



National Research University Higher School of Economics



The Modern Blockchain Ecosystem



Sergey Avdoshin

**Head of Software Engineering School
Computer Science Faculty**

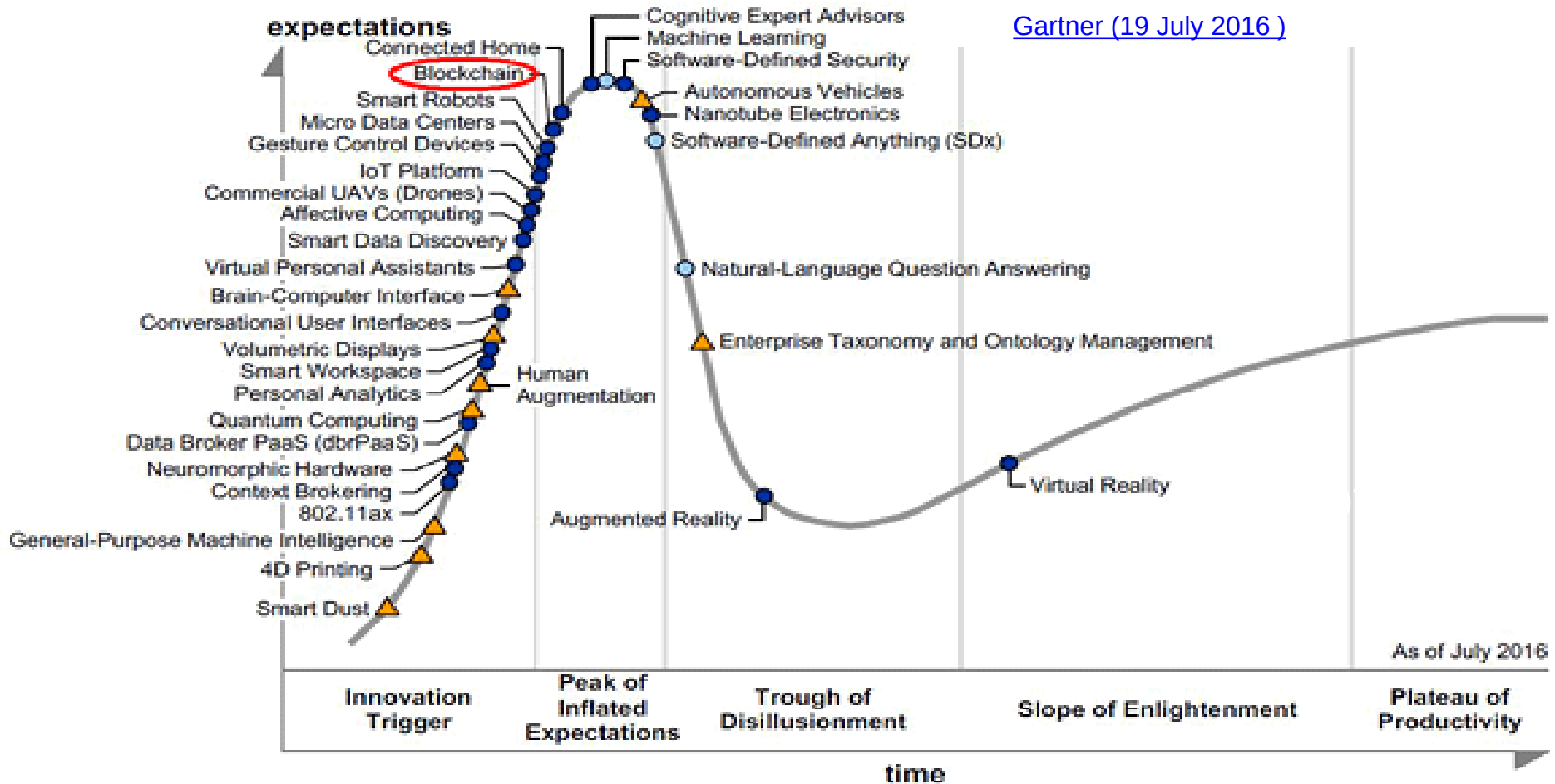


Media



Hype Cycle for Emerging Technologies

[Gartner \(19 July 2016\)](#)



Years to mainstream adoption:

○ less than 2 years

● 2 to 5 years

● 5 to 10 years

▲ more than 10 years

⊗ obsolete

⊗ before plateau



Definitions

A **blockchain** is a type of distributed ledger, comprised of unchangeable, digitally recorded data in packages called blocks (rather like collating them on to a single sheet of paper). Each block is then 'chained' to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions.

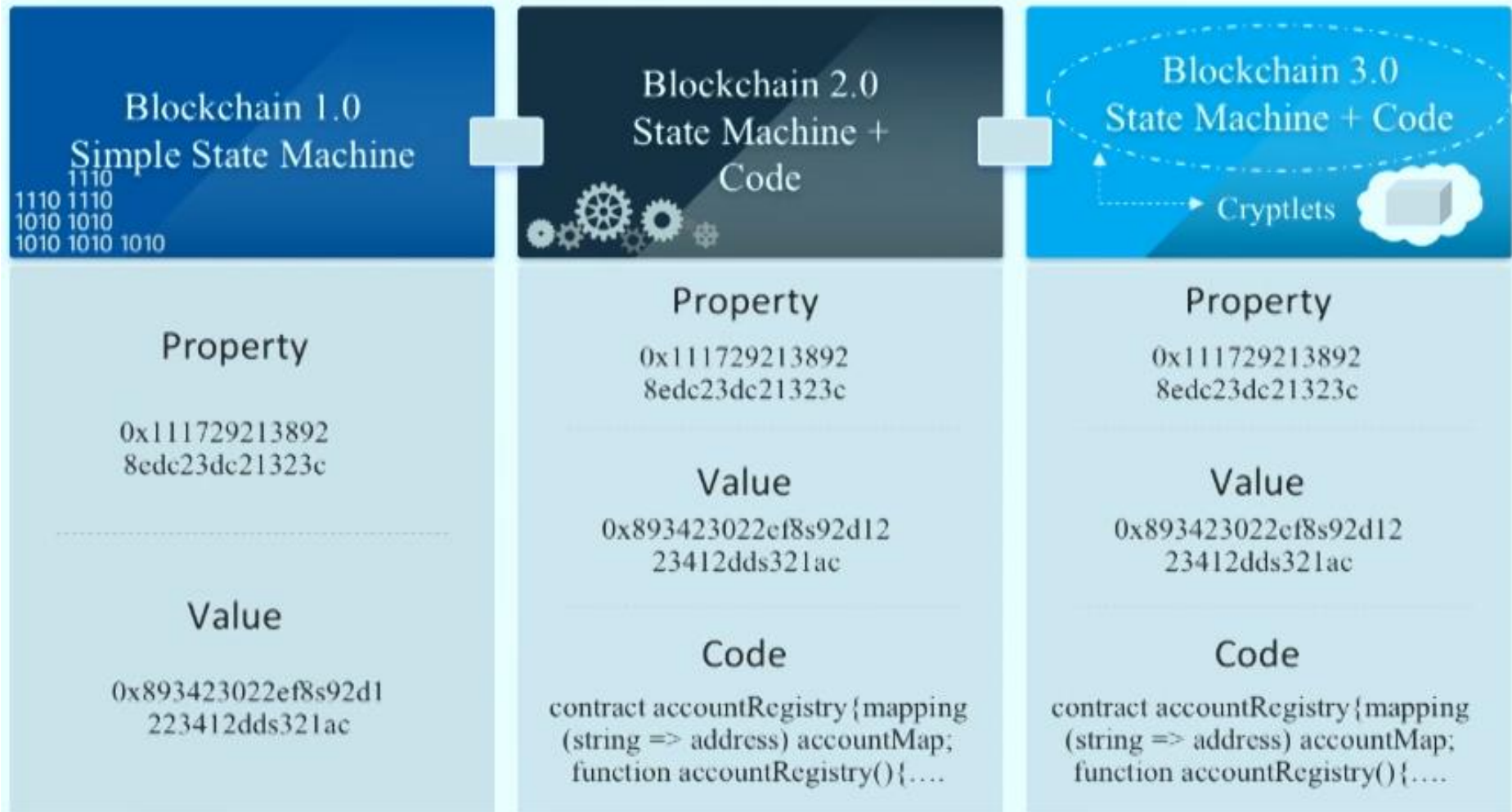
[Blockchain Glossary](#)

Блокчейн – это многофункциональная и многоуровневая информационная технология, предназначенная для надежного учета различных активов.

