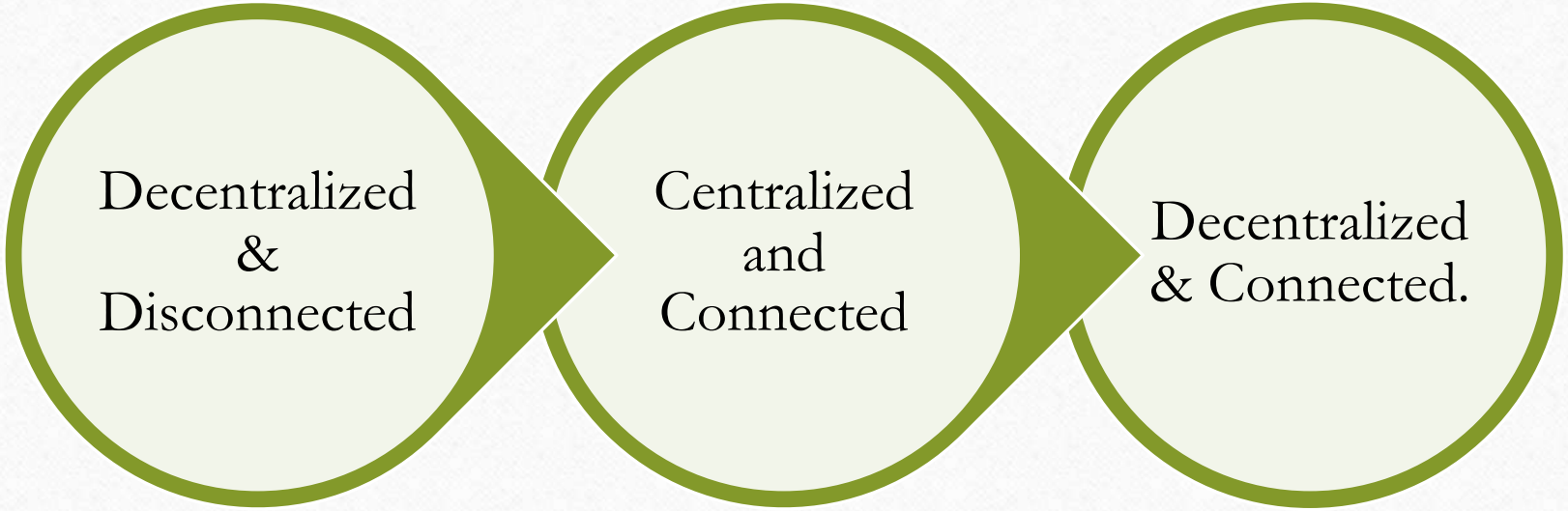
DCentrum and TalentSprint brings

Workshop on Mechanism Design & Cryptonomics (2nd Feb, 2020)

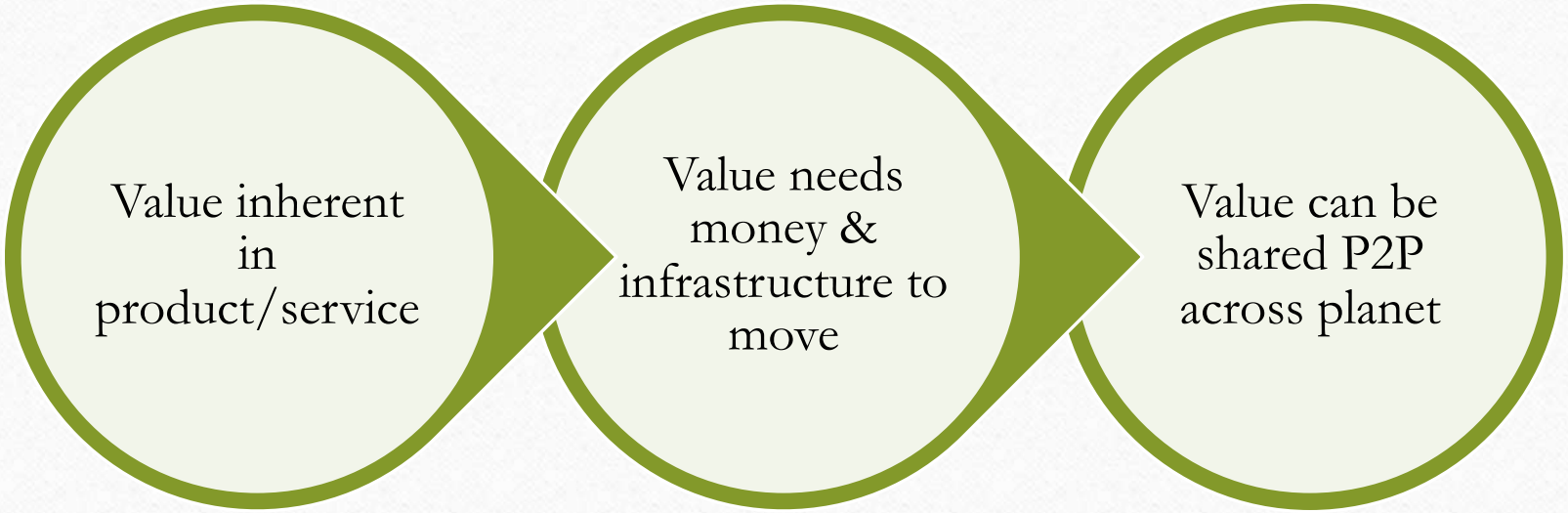
Sunil Aggarwal, Dean, Blockchain Programs, TalentSprint.

