

Jamming on Cryptoeconomics at Polychain: Observations, Ideas & Trends

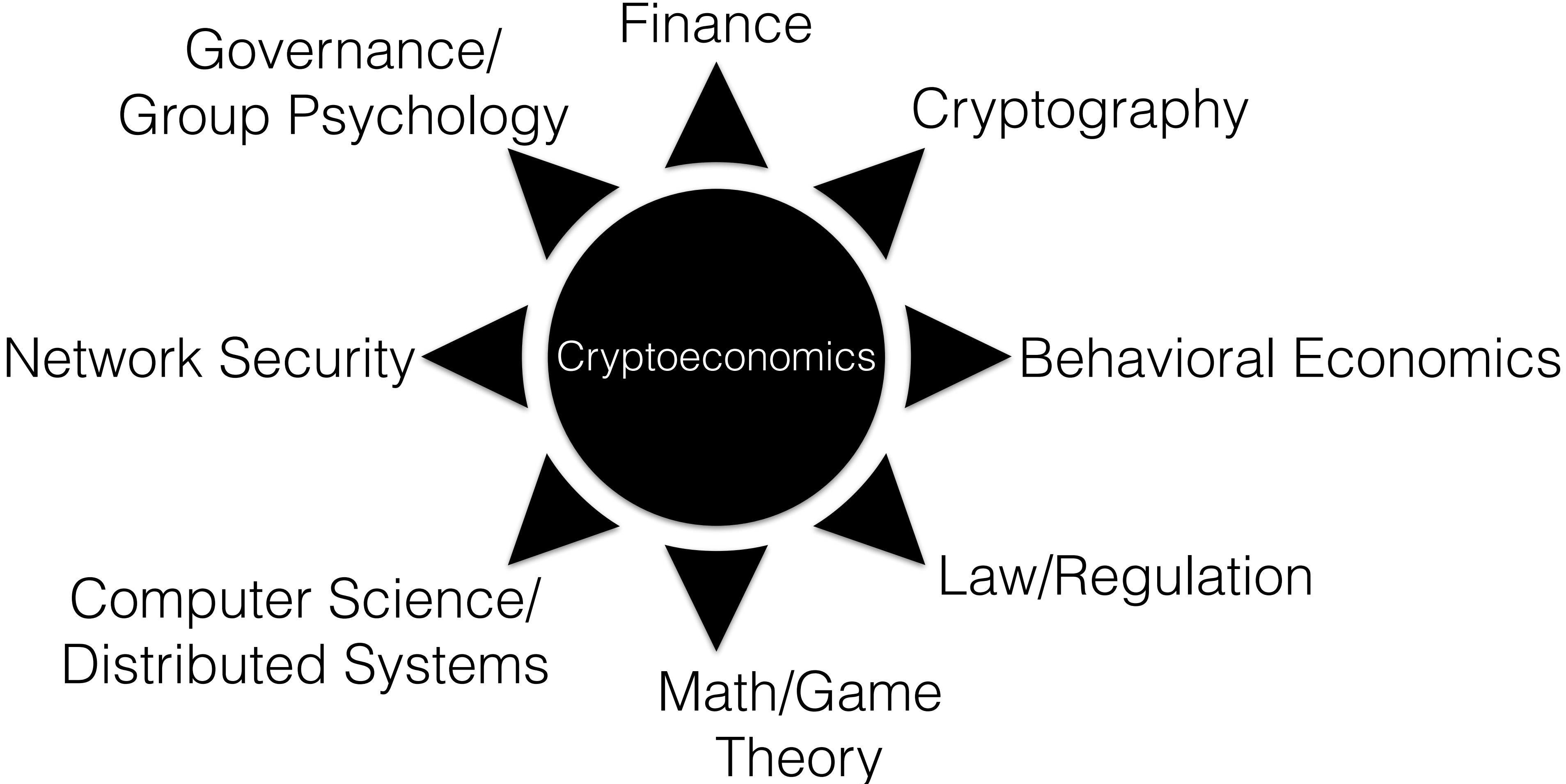
Ryan Zurrer, May 2018

**POLYCHAIN
CAPITAL**

Cryptoeconomics

The study of how we use digital incentivization to drive specific resources and behaviours among self-interested agents on decentralized networks, thereby inherently delivering security and accelerating network effects.