[Melanie Swan. Blockchain: Blueprint for a New Economy.](#)

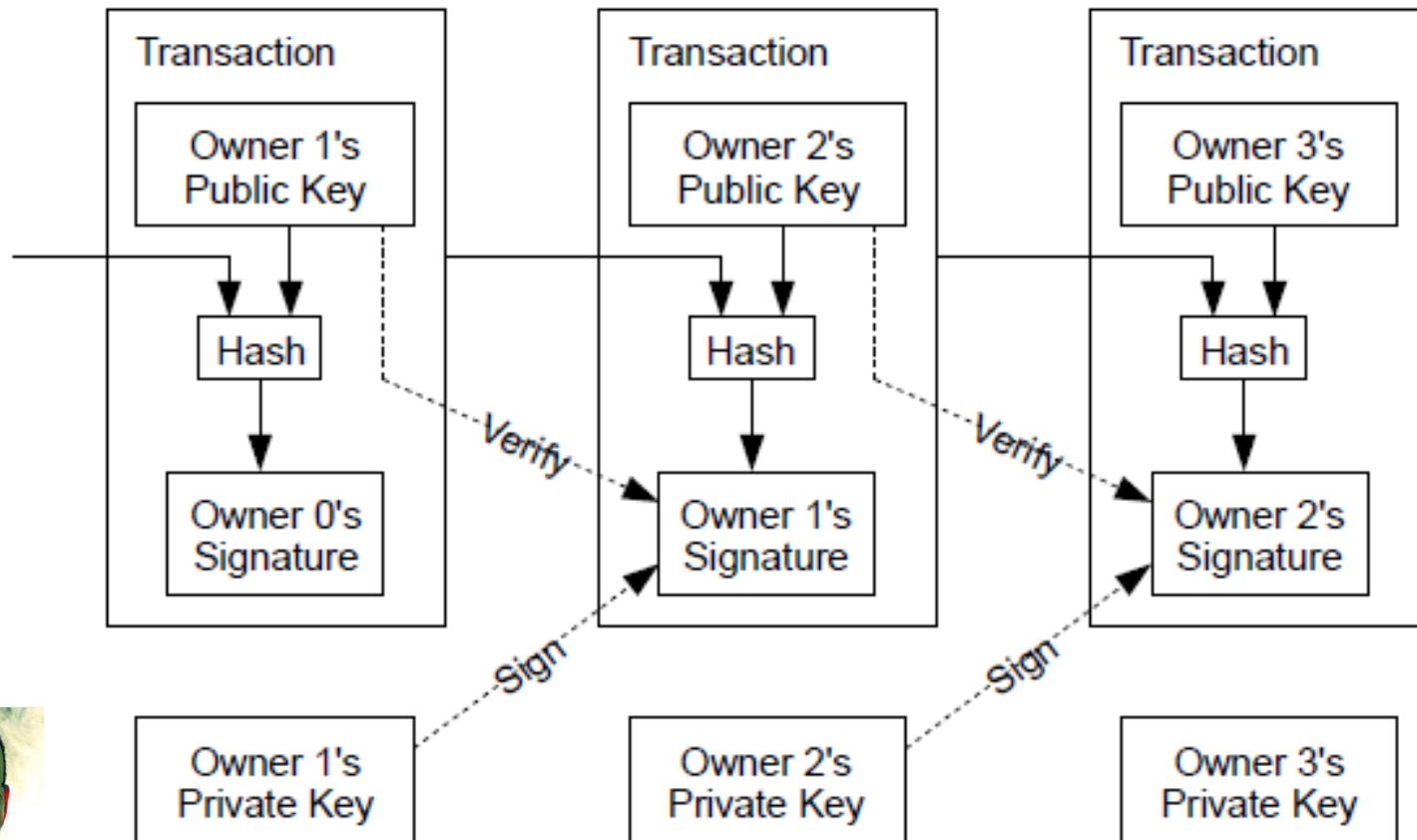


Blockchain Evolution





Transactions



[Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 31.10.2008](#)



A Chain of Transactions

Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18

INPUTS From		OUTPUTS To	
From (previous transactions Joe has received):		Output #0 Alice's Address	0.1000 BTC (spent)
Joe	0.1005 BTC	Transaction Fees:	0.0005 BTC

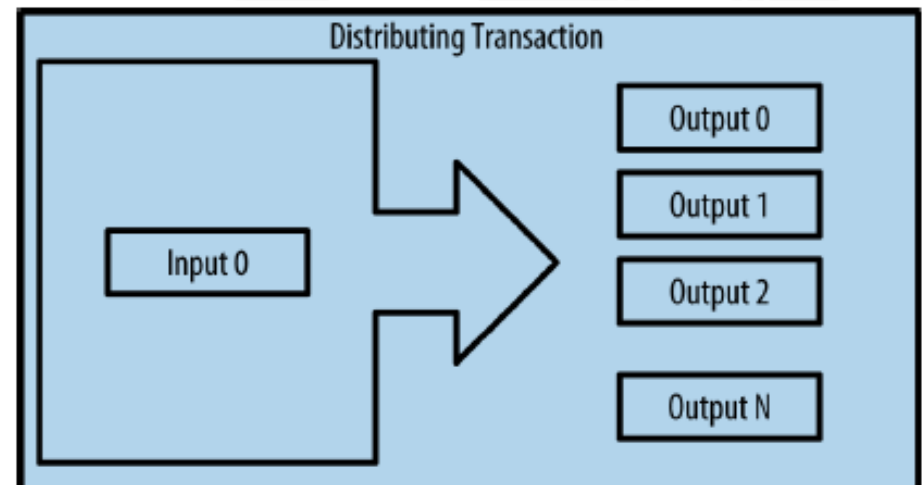
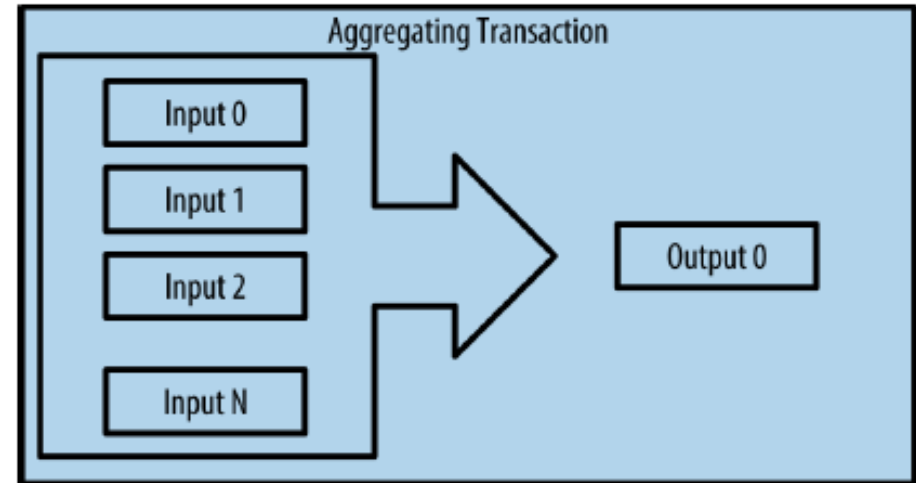
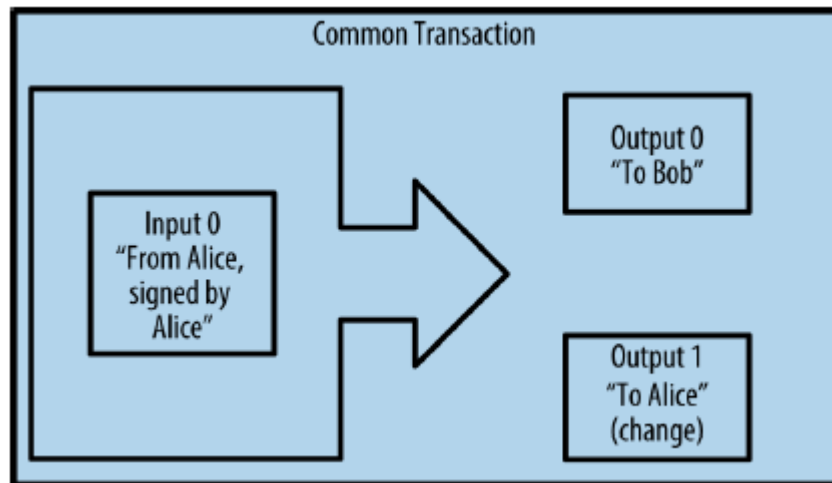
Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

INPUTS From		OUTPUTS To	
7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0		Output #0 Bob's Address	0.0150 BTC (spent)
Alice	0.1000 BTC	Output #1 Alice's Address (change)	0.0845 BTC (unspent)
		Transaction Fees:	0.0005 BTC

Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4

INPUTS From		OUTPUTS To	
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0		Output #0 Gopesh's Address	0.0100 BTC (unspent)
Bob	0.0150 BTC	Output #1 Bob's Address (change)	0.0045 BTC (unspent)
		Transaction Fees:	0.0005 BTC

Transaction Forms





Blocks Linked in a Chain

Size	Field	Description
4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header
1-9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

The Structure of a Block

Block Height 277314

Header Hash:

0000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249

Previous Block Header Hash:

0000000000000038388d97cc6f2c1d
fe116c5e879330232f3bff1c645920bdf

Timestamp: 2013-12-27 22:55:40

Difficulty: 1180923195.26

Nonce: 3797028665

Merkle Root: 02327049330a25d4d17e53e79f
478cbb79c53a509679b1d8a1505c5697afb326

Transactions

Block Height 277315

Header Hash:

000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569

Previous Block Header Hash:

0000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249

Timestamp: 2013-12-27 22:57:18

Difficulty: 1180923195.26

Nonce: 4215469401

Merkle Root: 5e049f4030e0ab2debb92378f5
3c0a6e09548aea083f3ab25e1d94ea1155e29d

Transactions

Block Height 277316

Header Hash:

000000000000001b6b9a13b095e96db
41c4a928b97ef2d944a9b31b2cc7bdc4

Previous Block Header Hash:

000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569

Timestamp: 2013-12-27 23:11:54

Difficulty: 1180923195.26

Nonce: 924591752

Merkle Root: c91c008c26e50763e9f548bb8b2
fc323735f73577effbc55502c51eb4cc7cf2e

Transactions



The Structure of the Block Header

Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Difficulty Target	The proof-of-work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the proof-of-work algorithm

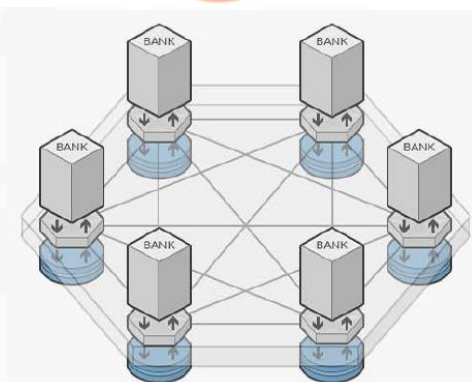
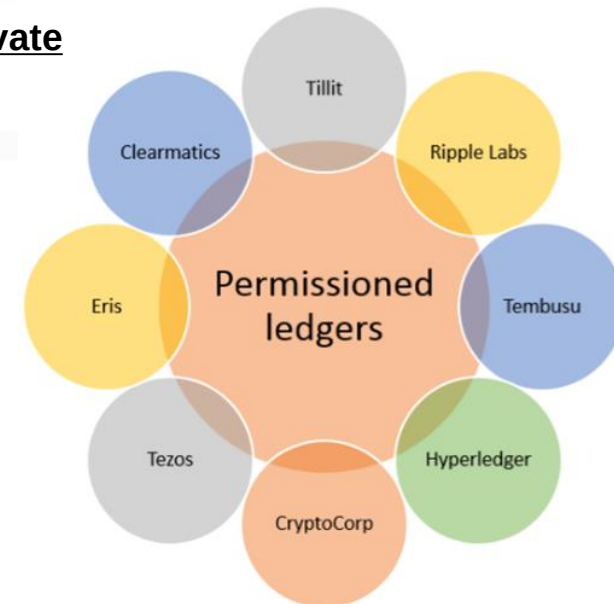
Distributed Ledger Taxonomy



**Unpermissioned Public
shared ledger
= The Internet**

**Permissioned Private
shared ledger
= An Intranet**

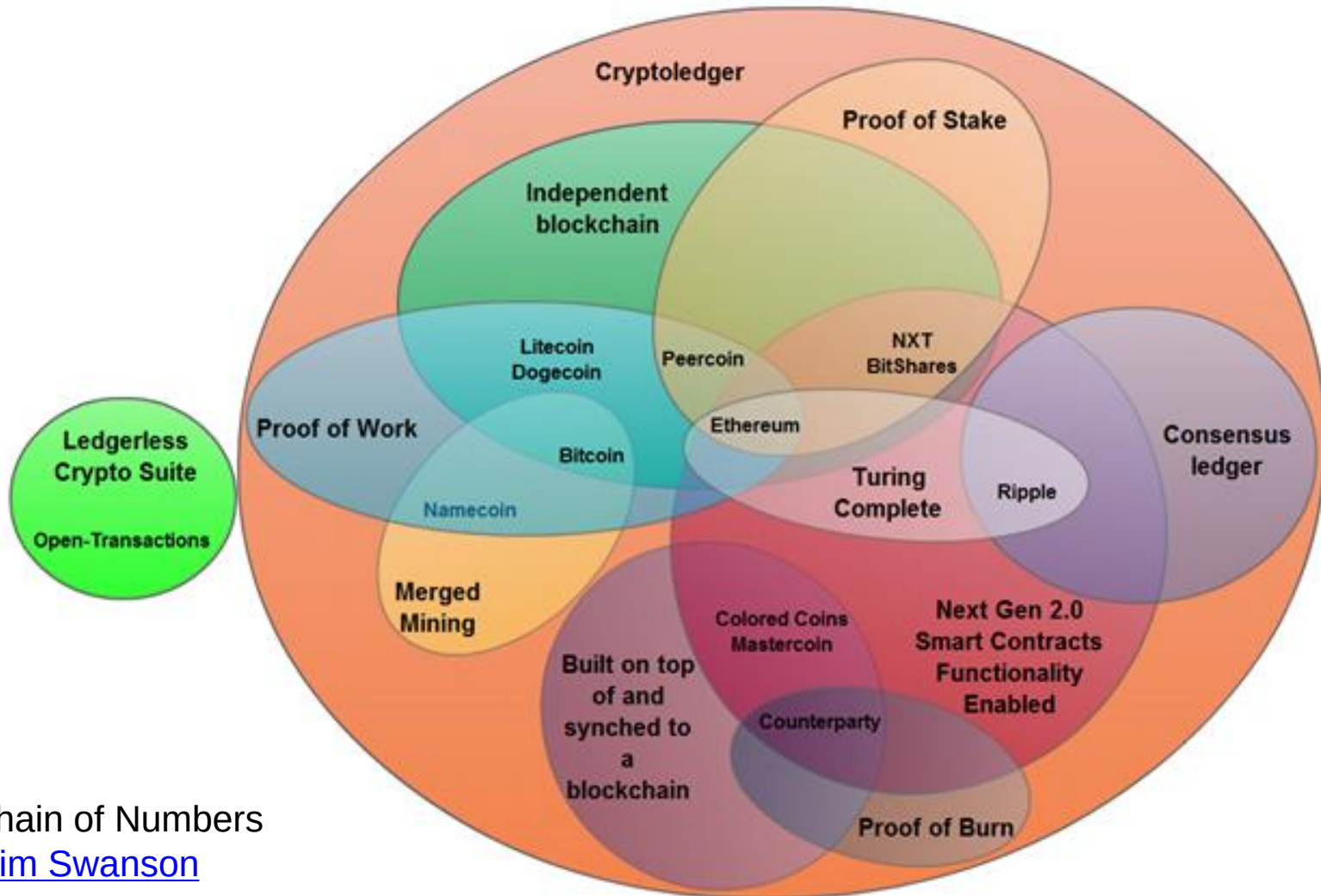
**Hybrid
permissioned public
shared ledger
= Syndicate**



Decentralised Clearing and Settlement with
HYPERLEDGER

[Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. By Tim Swanson Published: 06.04.2015](#)

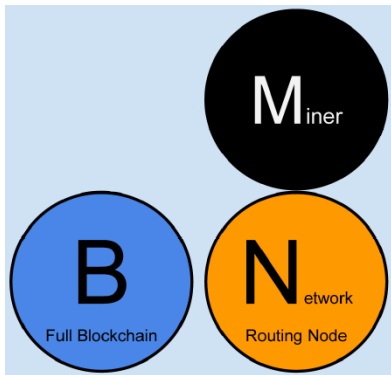
Current Cryptoprotocol Infrastructure



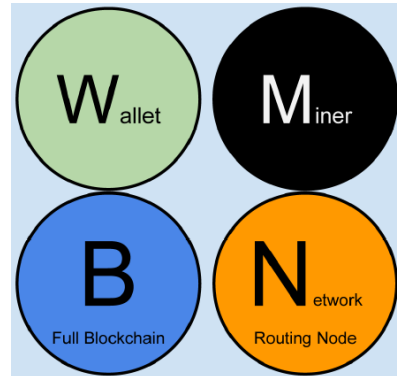
Great Chain of Numbers
by [Tim Swanson](#)



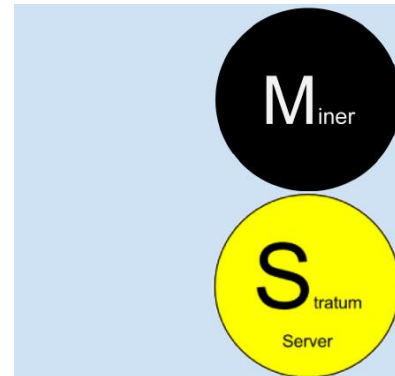
Nodes Types on the Extended Bitcoin Network