History is at the verge of a two-layered shift-1



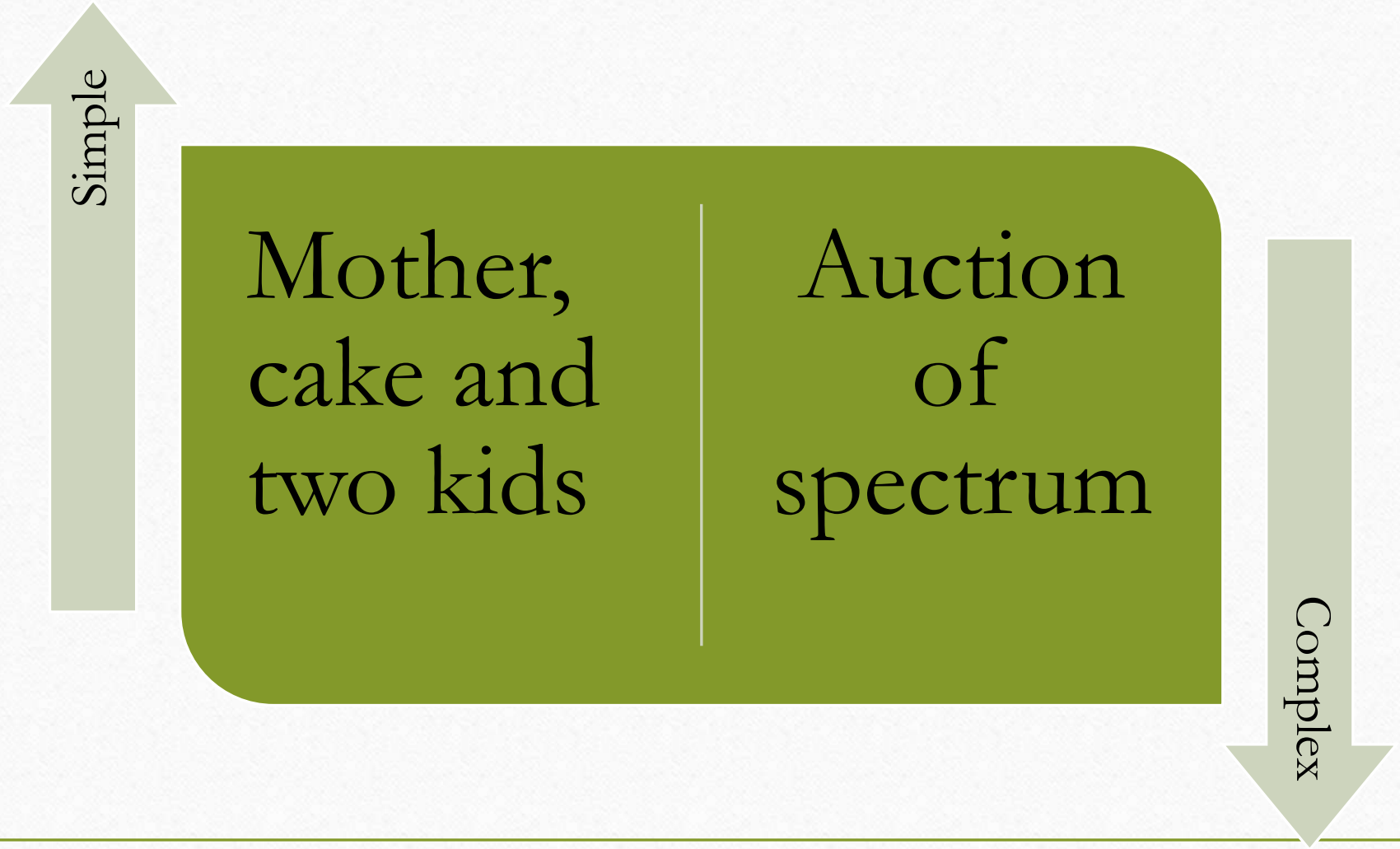
ORGANISATIONAL

History is at the verge of a two-layered shift-2



MERGER OF MONEY AND VALUE

Mechanism Design



Bitcoin and Mechanism Design: P2P electronic cash

- **UNIQUE TRANSACTION**
- No double-spend, Digital Signature Algorithm
- Use cryptographic algorithm SHA-256
- Public Key cryptography and UTXO model
- **IMMUTABLE LEDGER**
- Hash pointers and Merkle-proof architecture
- Longest chain with cryptographic proofs
- **INCENTIVIZATION OF LEDGER-KEEPERS**
- Game theoretic design
- Proof of work and Random Nonce
- Block reward, four-year halving
- Digital Scarcity with 21 million bitcoins
- **MINERS**, BUYERS & SELLERS come together to build a planetary money system