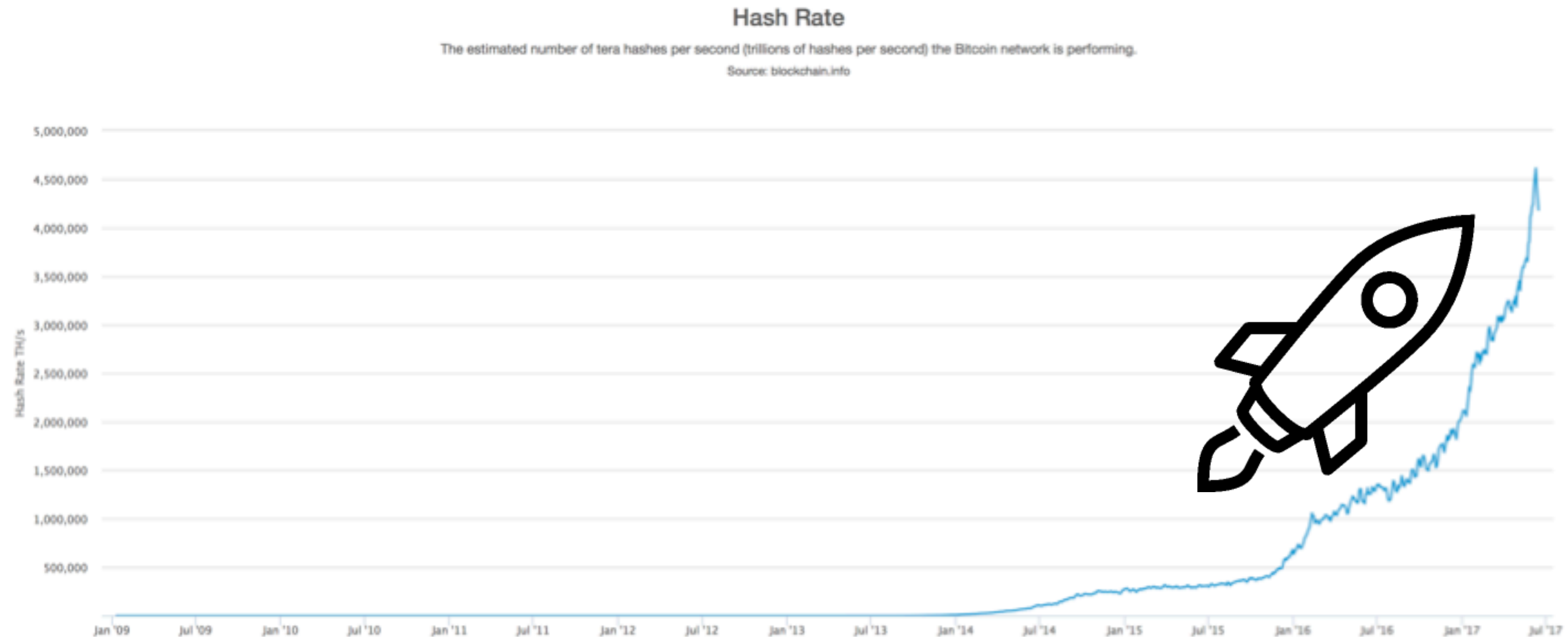
Cryptoeconomics is an amazing convergence of different fields



Tokens act like Rocket Fuel for Network Effects

When designed correctly, tokens can not only drive certain desired behaviours, but they can accelerate them quite dramatically.

Example: Bitcoin's block reward drove an incredible amount of computational resources to be dedicated to securing the network



Keepers

Observations

Incentivization should drive users' cost of interacting on a network to near-0 (Ex: Filecoin, early Bitcoin)

Police layer (Ex: Fisherman in Polkadot, Challengers in Truebit) is a new construct that presents unique challenges and opportunities in incentivization. Randomization could be big part of the solution.

**Transactional,
consumer layer**

**Utility layer
(miners)**

**Police/challenger
layer**

Keepers

Types of Keepers

Resource-Transactional Keepers: provide some specific resource to a network such as computation, storage, intelligence, etc.

Gatekeepers of Trust: maintain trust in the system via validation and verification of said validation.

Arbitrage Keepers: maintain stability of the system through exploitation of arbitrage opportunities and profiting from inefficiencies in the market.

Technologists/entrepreneurs who plan to be Keepers need to scale and professionalize more quickly in next-gen networks.

