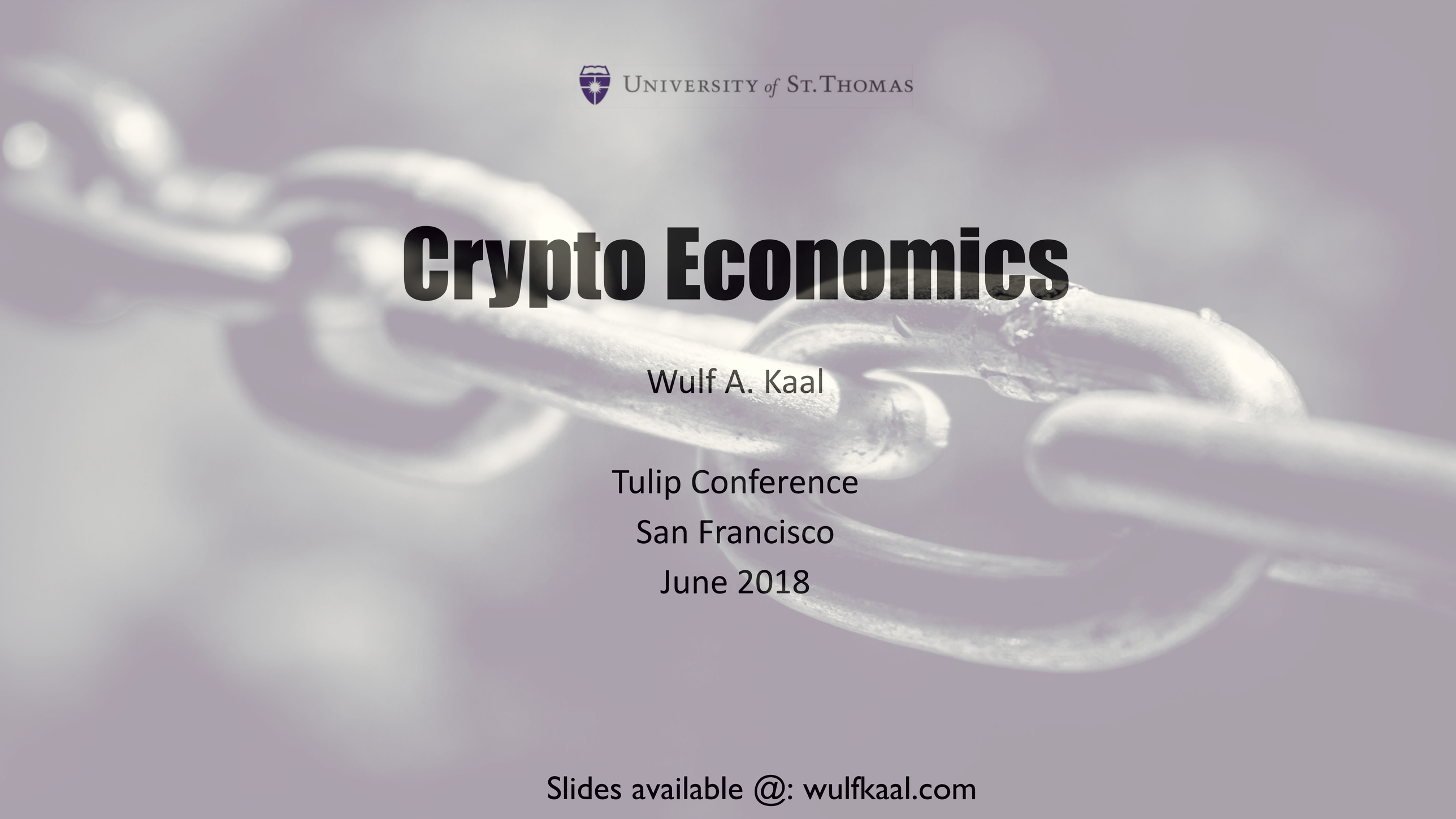


University of St. Thomas

Crypto Economics

Wulf A. Kaal

Tulip Conference

San Francisco

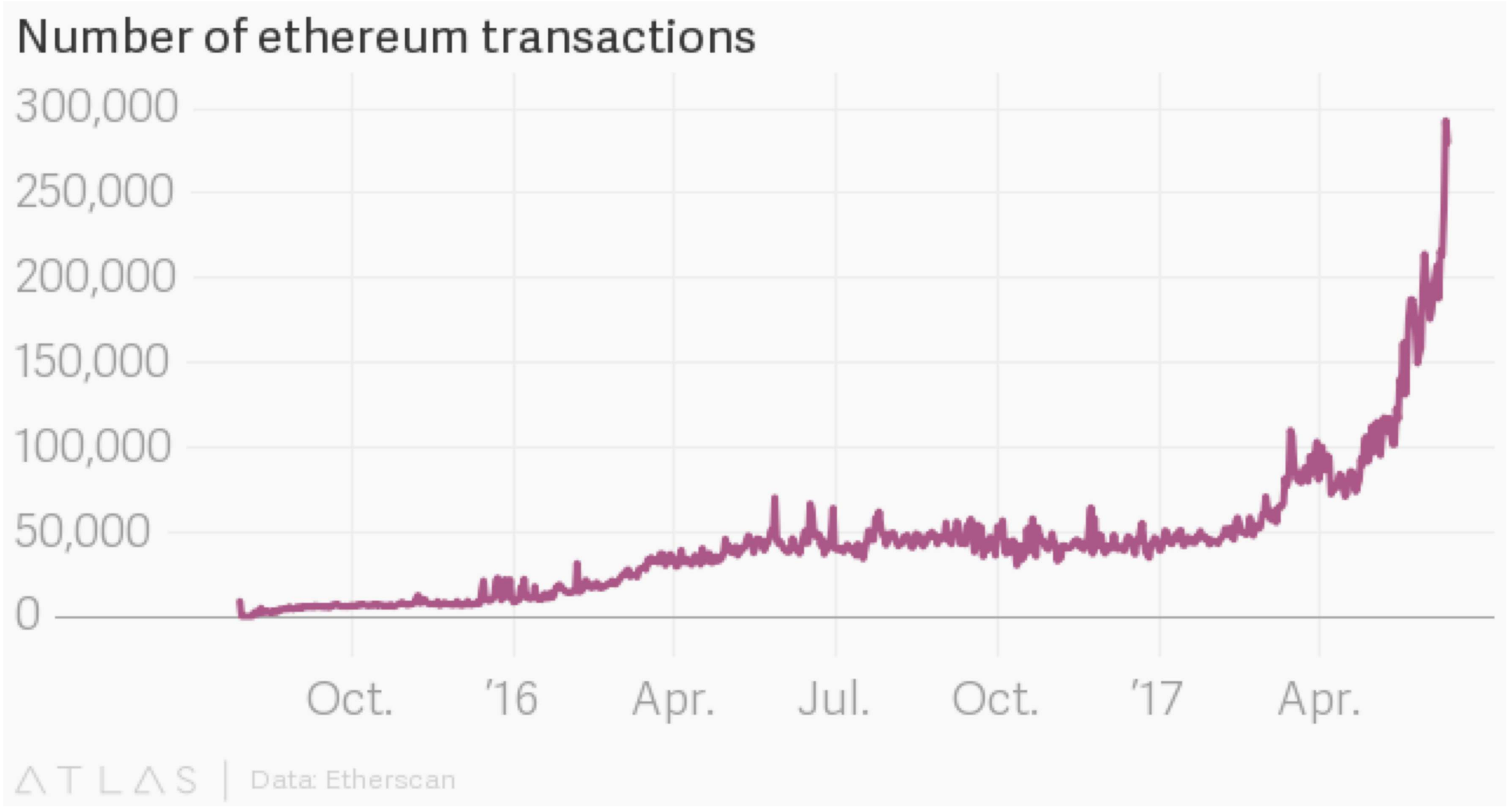
June 2018

Slides available @: wulfkaal.com

Outline

- A new Discipline: Crypto Economics
- Basics – Crypto Macroeconomics, Microeconomics, Monetary Policy, Fiscal Policy
- Token Models
- Outlook