Ethereum & Mechanism Design: EVM

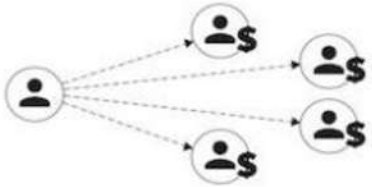
- Modelled a PoW blockchain on the virtual machine model
- Enhanced the block header space into smart contract space
- Introduced a specific language, Solidity
- Account types: Normal and Contract Address
- Smart Contract modelled on app framework
- Gas fee model to stop looping
- Standardization of contracts ERC20 and so on
- Users, miners, app developers come together to use a world computer

Basic Attention Token (BAT)

- Built a browser (BRAVE) that blocks all ads and ad trackers by default
- Builds a "choice architecture" by offering an opt-in advertising framework
- Advertisers pay for ads in their own currencies
- Users get 70% of the ad revenue in BAT tokens (publishers also get revenue)
- Users pay publishers in BAT
- BAT supply is limited and fixed at 1.5 billion
- Built a repertoire of verified publishers for receiving BAT
- Circular economy of users, publishers and advertisers gets complete.

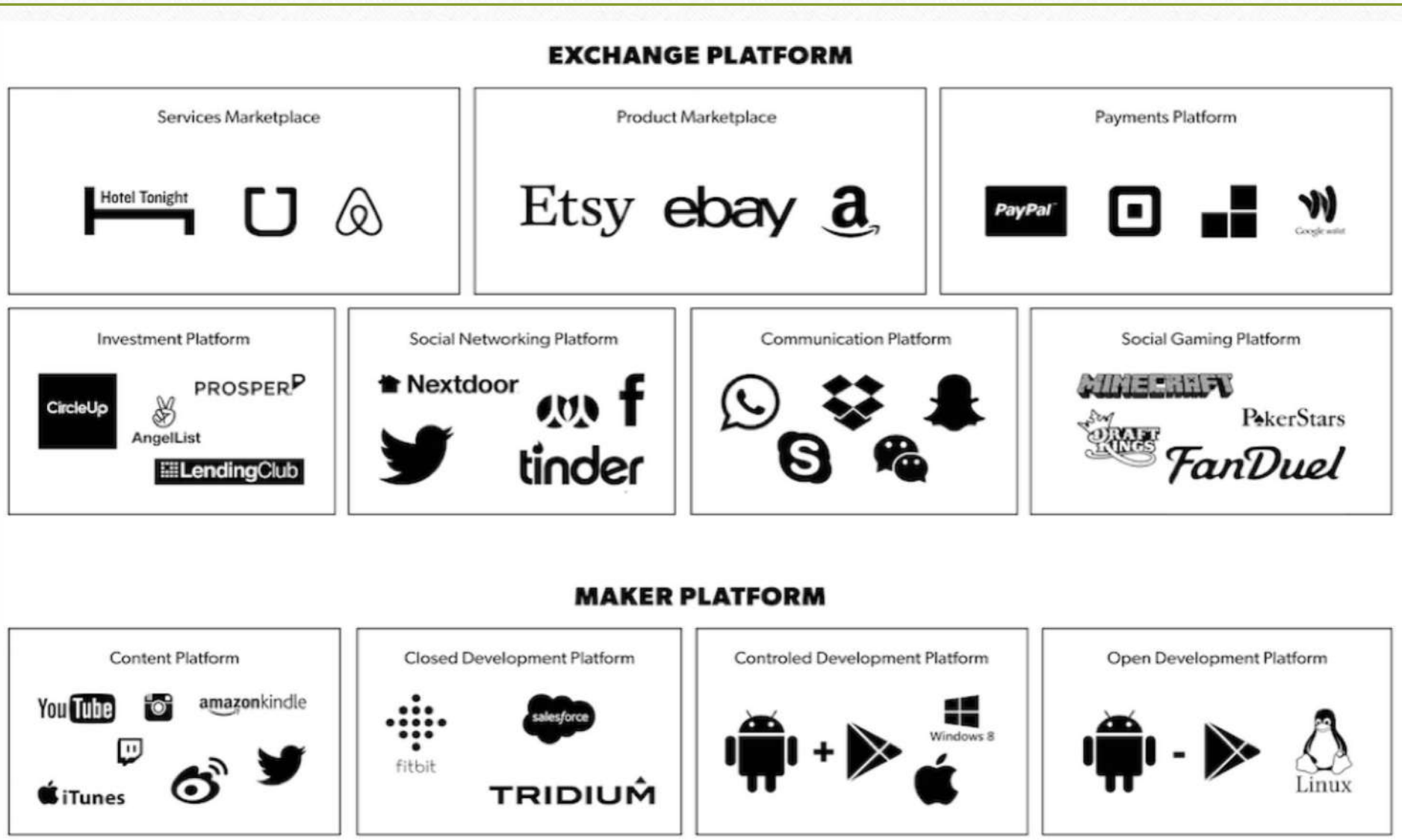
Mechanism Design & Blockchain

BUSINESS MODELS

Platform		Many make, many sell
Software Company		Make one, sell many
Service Provider		Hire one, sell one
Product Company		Make one, sell one