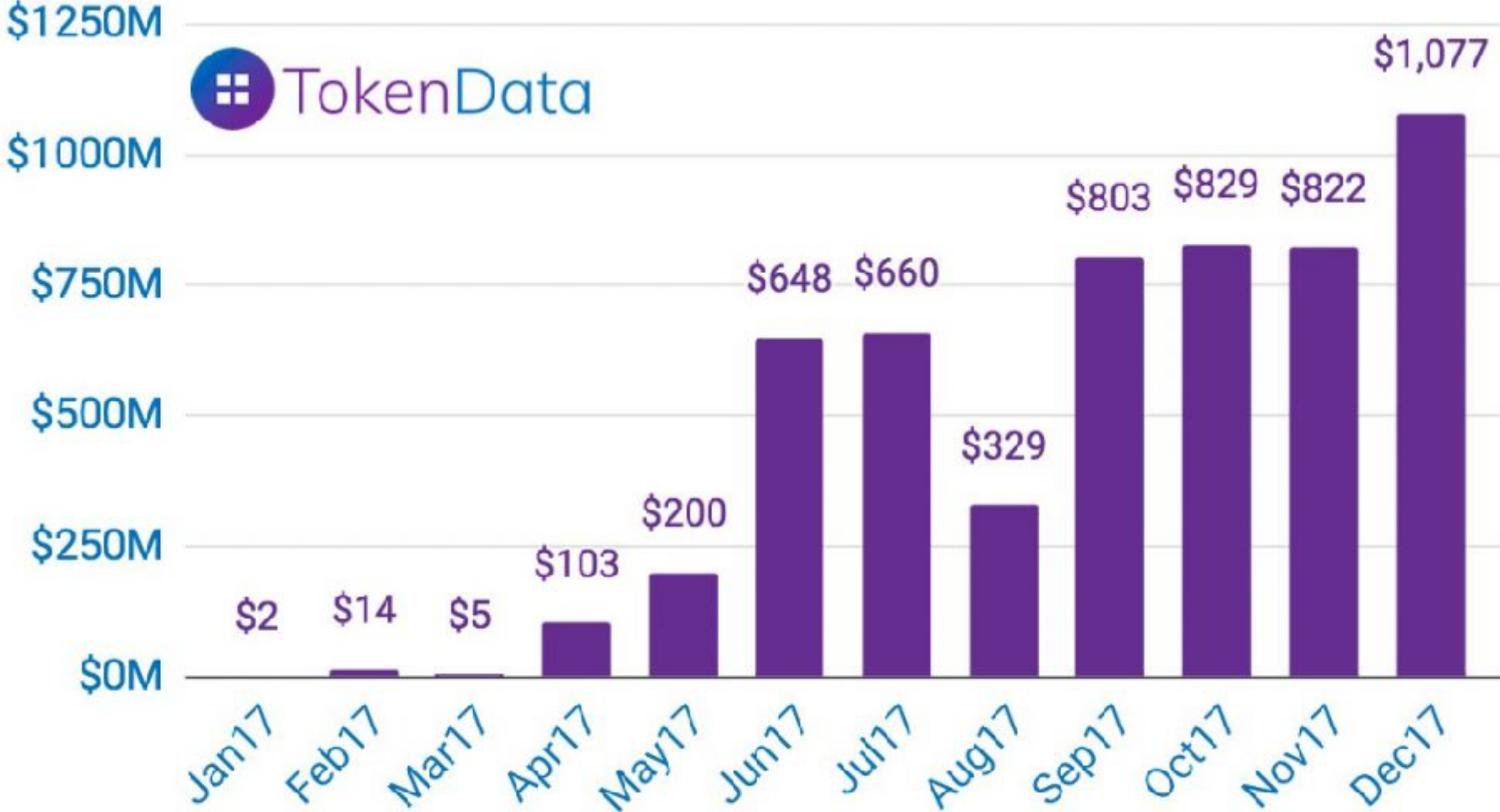
Outlier Growth as Funding Mechanism

2017 saw 5bn raised via token offerings (ICOs)

Outpaced VC capital deployment.

As regulatory concerns arise, new mechanisms are being explored - Air Drops, Lock & Drops, accredited investor SAFT rounds, governance-mechanisms, Block Rewards, etc.