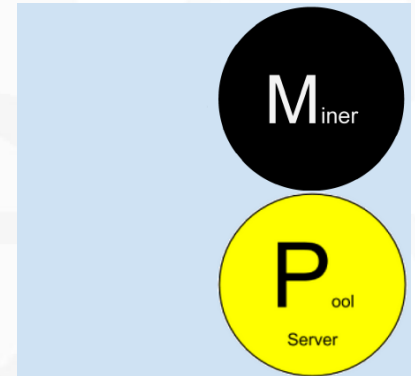
Solo Miner



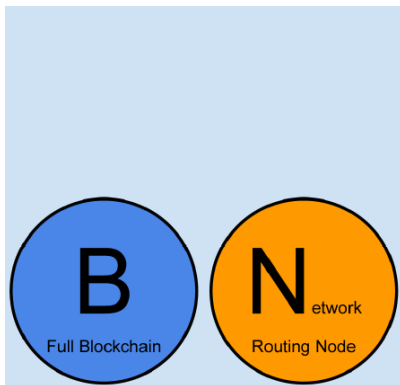
*Reference Client
(Bitcoin Core)*



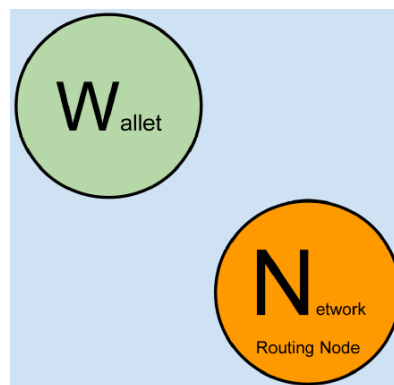
Stratum Node



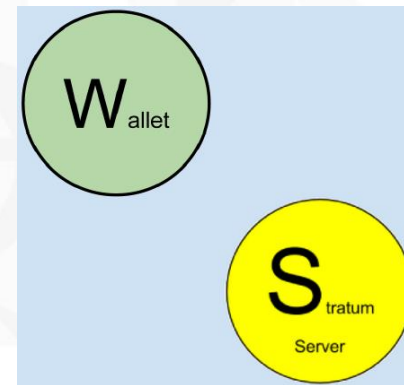
Pool Mining Node



Full Block Chain Node



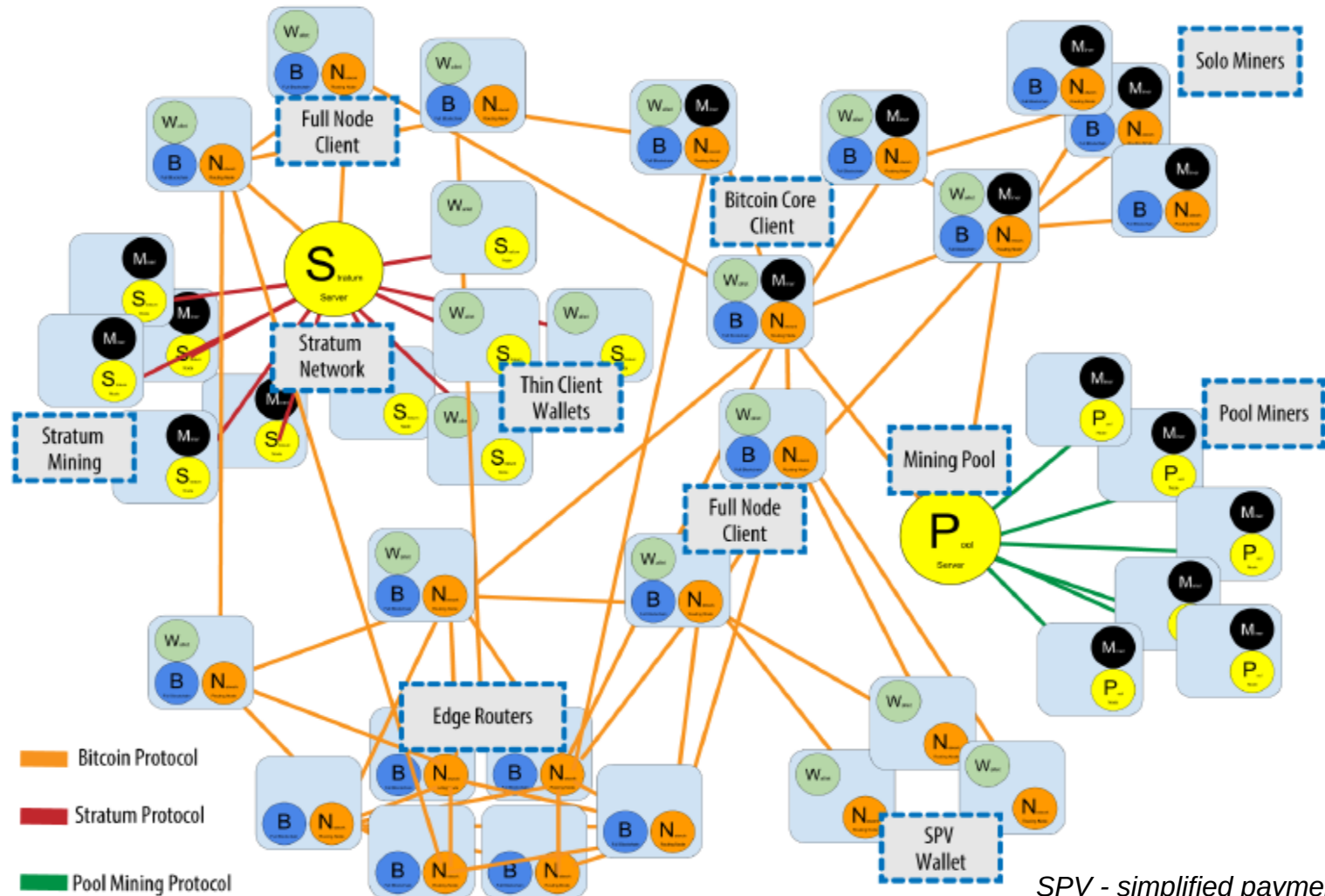
Lightweight Wallet



Lightweight Stratum Wallet



The Extended Bitcoin Network



SPV - simplified payment verification

Bitcoin Nodes

1	US	8705
2	Germany	3476
3	Unknown	2697
4	UK	1859
5	China	1849
6	RF	1574
7	Canada	971
8	France	912
9	Netherlands	853
10	Japan	663
11	Australia	562
12	Ukraine	545
13	Italy	472
14	Sweden	446
15	Switzerland	406
...	Other	6618



The map shows concentration of **32608 Bitcoin Nodes**





Mining

«Bitcoin opens up an entire world of opportunities. We are just now starting to realize how impactful this can be and we are very excited about the future».

Marco Streng
CEO, Genesis Mining





Wallets

«At Coinbase, we are excited about the progress made thus far but we are still in the early days of the technology and even more excited about the app ecosystem and what the future of Bitcoin applications will look like».



Adam White
VP of Business Development,
[coinbase](https://www.coinbase.com)





Choose your Wallet



WEB WALLETS

Simplest and most convenient to use, but your private key data is handled by a third party, which can be risky.

Most-trusted Web wallets: Coinbase, My Wallet (Blockchain), Strongcoin.



DESKTOP WALLETS

They do not depend on a third-party service – but they can be spied upon by malware. You can access them only on your desktop or laptop.

Most-trusted desktop wallets: Hive, Bitcoin Core, MultiBit, Armory.



MOBILE WALLETS

Mobile and easy to use for on-site purchases. But they rely on the Internet and cell network – and some of them transfer data through third parties.

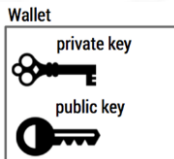
Most-trusted mobile wallets: Mycelium, Blockchain, and Bitcoin wallet



HARDWARE WALLETS

They are the most secure because they are offline. For a comparison, think of them as an offline safe.

Popular Bitcoin client with cold storage: Armory





Choose your Wallet



**Bitcoin
Core**



**Bitcoin
Knots**



Copay



Airbitz



GreenBits



Mycelium



BitGo



**Green
Address**



Coinomi



Coin.Space



**Simple
Bitcoin**



MultiBit HD

Wallet





Hardware & Storage

«Bitcoin paved the way to decentralized security, and will jumpstart the usage of personal privacy devices».

[Eric Larcheveque](#)

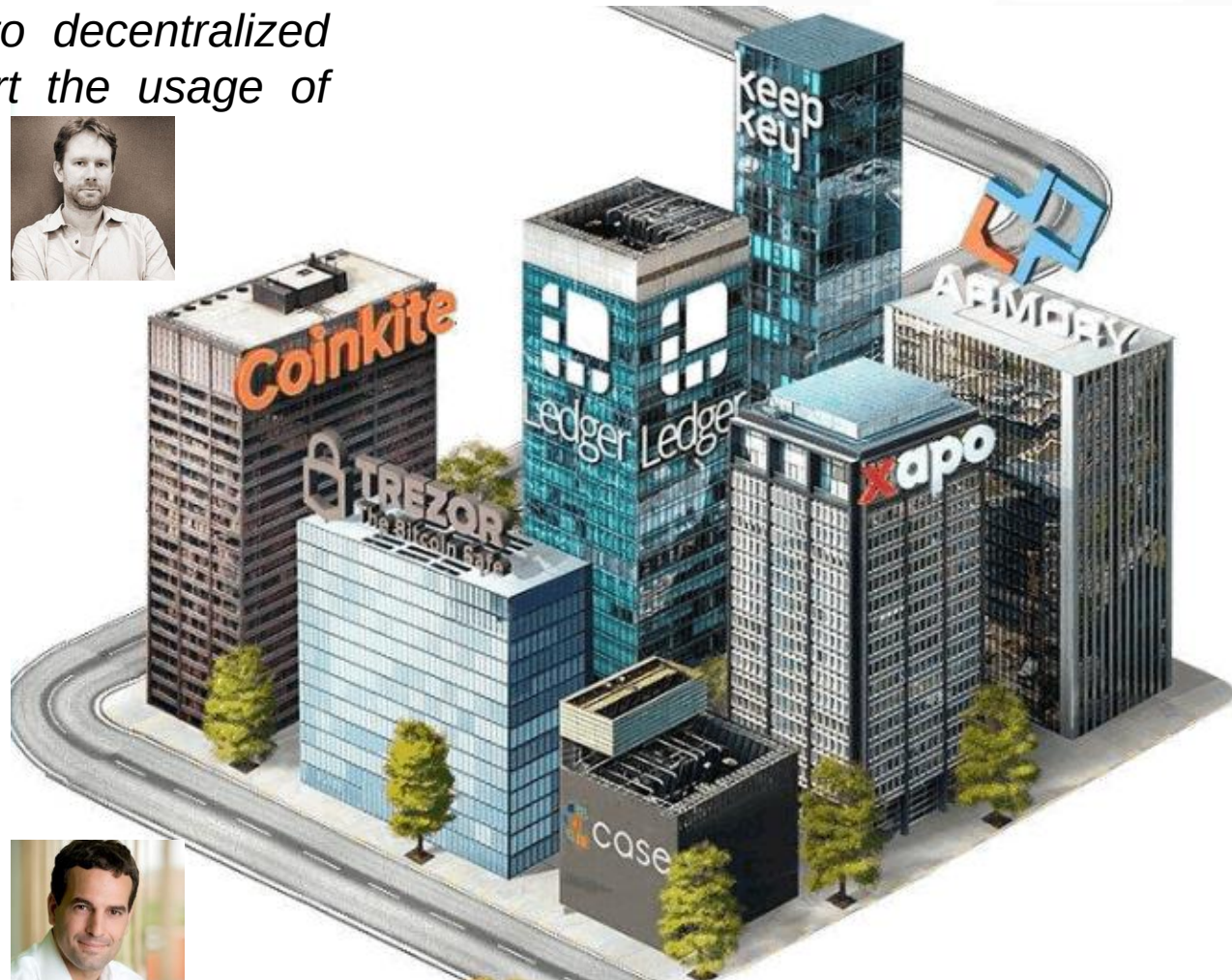
CEO, [Ledger](#)