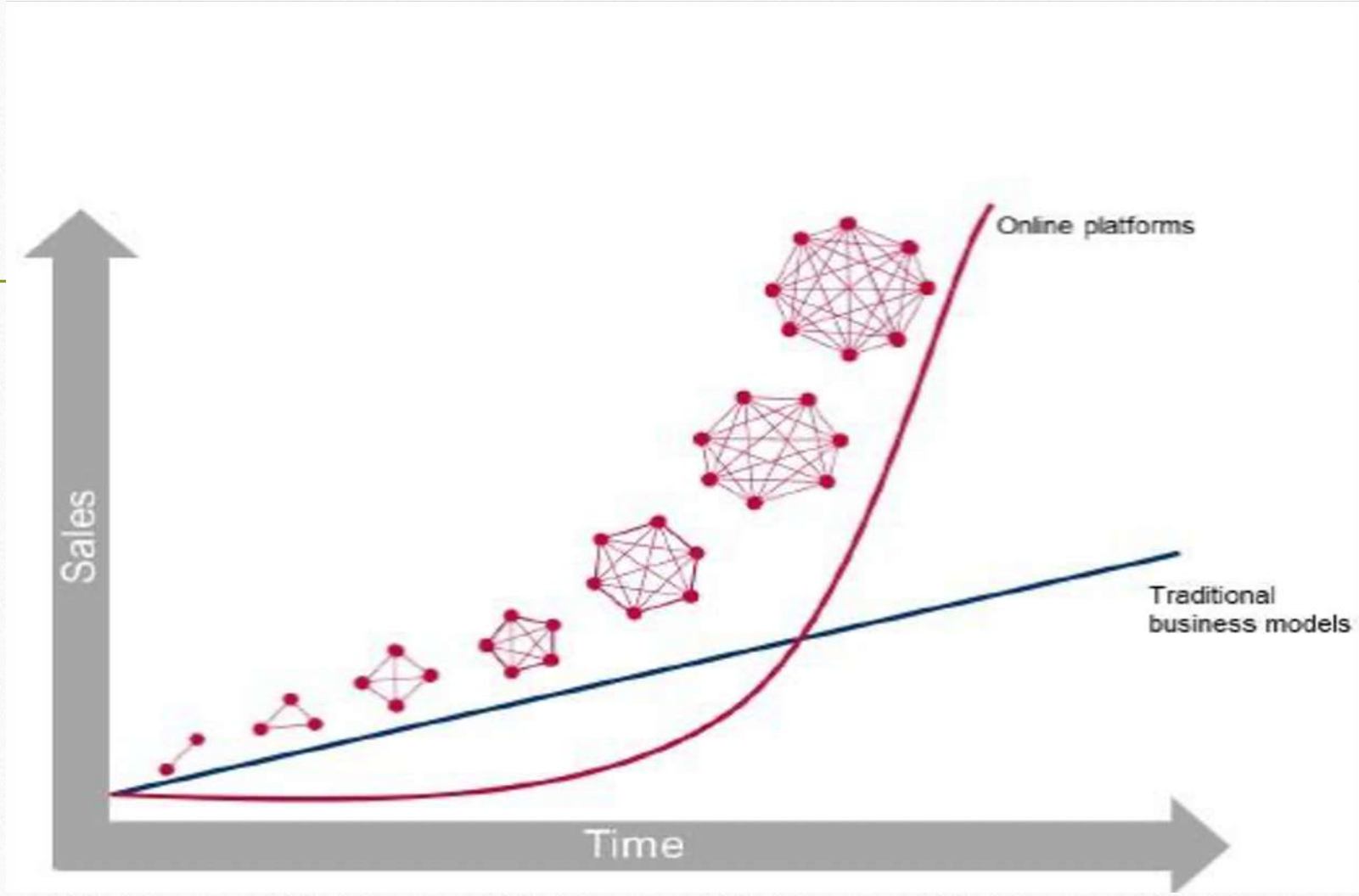
Source: https://www.applicoinc.com/blog/platform-vs-linear-business-models-101/