USD Raised by ICOs in 2017 - Monthly Totals



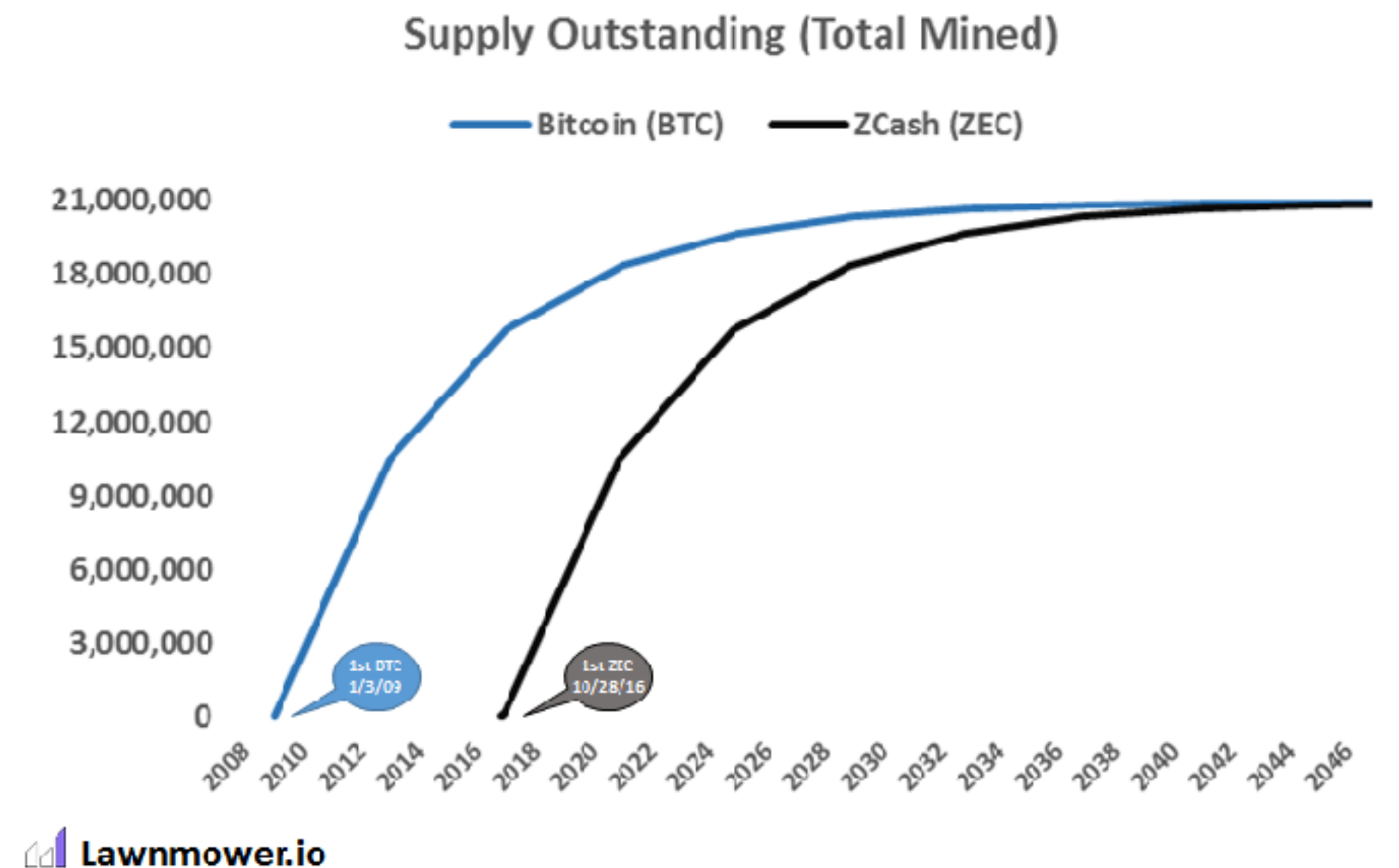
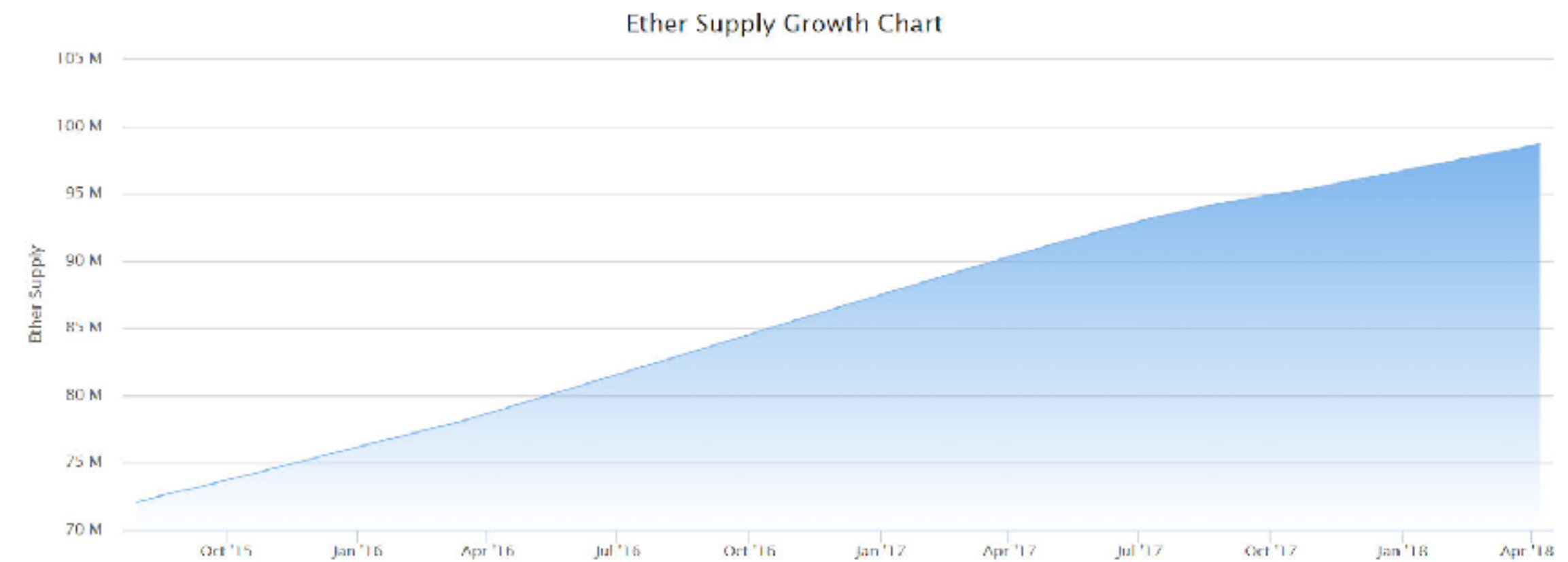
Return of the Block Reward!

