distributed ledger technology to help the two billion people worldwide who lack bank accounts.

April 18, 2017

BILL & MELINDA
GATES foundation

Identity

- A new breed of apps and services will grow on top of a cross-chain system of decentralized identifiers linked to identity hubs encoded with semantic data

China

- A national priority (13th Five-Year National Informatization Plan, 2015)

Futurism

NEWS

INFOGRAPHICS

VIDEOS



China to Start Using Blockchain to Collect Taxes and Send Invoices



coindesk

China's Central Bank is Testing a Blockchain-Backed Digital Currency

Jan 26, 2017 at 04:20 UTC by Pete Rizzo

Blockchain Ecosystem in 2017



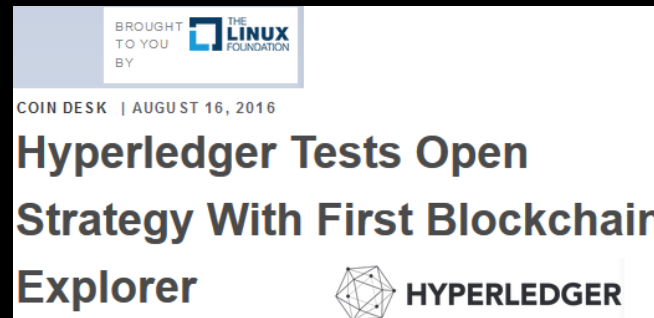
<https://techcrunch.com/2017/10/16/mapping-the-blockchain-project-ecosystem/>

BLOCKCHAIN PROJECT ECOSYSTEM



Blockchain education

- Blockchain University (Mountain View, 2014)
- Institute for Blockchain Studies (Melanie Swan, 2014)
- Hyperledger Project (Linux Foundation, 2016): a joint effort to advance blockchain technology (IBM, Accenture, Intel, Fujitsu, Hitachi, etc)
- The technology is almost entirely open-source



Blockchain education

- 2016: \$1 billion invested by Wall Street



June 23, 2016 :

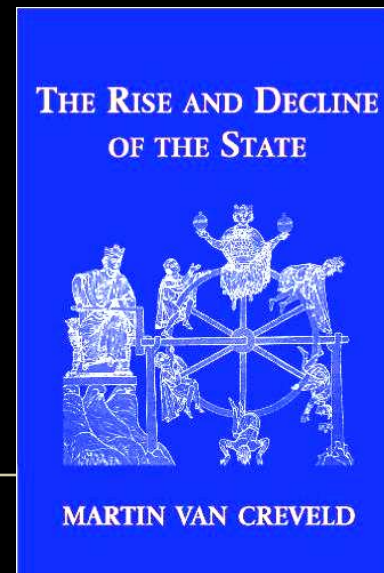
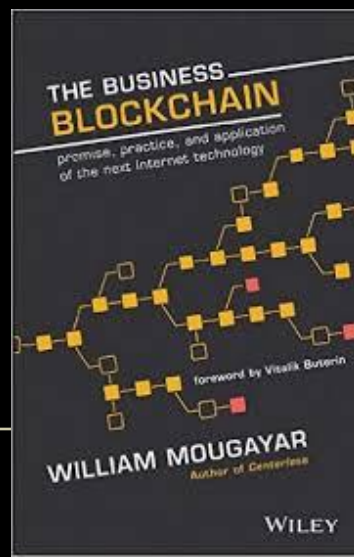
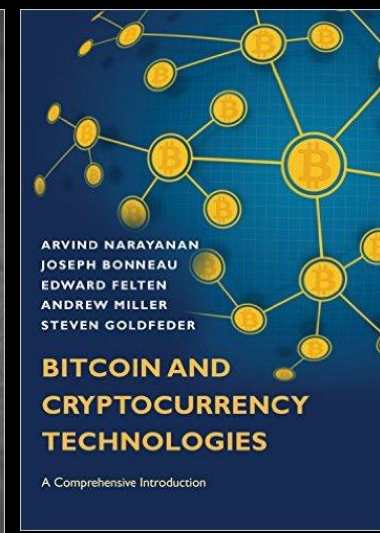
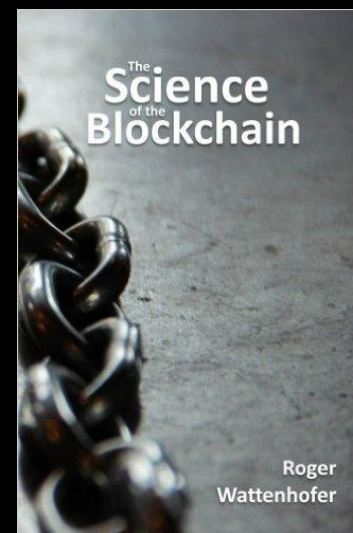
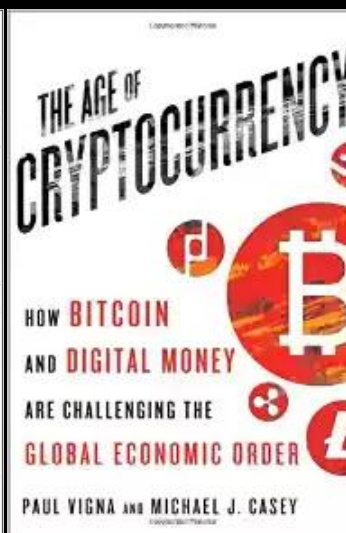
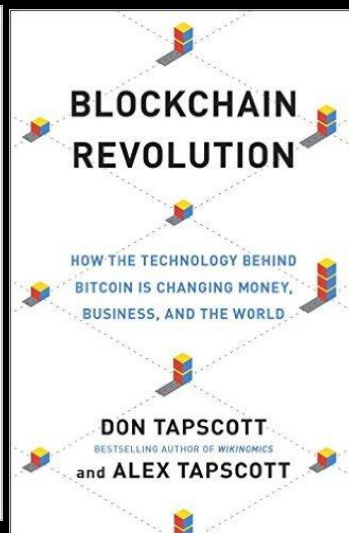
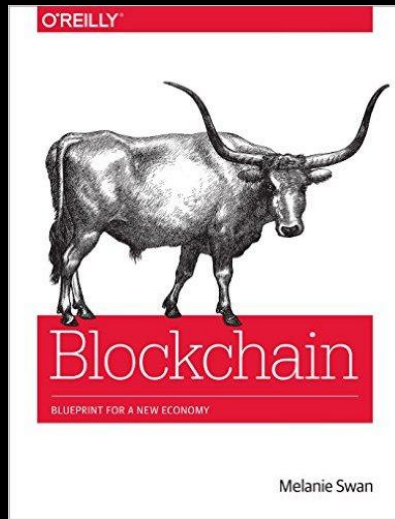
Wall Street Blockchain Investments
Top \$1Billion Annually

Blockchain art



'Satoshi Creator of Blockchain' artwork for Spells of Genesis, by Yodark

Bibliography



Contact

- www.scaruffi.com