Rise of Platform business models



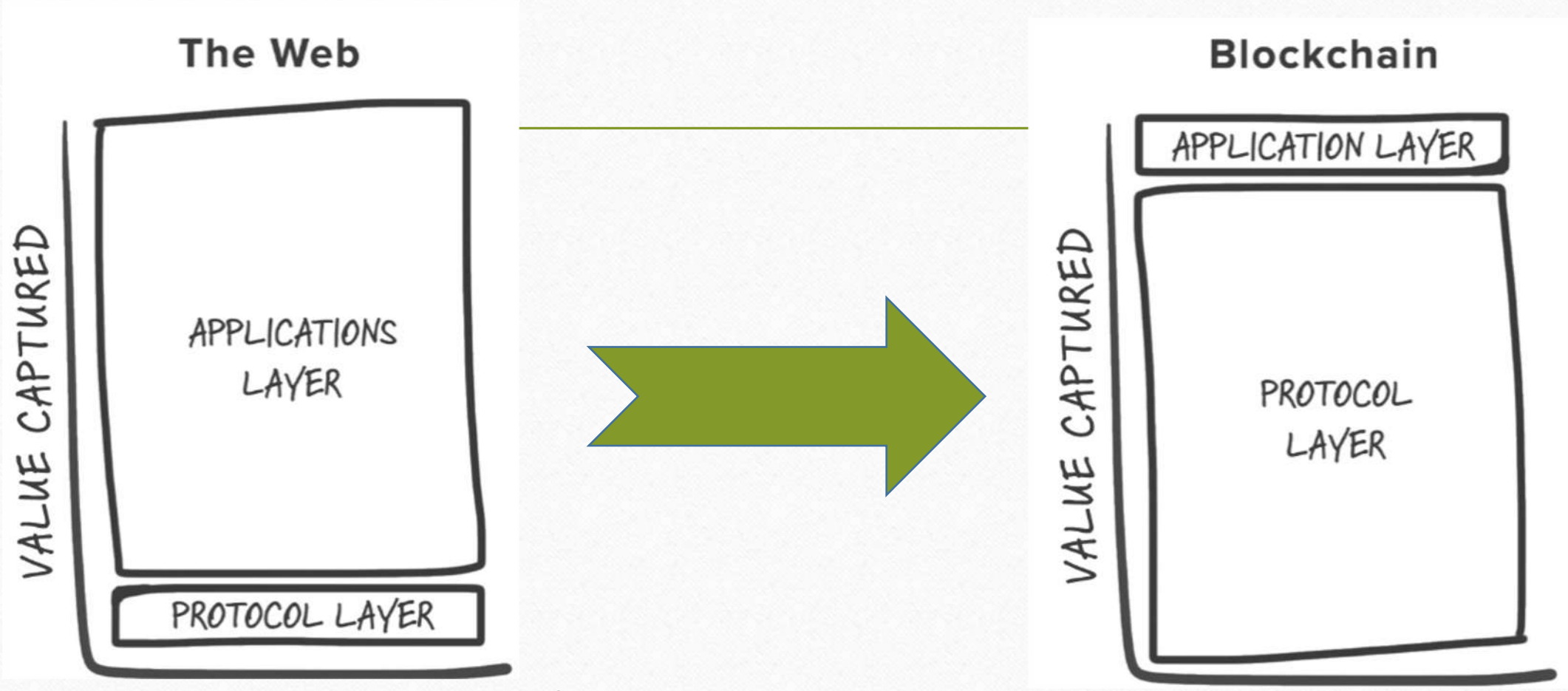
Source: https://www.pinterest.es/pin/117304765278614065/

BUSINESS GROWTH



Source: https://www.aitrends.com/ai-adoption/instead-jobs-artificial-intelligence-killing-business-models/

“Fat Protocols” a term by Joel Monegro, Aug, 2016



Source: http://www.usv.com/blog/fat-protocols

How protocols-applications relation reversed in Blockchain universe?

- "Value concentrates at the shared protocol layer"
- "Only a fraction of value is distributed at the applications layer."
- It's a stack with "fat" protocols and "thin" applications.
- Shared data layer & a cryptographic access token make it unique
- Bitcoin network $170 billion, Ethereum ($ 19 billion) & EOS $3.9 billion (30th Jan, 2020)

"Fat" and "Protocol" = Crypto + Economics

- Blockchains are "Crypto-economic Protocols" (Vitalik Buterin)
- They reduce the cost of verifying the attributes of a transaction
- They reduce the cost of networking
- Merger of sequential and combinatorial innovation
- Beyond the traditional dichotomy of market and firm
- Beginning of a unique market design (unseen & unimagined)

Blockchain alters the nature of firm

- 1937 article "The Nature of Firm" by Ronald Coase
- Coase discussed firm in the context of market economy
- A firm remained centre of transactions
- Blockchain is not a firm but does what only a firm used to do
- Bitcoin is a centre of payment transactions
- Ethereum is a centre of innovation value transfer

How blockchain disrupts the fundamental?

- Boundaries of where price mechanism is suspended is being changed
- Blockchain favours market economy but not market firm
- Blockchain replaces firm as a proxy of contracts that define transaction costs
- Blockchain adds cryptographic stigmergy

Blockchains & economic institutions of capitalism

Before 2009				
Hierarchy				
Government		Firms		Market
After 2009				
Government	Blockchain	Firms	Blockchain	Markets

Source: https://medium.com/cryptoeconomics-australia/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4

Desired Parameter	Property we achieve by optimizing the parameter
Minimize Data Revealed	Privacy
Minimize Latency	Scalability
Maximize Throughput	Scalability
Minimize how much each node stores	Scalability
Maximize ease of integration between multiple blockchains	Interoperability
Maximize honest platform usage	Incentivization
Maximize ease of deciding protocol changes	Governance
Minimize computation of each node	Energy Efficiency