Block rewards are a superior way to incentivize the Keepers of a network over the long term.

Distributing tokens over time in exchange for providing some valuable resource to a network is a great way to reduce costs to users while ensuring security and delivering network effects.



- 70% to Filecoin Miners (Reward)
- 15% to Protocol Labs (Genesis)
- 10% to Investors (Genesis)
- 5% to Filecoin Foundation (Genesis)



Governance

Networks with governance will evolve faster and avoid forks

Interesting data point to sample sentiment signals from different constituents in a network (consumers, keepers, token holders, etc.) for major overarching decisions regarding the evolution of the network.

Primary lack of progress in Bitcoin and subsequently Ethereum comes down to inertia around governance. Debates continue incessantly and are directionally controlled by a vocal minority.

Forks are not a form of governance, they are a failure of governance!

Communities > teams, governance is a noble pursuit and merits experimentation

Governance

Governance is really hard and should be “grandfathered in over time” via participatory communities. Ex: MakerDAO

Mechanisms for achieving quorum are crucial. Ex: Polkadot’s governance committee, Delegated vs. Nominated governance.

Tools, information dissemination, professional services similar to staking are part of the solution.

2018 will present some grand experiments in governance.

1. Return of DAO 2.0?
2. Network raids driven by governance. Ex: Pre-genesis forks via governance such as Tezos.
3. New governance models that allow for agile development and outlier remuneration to attract/retain talented developers at the protocol layer.

Major Ecosystems

Layer 1 protocols with novel consensus mechanisms, some considerable innovation in transaction execution and offering rich topography for decentralized application developers.



Metaprotocols

NuCypher

Truebit

1protocol - Vest

Keep

Layer 2 protocols that are a tool or serve some specific use-case that is necessary for many networks.

Gains further network effects and security because they operate simultaneously on top of different Major Ecosystems.

More balanced revenue streams for Keepers because of exposure to multiple tokens and opportunities.