«Today there are more than 100,000 Bitcoin transactions per day for more than \$100 million and there are more than 5,000 servers acting as nodes of network: Bitcoin is a lot less likely to disappear today than it was 2 years ago when the price was over \$1,000 per Bitcoin».

Wences Casares

Founder & CEO, [xapo](#)





Choosing your Storage





Exchanges

«Bitcoin startups like Gemini are ushering in a new chapter of legitimacy and integrity that will allow Bitcoin to go mainstream and fulfill its ultimate promise».

Tyler Winklevoss
Co-Founder and CEO, Gemini





Crypto-Currency Market Capitalizations

#	Name	Symbol	Market Cap	Price	Available Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	\$18,941,409,561	\$1170.17	16,186,887	\$112,328,000	0.09%	1.47%	11.25%
2	Ethereum	ETH	\$1,297,432,217	\$14.53	89,269,378	\$23,789,800	-0.38%	7.34%	13.80%
3	Ripple	XRP	\$211,065,407	\$0.005682	37,144,100,247 *	\$384,270	0.49%	-0.35%	-3.02%
4	Dash	DASH	\$201,546,829	\$28.28	7,126,707	\$4,494,860	-0.24%	4.04%	27.35%
5	Litecoin	LTC	\$190,844,386	\$3.82	49,966,457	\$2,936,130	0.07%	-0.24%	1.60%
6	Monero	XMR	\$167,801,390	\$11.97	14,021,424	\$1,561,820	0.02%	1.64%	-3.24%
7	Ethereum Classic	ETC	\$111,075,741	\$1.24	89,231,080	\$1,064,780	-0.14%	0.21%	1.99%
8	NEM	XEM	\$57,572,910	\$0.006397	8,999,999,999 *	\$85,856	-0.18%	-0.25%	-2.82%
9	Steem	STEEM	\$25,680,787	\$0.108703	236,247,273	\$62,836	0.92%	-6.65%	-6.16%
10	Factom	FCT	\$24,688,279	\$2.82	8,753,219 *	\$345,870	-0.52%	-3.62%	-12.10%
95	TrumpCoin	TRUMP	\$692,843	\$0.106056	6,532,801	\$3,966	-0.48%	2.53%	5.00%
112	PutinCoin	PUTIN	\$486,529	\$0.005500	88,461,560	\$31,681	-3.28%	-18.58%	41.11%

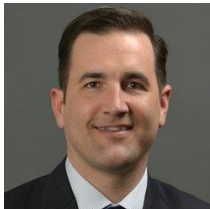
* Not Mineable



Payment Processors

«The original vision for Bitcoin was the creation of a peer to peer payment system for the Internet. We believe in that vision. The consistent growth we have seen in Bitcoin transactions over the last year shows that our customers are beginning to share that belief.

Bitcoin has put online payments into the hands of merchants and consumers. That change is going to be hard to ignore. This technology is on track to become a part of every major payment system in the coming five years».



Stephen Pair
CEO, [BitPay](#)





Merchants

«Bitcoin affords our customers an easy checkout process, while protecting us against fraud and chargebacks. We could not be happier with the results».