Blockchain parameters' optimization

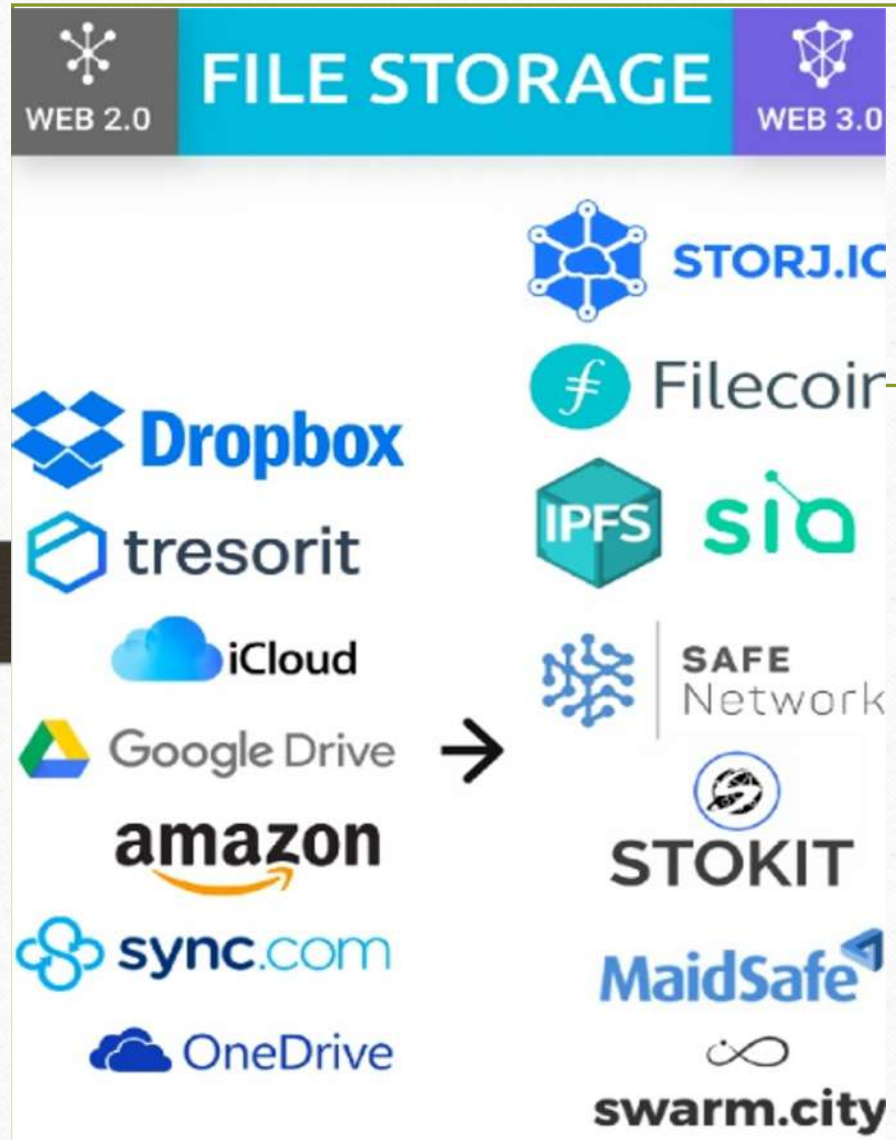
BLOCKDATA | PLATFORMS COMPARED |

JOIN OUR TELEGRAM CHANNEL FOR MORE @BLOCKDATA_OFFICIAL

VERSION 1.4
ISSUE DATE 18/06/18

	QTUM	ETHEREUM	NEO	WANCHAIN	LISK	ARK	EOS	STRATIS	WAVES
NAME	QTUM	ETHEREUM	NEO	WANCHAIN	LISK	ARK	EOS	STRATIS	WAVES
TOKEN	QTUM	ETH	NEO	WAN	LSK	ARK	EOS	STRAT	WAVES
ISSUE DATE	16/03/2017	24/07/2014	01/06/2014	03/10/2017	04/05/2016	21/03/2017	02/07/2017	06/08/2016	15/04/2016
LANGUAGE SUPPORT	Solidity	Solidity	C#, Java, NET, Kotlin, Python	Solidity	Javascript	Javascript	WebAssembly, C, C++	C#, .NET	Scala
CONSENSUS MECHANISM	PoS	PoW / PoS	dBFT	PoS	DPoS	DPoS	DPoS	PoS	LPoS
TPS	70 p/s	15 p/s	1000 p/s (P*)	N/A	5 p/s	25 p/s	100,000 p/s (P*)	20,000 p/s (P*)	100 p/s
BLOCKTIME	120 s	15 s	15 s	N/A	10 s	8 s	0.5 s	60 s	3 s
DAPPS	✓	✓	✓	✓	✓	✓	✓	✓	✓
SDK	✓	✓	✓	In progress	In progress	In progress	✓	✓	✓
ATOMIC SWAPS	✓	✓	✗	✗	✗	In progress	✗	✗	In progress
SIDECHAINS	✓	✓	✓	✓	In progress	✓	✗	✓	In progress
SMART CONTRACTS	✓	✓	✓	✓	In progress	In progress	✓	✓	In progress
CIRCULATING SUPPLY	88.664.516	100.149.205	65,000,000	106,152,493	107.068.862	103.277.536	896.149.492	98.900.026	100,000,000
MARKET CAP	$920.027.350	$49.821.325.284	$2.462.830.500	$303.742.619	$664.492.915	$158.382.298	$9.241.900.098	$297.690.068	$344.406.000
FUNDS RAISED	-$15,600,000	-$18,400,000	-$5,000,000	-$35,558,190	-$5,700,000	-$1,000,000	-$185,000,000	-$610,908	-$16,400,000
TEAM SIZE	-18	-159	-61	-42	-44	-34	-49	-32	-80