Examples & Ideas around Cryptoeconomic models

We remain in the infrastructure era....for now

Fat Protocols: Outlier value will continue to accrue further down the decentralized software stack known as Web3

Scalability remains an interesting challenge to enable consumer Dapps.

New standards for cross-chain communication will enable rich interaction, atomic swaps and novel use cases.

Market Trends

Web Assembly VMs are the future! Higher performance, web-based, extensible, improved scalability. JavaScript Smart Contracts compiled to WASM VM will be incredibly powerful for adoption and cross-chain communication.

SAFTs are being replaced by early-stage equity deals and patience around the token model (due in part to regulatory concerns). Token crowdfunds (ICOs) remain an incredibly powerful way to build a war chest and propagate a community.

Trough of disillusionment with Crypto Winter: Technical talent is the primary resource bottleneck. New wave of talent will require 18-24 months to produce interesting results.

Many new attempts at layer-1 blockchains (Major Ecosystems). Requires substantial innovation to survive. Many technologies will suffer from network raiding.

Network Raiders

We are moving into a far more competitive and adversarial era in the history of crypto. Networks will be forked, attacked and mass movements of people and capital will happen with extraordinary speed.

Types of Network Raids:

Traditional Network Raid: exploit of an active network in order to short or request ransom. Ex: IOTA coordinator node

Rent-seeking Token Fork: When a token doesn't add value to a network, participants can fork the network and remove the token. Ex: Ethereum is raiding Raiden currently.

Governance Fork: When a community wants to remove a tyrant leader or some malicious actor. Ex: Tezos and Polychain led a pre-genesis governance fork on the Tezos Foundation board.

Hostile Chain Takeover: One chain actively attacks another to steal its participants. Ex: Dogecoin migrating to Ethereum via Truebit.

Crypto-Financial Primitives

- Cross-chain swaps —> derivatives & shorts
- Collateralized debt positions enable short-selling, stable-coins, decentralized debt instruments
- Gas token & mining derivatives

Capital in derivatives today is 524.4 trillion! (investopedia)

SportsDAO

A self-governing, meritocratic, decentralized autonomous organization that leverages the wisdom of the crowd and cryptoeconomic incentives to improve the decisions of a sports franchise.

In the best case, the fanbase (or SportsDAO token holders) could contribute positively to better decision making thereby leading to better overall performance of the team. However, even in the worst case where the input from the fanbase isn't helpful, the team would dramatically improved fan engagement which should lead to a more loyal, higher-revenue fanbase.



Carbon Token Ecosystem

A self-organizing P2P consensus mechanism and marketplace that allows consultants to verify carbon offsets of producers and consumers.

<https://medium.com/@rzurrer/the-carbon-token-ecosystem-white-paper-a-decentralized-p2p-self-organizing-consensus-mechanism-and-aa218bdeeb64>

1. Generator requests to the Collective of Verifiers to begin the evaluation and parameterization process.



2. The Collective of Verifiers selects the Local Verifier to evaluate and parameterize the Generator.



3. The Local Verifier mobilizes to evaluate and parameterize the Generator.



4. The Local Verifier then proposes the Generator's parameters to the Collective of Verifiers for debate and approval of the Generator's Carbon Ratio within the standards of the Carbon Algorithm.



5. The Generator is then connected to the Carbon Token Ecosystem and begins to "mine" Carbon Tokens.



6. The Collective of Verifiers monitors the mining of Carbon Tokens for coherence over time. A portion of Carbon Tokens go to the Local Verifier, the Collective of Verifiers and the Pool of Consumer Verifiers. Verifier Reputation is redistributed among Verifiers.



7. The Consumer (who has also been on-boarded and parameterized) purchases Carbon Tokens to retire them thereby off-setting emissions.



8. Regulators and the public can follow and audit the performance of Generators and Consumers over time.



Shit happens! This is vanguard technology

Emotions and decisions don't mix very well. Proceed with caution in a crisis moment and be patient.

Prepare for all potential outcomes and recognize that we exist in highly adversarial environments. Bounties = network raiding insurance

Be reasonable, relatively forgiving within your community and understand where we are in the lifecycle of this technology.

Have fun and don't take yourself so seriously!

Reach out and come jam with us!

Twitter: @rzurrer

Medium: medium.com/rzurrer

Reddit: u/rzurrer

WeChat: rzurrer