Steven Leeds
CMO, TigerDirect

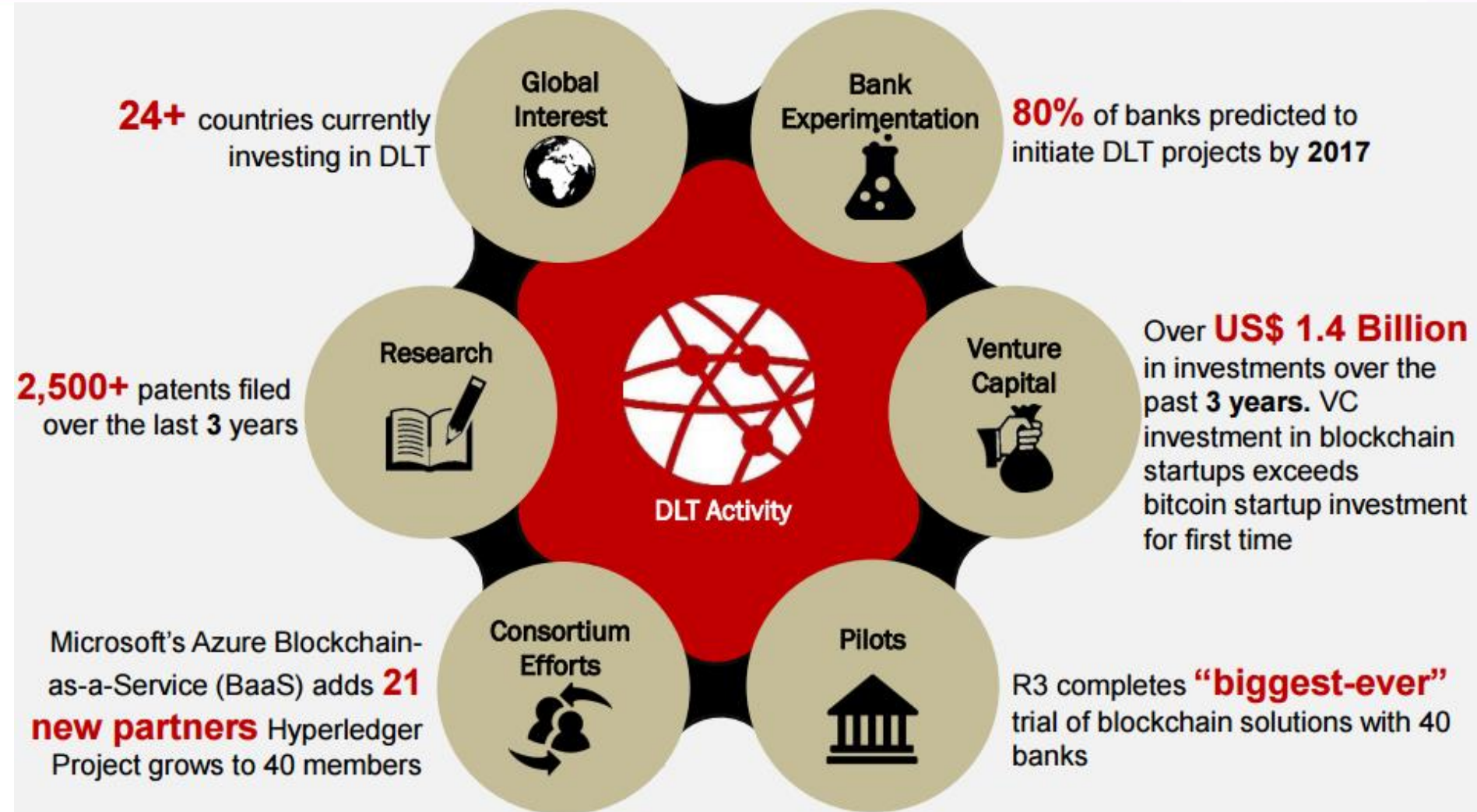




Investment & Banking



Current State of Blockchain – 2016



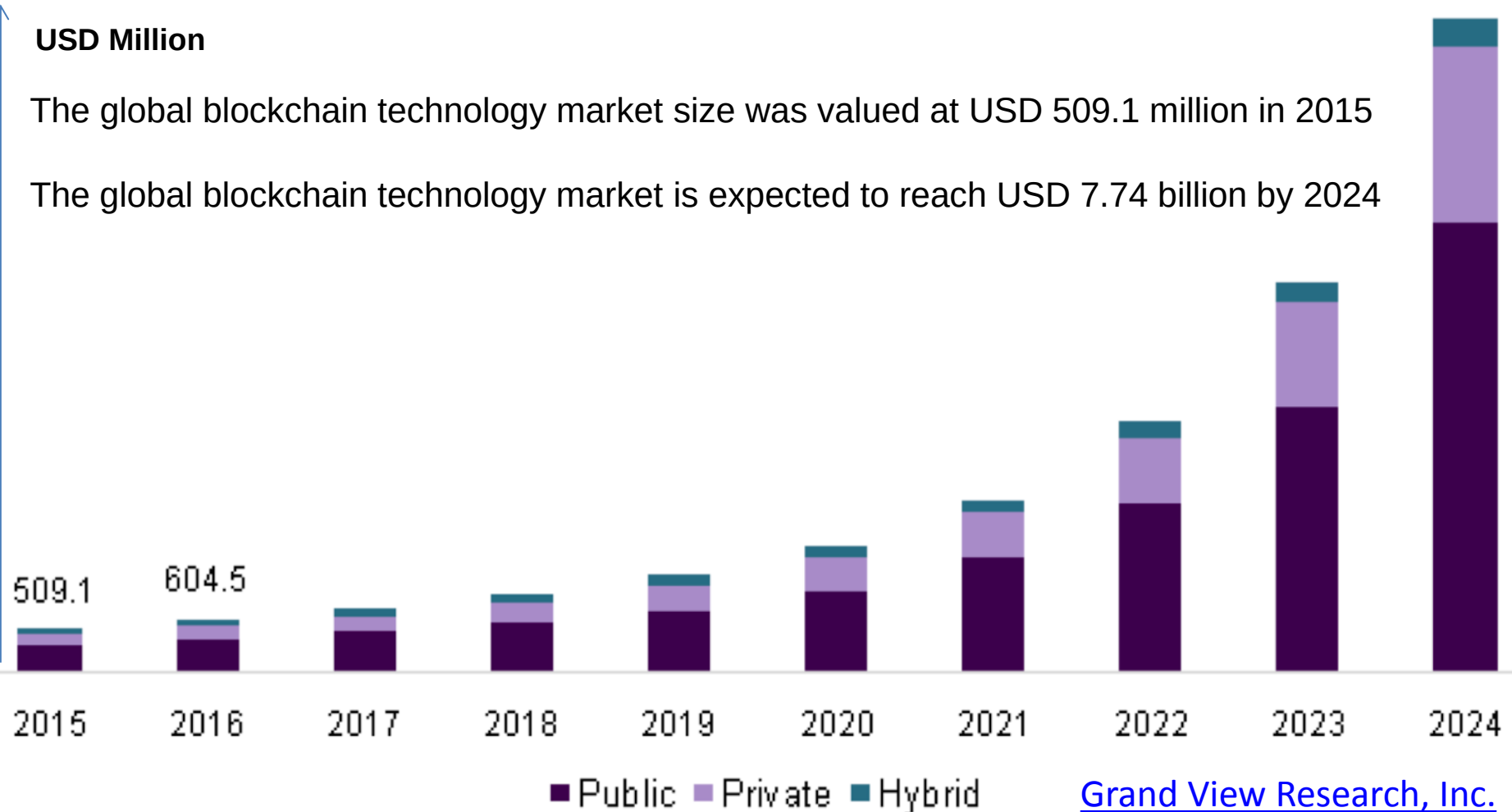


Global Blockchain Technology Market by Type

USD Million

The global blockchain technology market size was valued at USD 509.1 million in 2015

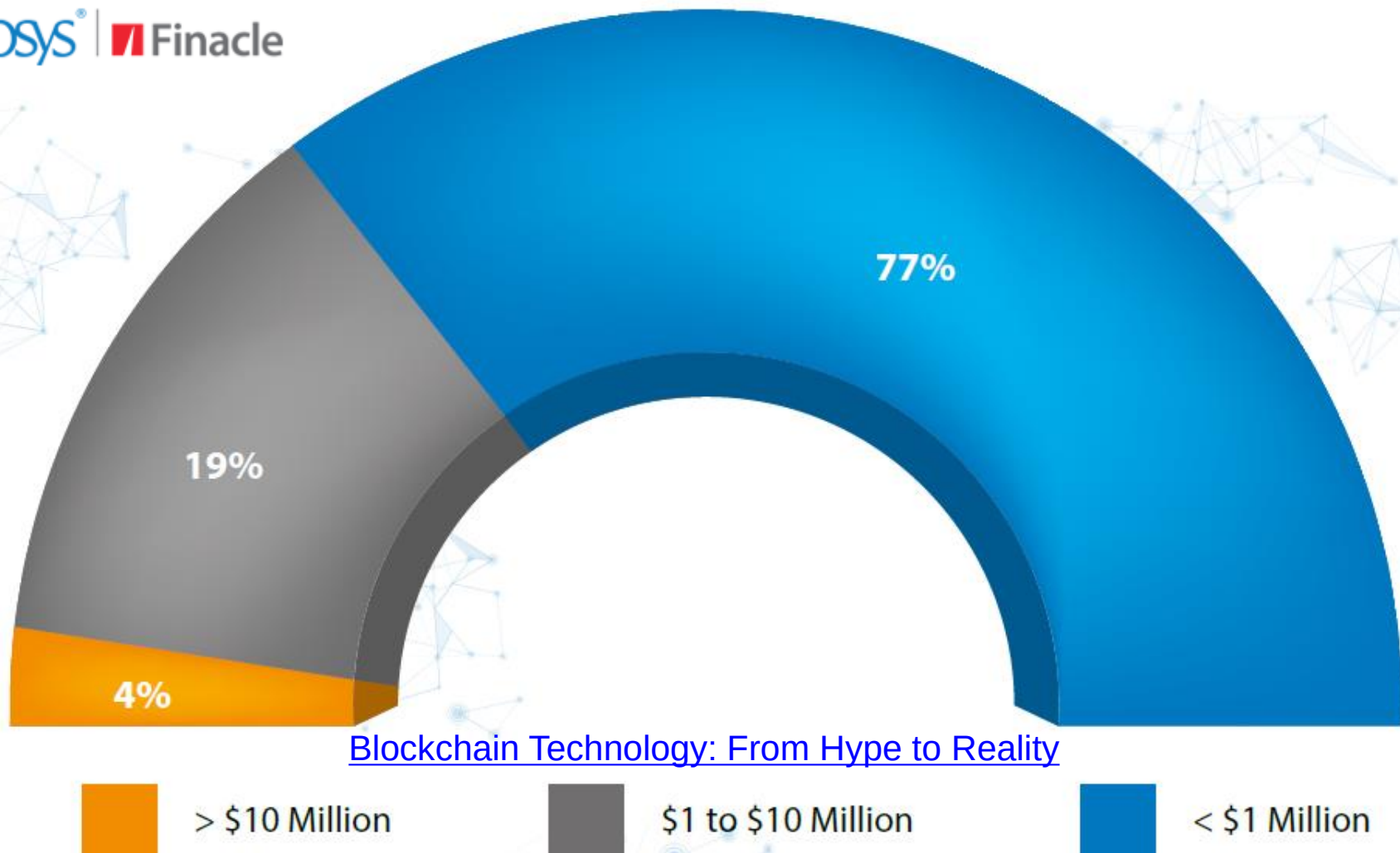
The global blockchain technology market is expected to reach USD 7.74 billion by 2024





Bank's Investments in Blockchain 2017

Infosys | Finacle





Media & Advocacy

«We are privileged to be at the nexus where information meets technology, using a multimedia platform to support the adoption and innovation of Bitcoin and the blockchain. In only two years, the audience for digital currency news has exploded from Fintech specialist to the man on the street. This is now a mainstream media topic, and what happens in Bitcoin happens to the world».



[David Bailey](#)
CEO, [BTC Media](#)





Developer Tools

«It is exciting to be a part of the growth and maturation of the blockchain and Bitcoin ecosystem. Previously we saw products geared towards true believers or technical wizards. We are beginning to see practical, intuitive applications being built for real mainstream users with intuitive, consumer friendly user experiences. This shift has allowed financial institutions, corporations and regulators to take a second look, embracing a platform they once resisted».

[Justin Newton](#)
CEO, [Netki](#)





Blockchain Technology

«Bitcoin will serve a purpose and Ethereum will serve a different one. The ideas I see coming out of it are immense and are the most adventurous in years. The opportunity is huge and I hope a lot of the investment types understand that real, long term money is happening on the fringes».