Source: https://twitter.com/biggzi/status/1008707232354197504



Blockchain-based data Storage

- Utilize unused storage capacity across desktops, servers and storage devices
- Reward crypto-tokens for using space
- It will cost a fraction of current offerings

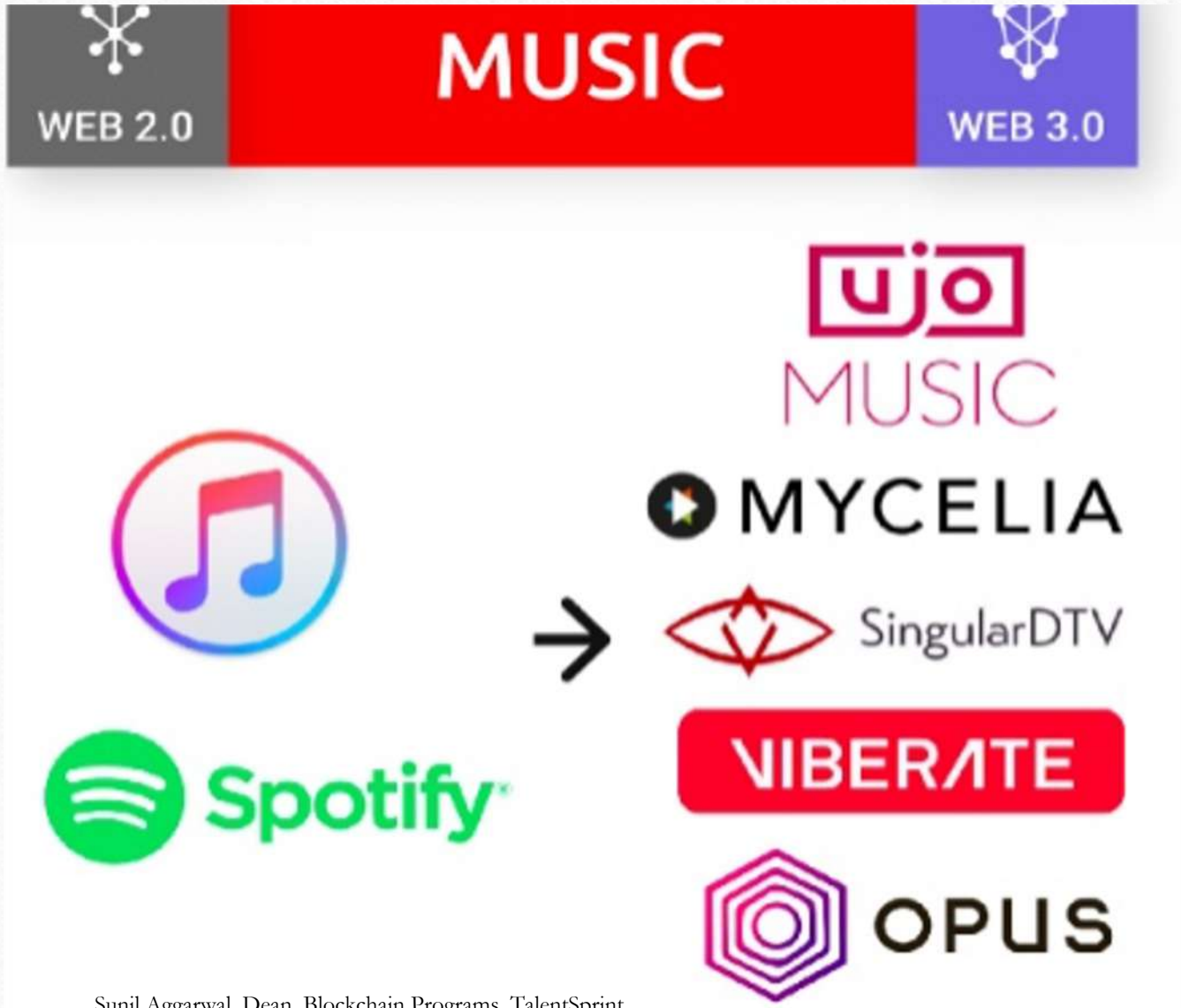
Image Source: https://medium.com/@matteozago/why-the-net-giants-are-worried-about-the-web-3-0-44b2d3620da5

Social network = Social economy

- End of surveillance networks
- End of data theft
- Privacy guaranteed
- End of unequal data empires
- End of "winner takes all" culture

Blockchain VOD

- Platform-independent approach
- Transparent content monetization
- Content ownership safe
- Artist community at the centre