[Tony Sakich](#)

Director of Marketing, [Augur](#)



Crowdsales



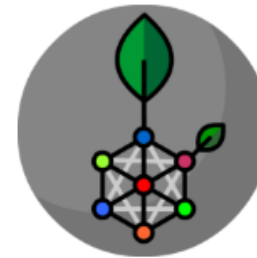
Cosmos

A Network of Distributed Ledgers



Internet of Coins

Decentralized Inclusive Cryptocurrency Ecosystem



Rootstock

Smart Contracts Platform on Bitcoin



Bitsquare

Decentrilized Bitcoin Exchange

Upcoming Crowdsales



Gnosis

Prediction Markets on Ethereum



Filecoin

IFPS based Data Storage Network

Anticipated Projects

Anticipated Projects



Dynamis

Peer to Peer Insurance



Hivemind

Sidechain for Prediction Markets

Anticipated Projects



Successful Crowdsales



Omni Layer

Trustless Financial Ecosystem



NXT

New Economy Movement



NEM



Safe Network

Distributed Data Management Service



BitShares

An industrial-grade financial smart contract platform



Storj

Decentralized Cloud Storage



Ethereum

Smart Contract and Decentralized Application Platform



GetGems

Messaging that Pays



Neucoin

Cryptocurrency for Microtransactions



Factom

A Data Layer For The Blockchain



Augur

Future of the Prediction Markets



Iota

Cryptocurrency for Internet-of-Things



Lisk

Decentralized Application Platform



Waves

Asset/Custom Tokens Platform



Synereo

Social Platform Owned by the People Who Use It



Virtual Accelerator

ether.camp Accelerator build on Ethereum Smart Contracts



Humaniq

Discover the unbanked. Platform for financial and technology startups



Chronobank

The most sustainable stable coins



Russian Blockchain Projects



Golos

Social Media Blockchain Platform
for russian-speaking community



eGaaS

Electronic government as a service



Wings

A decentralized platform to create,
join and manage DAOs

[Мастерчейн](#)

[Общероссийская база биометрических параметров](#)



Financial Services

«Bitcoin use is continuing to grow across borders. 12% of our users, all of whom are international receiving wages from US employers, encompass over 50% of our volume. While we continue to see growth with domestic employees receiving wages from the like of Google, Microsoft or even the U.S.Navy, we foresee the international use-case growing significantly over the next few years until the value of Bitcoin stabilizes».

[Jonathan Chester](#),
Founder & President, [BitWage](#)





Blockchain in Financial Services

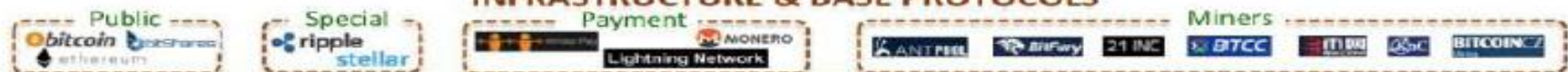
APPLICATIONS & SOLUTIONS



MIDDLEWARE & SERVICES



INFRASTRUCTURE & BASE PROTOCOLS





Companies that pay BitWare workers



USAGE

RATES

JOBS

30595 jobs

Google

airbnb



upwork



9,900+

Registered Users



16,000,000+

International Wages (USD Volume)



The Mega-Master Blockchain List

I. Financial Instruments, Records and Models

II. Public Records

III. Private Records

IV. Other Semi-Public Records

V. Physical Asset Keys

VI. Intangibles

VI. Other



Blockchains and the Internet of Things

NIST Special Publication 800-183

Networks of 'Things'

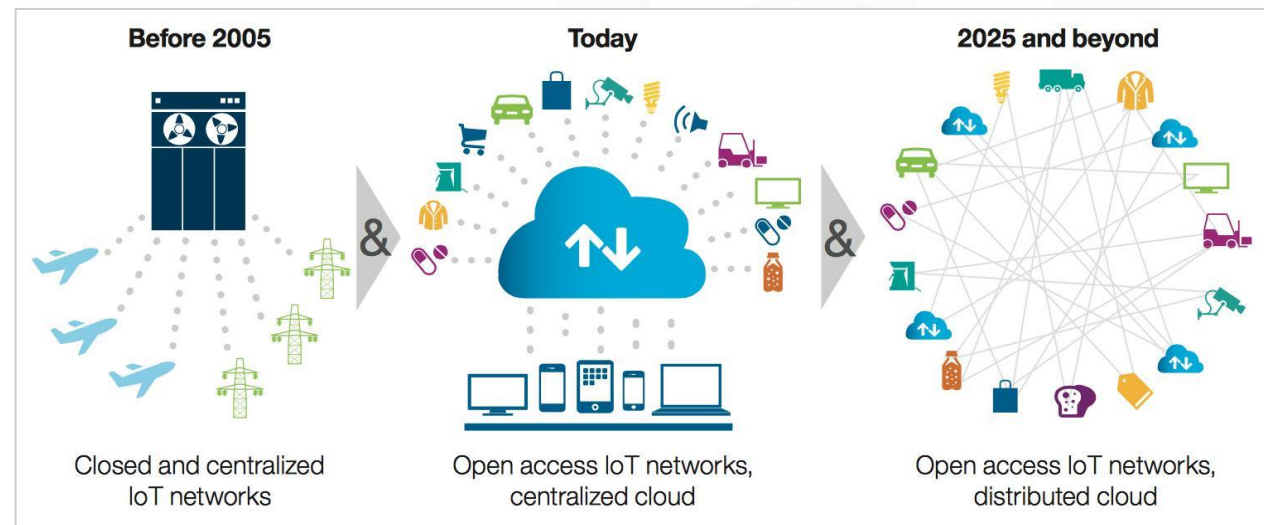
Jeffrey Voas

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.SP.800-183>

COMPUTER SECURITY

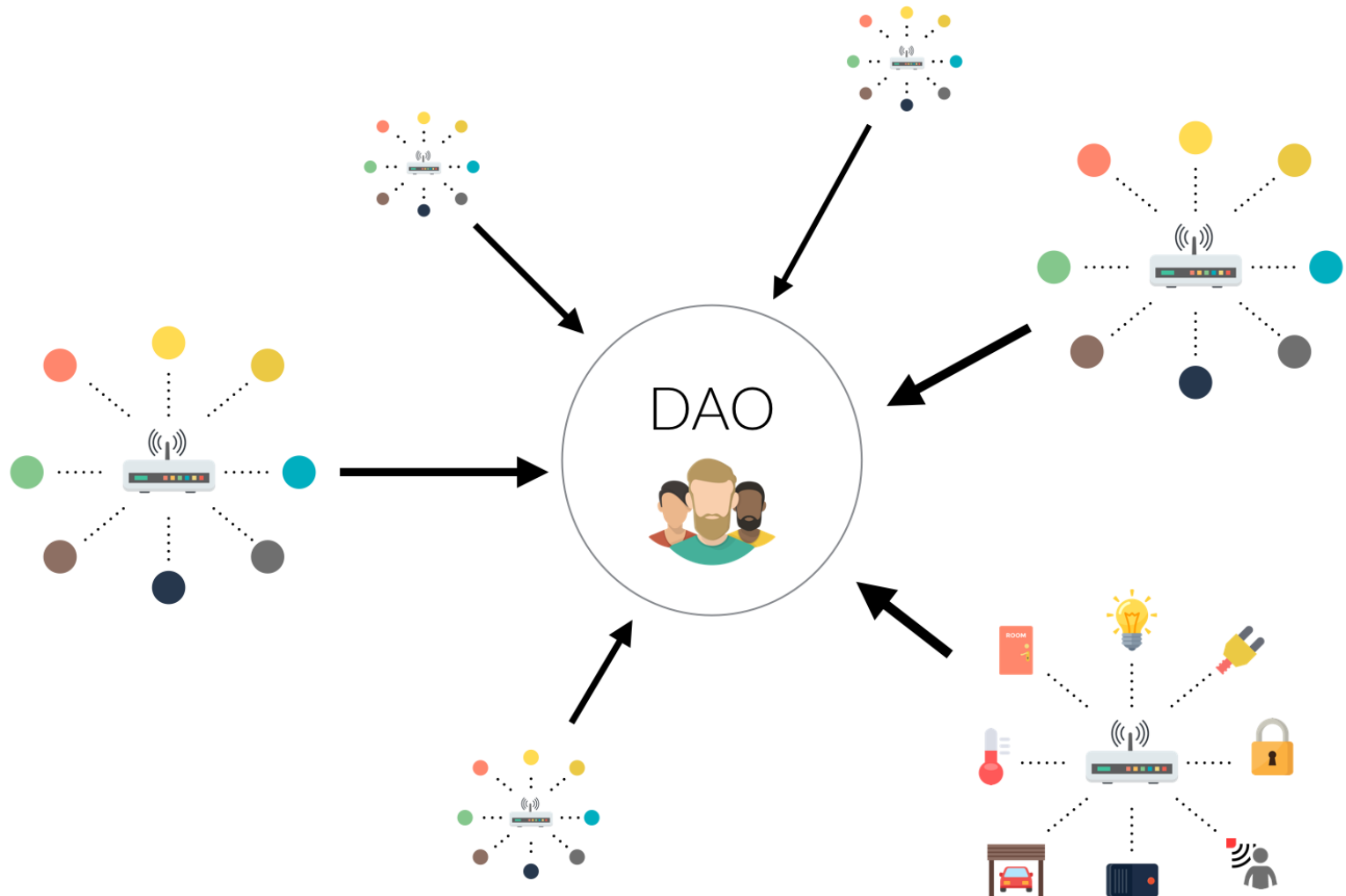
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

<http://www.postscapes.com/blockchains-and-the-internet-of-things/>
<https://developer.ibm.com/dwblog/2016/blockchain-internet-of-things-iot/>