Music Streaming

- End of middleman culture
- Rise of fan economy
- Parallel revenue chains
- Distribution of revenue for multiple artists

Cryptonomics as a popular discourse

Naval Ravikant's 37 Tweets

- **1/Blockchains will replace networks with markets**.
- 2/ Humans are the networked species. The first species to network across genetic boundaries and thus seize the world.
- 3/ Networks allow us to cooperate when we would otherwise go it alone. And networks allocate the fruits of our cooperation.
- 4/ Overlapping networks create and organize our society.
- 5/ **Money is a network. Religion is a network. A corporation is a network. Roads are a network. Electricity is a network...**

Naval Ravikant's 37 Tweets

- 6/ Networks must be organized according to rules. They require Rulers to enforce these rules. Against cheaters.
- **7/ Networks have "network effects." Adding a new participant increases the value of the network for all existing participants.**
- 8/ Network effects thus create a winner-take-all dynamic. The leading network tends towards becoming the only network.
- 9/ **And the Rulers of these networks become the most powerful people in society**.
- 10/ Some are run by kings and priests who choose what is money and law, sacred and profane. Rule is closed to outsiders and based on power.

Naval Ravikant's 37 Tweets-II

- 11/ Many are run by corporations. The social network. The search network. The phone or cable network. Closed but initially meritocratic.
- 12/ Some are run by elites. The university network. The medical network. The banking network. Somewhat open and somewhat meritocratic.
- 13/ A few are run by the mob. Democracy. The Internet. The commons. Open, but not meritocratic. And very inefficient.
- 14/ Dictatorships are more efficient in war than democracies. The Internet and physical commons are overloaded with abuse and spam.
- **15/ The 20th century created a new kind of network - market networks. Open AND meritocratic.**

Naval Ravikant's 37 Tweets

- 16/ Merit in markets is determined by a commitment of resources. The resource is money, a form of frozen and trade-able time.
- 17/ The market networks are titans. The credit markets. The stock markets. The commodities markets. The money markets. They break nations.
- 18/ Market networks work where there is a commitment of money. Otherwise they are just mob networks. The applications are limited.
- **20/ Blockchains are a new invention that allows meritorious participants in an open network to govern without a ruler and without money.**
- **21/ They are merit-based, tamper-proof, open, voting systems.**

Naval Ravikant's 37 Tweets-IV

- 22/ The meritorious are those who work to advance the network.
- **23/ As society gives you money for giving society what it wants, blockchains give you coins for giving the network what it wants.**
- 24/ It's important to note that blockchains pay in their own coin, not the common (dollar) money of financial markets.

Naval Ravikant's 37 Tweets-V

- 25/ Blockchains pay in coin, but the coin just tracks the work done. And different blockchains demand different work.
- **26/ Bitcoin pays for securing the ledger. Ethereum pays for (executing and verifying) computation.**
- 27/ Blockchains combine the openness of democracy and the Internet with the merit of markets.
- **28/ To a blockchain, merit can mean security, computation, prediction, attention, bandwidth, power, storage, distribution, content...**
- 29/ Blockchains port the market model into places where it couldn't go before.

Naval Ravikant's 37 Tweets-VI

- **30/ Blockchains' open and merit based markets can replace networks previously run by kings, corporations, aristocracies, and mobs.**
- 31/ It's nonsensical to have a blockchain without a coin just like it's nonsensical to have a market without money.
- **32/ It's nonsensical to have a blockchain controlled by a sovereign, a corporation, an elite, or a mob.**

Naval Ravikant's 37 Tweets

- 33/ Blockchains give us new ways to govern networks. For banking. For voting. For search. For social media. For phone and energy grids.
- 34/ Networks governed without kings, priests, elites, corporations and mobs. Networks governed by anyone with merit to the network.
- **35/ Blockchain-based market networks will replace existing networks. Slowly, then suddenly. In one thing, then in many things.**
- 36/ Ultimately, the nation-state is just a network (of networks).
- FIN/ Thank you, Satoshi Nakomoto. And to all the shoulders that Satoshi stands upon.

"12 Principles for Blockchain Economy" = "New Rules for the New Economy" Version 2.0

1. The Law of Connection: Embrace Dumb Power
2. The Law of Plenitude: More gives more
3. The Law of Exponential Value: Success is nonlinear
4. The Law of Tipping Points: Significance precedes momentum
5. The Law of Increasing Returns: Make virtuous circles
6. The Law of Inverse Pricing: Anticipate the cheap
7. The Law of Generosity: Follow the free
8. The Law of the Allegiance: Feed the web first
9. The Law of Devolution: Let go at the top
10. The Law of Displacement: The net wins
11. The Law of Churn: Seek sustainable disequilibrium
12. The Law of Inefficiencies: Don't solve problems

Summary

- Mechanism Design is the hot flavour of cryptonomics
- Fat protocols are new value propositions of internet phase 3.0
- Blockchains add a new market design unlike Coase's "Firm"
- Blockchains are a proxy for all contracts involved in transaction costs
- Naval Ravikant's 37 Tweets are popular metaphor for blockchain era