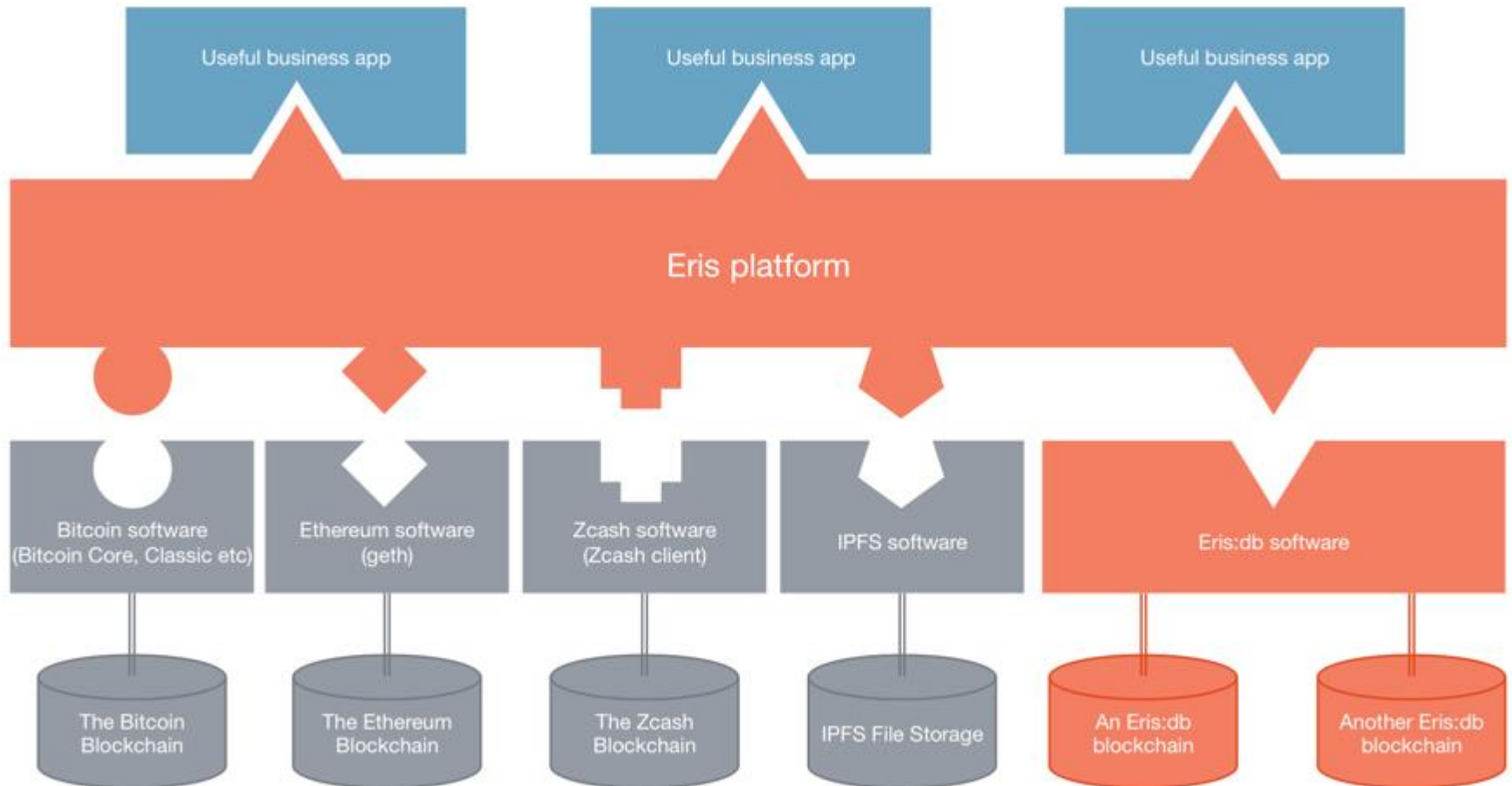


The Decentralized Autonomous Organization





Eris – The Ecosystem Application Platform





Future of Blockchains

Cosmos Roadmap

See the [Cosmos Roadmap](#) for more info.

Cosmos Essential Software and Services

- Tendermint
- Basecoin Framework
- Hub (IBC, PoS/Delegation, Governance)
- Bitcoin and Ethereum bridges
- DEX
- Ethermint

Cosmos Auxiliary Software and Services

- Blockchain Explorer
- Fluidity Smart Contract Framework
- Community Events and Support
- Additional Zones
- Cosmic Grants

Cosmos Development Timeline

The development timeline for Cosmos is split across five eras: Synthesis, Atomic Era, Galactic Era, Planetary Era, and Lunar Era.



CØSMOS
INTERNET OF BLOCKCHAINS

Inter-blockchain Communication (IBC)

Fundraising Event

Cosmos fundraising event starts March 2017.

Citations



“Если будет большой спрос на виртуальную валюту, то не исключено, что Сбербанк будет двигаться в этом направлении. Это крайне интересный глобальный эксперимент, который ломает парадигму выпуска денег. Запрет Bitcoin станет колоссальным шагом назад. Эту виртуальную валюту определенно не надо запрещать, ее нужно изучать и, возможно, регулировать надлежащим образом”.

Герман Греф,
Президент Сбербанка России



“Точно так же, как электронная почта заменила привычные почтовые отделения, а на смену телеграфу пришли SMS и такие сервисы, как Skype или Viber, скорее всего эта же тотальная автоматизация, доступность и избавление от посредников ждет и финансовый рынок, радикальные перемены на котором начинаются с виртуальных валют”.

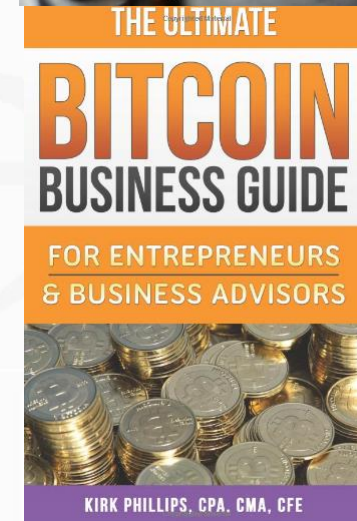
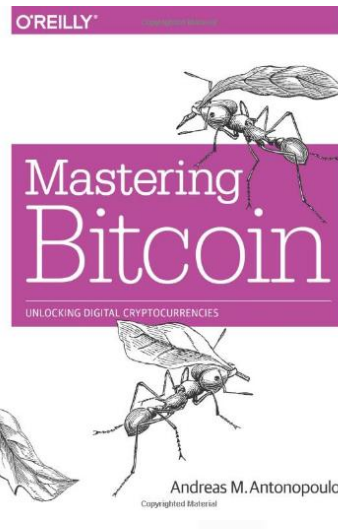
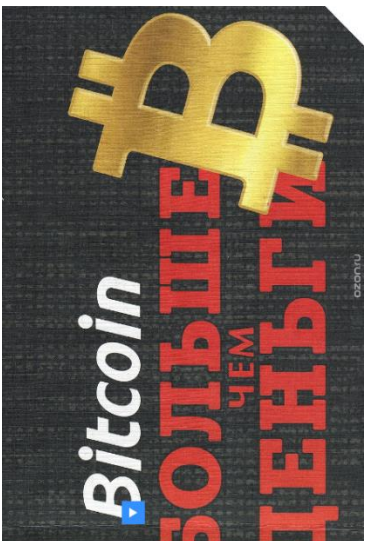
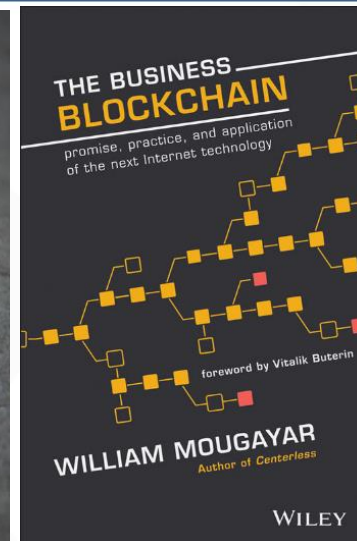
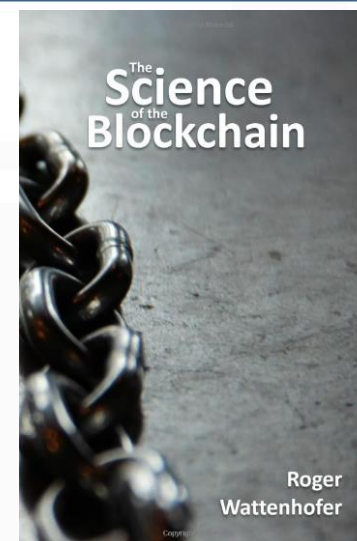
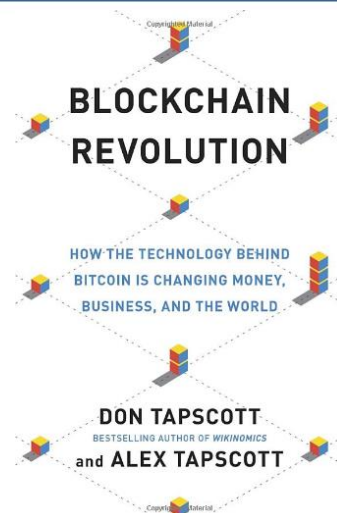
Евгений Воловик,
Росфинмониторинг, ФАТФ



Если бы у меня была машина времени, и я мог вернуться в 1993 год, я бы точно занялся созданием биткоина или другой подобной формы криптовалюты.

Марк Андрессен,
Инвестор, пионер интернета

For Further Reading





Did you enjoy this presentation?

Donate to us at:

Account: BTC



Account: LTC



or

Workshop R&D **Programmable crypto economy** (2017 September – 2018 May).
We invite you to participate in workshop.



Thank you
for your attention!