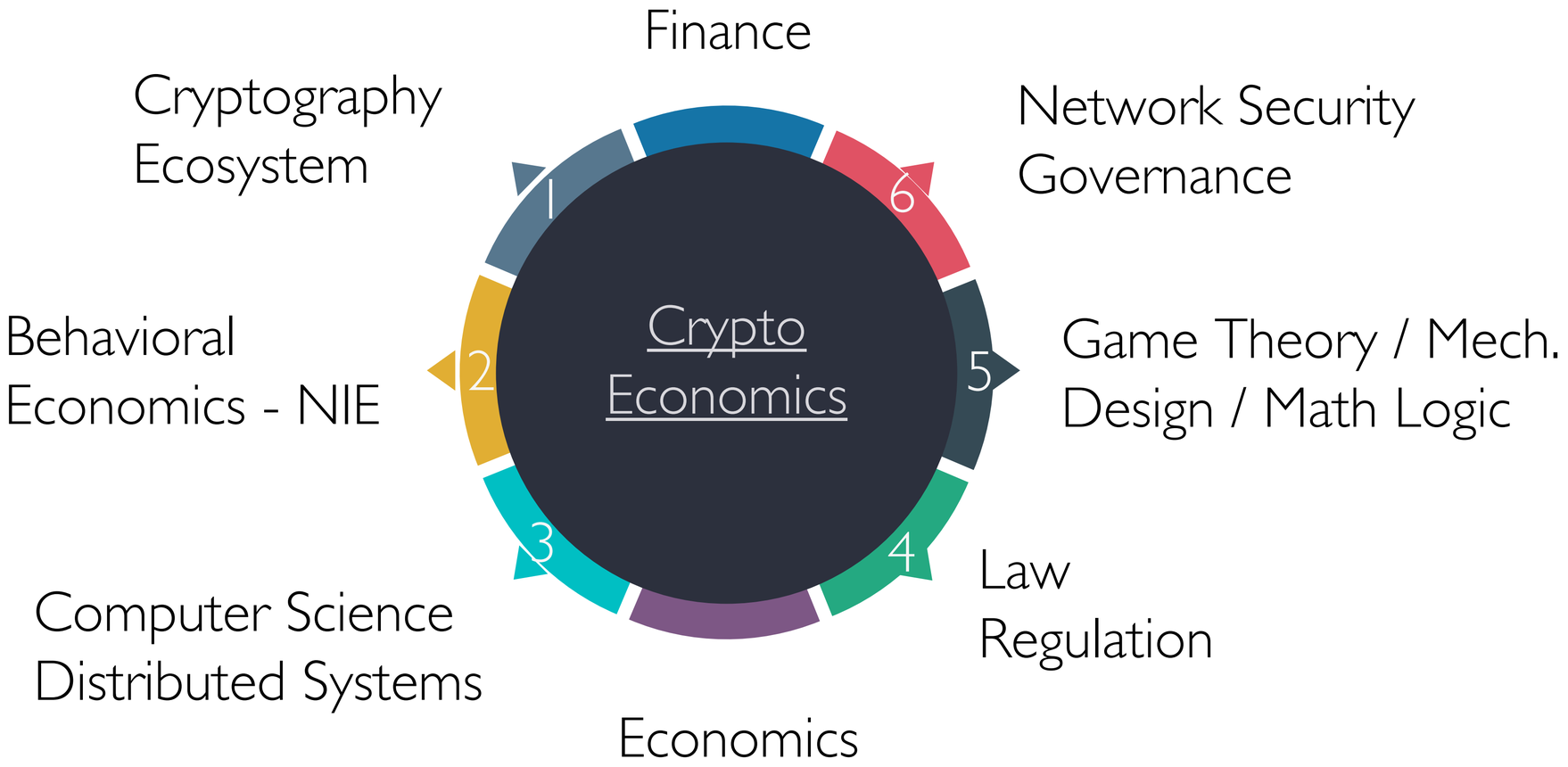
Birth of a new Discipline: Crypto Economics



Crypto Economics Distinguished

- "A formal discipline that studies protocols that govern the production, distribution, and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols." Vlad Zamfir
- Crypto economics: monetary policy via the creation of new tokens or currencies + mechanism design via the distribution and allocation of tokens according to economic incentives = creation of new forms of commerce & economies.

Crypto Economics – Convergence of Disciplines



The New Frontier: Blockchains as Economic Experimentation

- Every new token as the creation of a new economy with its own monetary policy and regulations plus internal rules of these new economies
- Cross-token finance: the rules governing how these new currencies exchange for other monies both crypto and fiat.
- Computational Infrastructure for blockchain economic laboratory:
  - The ledger for cryptocurrency transactions uses cryptography
  - Trust between counterparties via distributed (consensus) algorithms & cryptography.
- Crypto economics has most in common with mechanism design, a field related to game theory. In game theory, we look at a given strategic interaction (a "game") and then try to understand the best strategies for each player, and the likely outcome if both players follow those strategies

Blockchains as Economic Experimentation

- Unprecedented laboratory conditions for Economists:
  - Crypto Economies will enable economists to study economies at the most granular scale in history
  - Impact of micro on macro (e.g. impact of change in economic incentives on token price)
  - Impact of macro on micro (e.g. impact of new token creation on individual behavior).
- Outlook?
  - Crypto enabling unified theory of micro & macro economics?
  - Theory of the firm revised? : Coase was the first to spot an enduring truth: Successful economies need both the benign dictatorship of the firm and the invisible hand of the market.
  - What will be the role of the firm in crypto economics?

Evolution of the Theory of the Firm

- Coase: firms exist to reduce transaction cost e.g. firms are a response to the high cost of using markets.
  - A well-defined task can easily be put out to the market, where a contractor is paid a fixed sum for doing it.
  - The firm is needed when simple contracts of this kind will not suffice. Instead, an employee agrees to follow varied and changing instructions, up to agreed limits, for a fixed salary.
- Impact of Crypto Transaction Cost Economics
  - What is the role of the firm if the cost of using markets is lowered exponentially?
  - Lower Transaction costs for all market transactions
  - DAOs as market meritocracies unlike traditional firm
  - Peer to peer transactions facilitated by trust through technology
  - Trust enhancing devices e.g. Semada's reputation verification in decentralized autonomous and anonymous systems.

Back to Basics

CENTRALIZED

Macroeconomics:

- Overall economy – examines: employment, GDP, and inflation etc.

Microeconomics:

- Supply and demand interact in individual markets for goods and services.

DECENTRALIZED

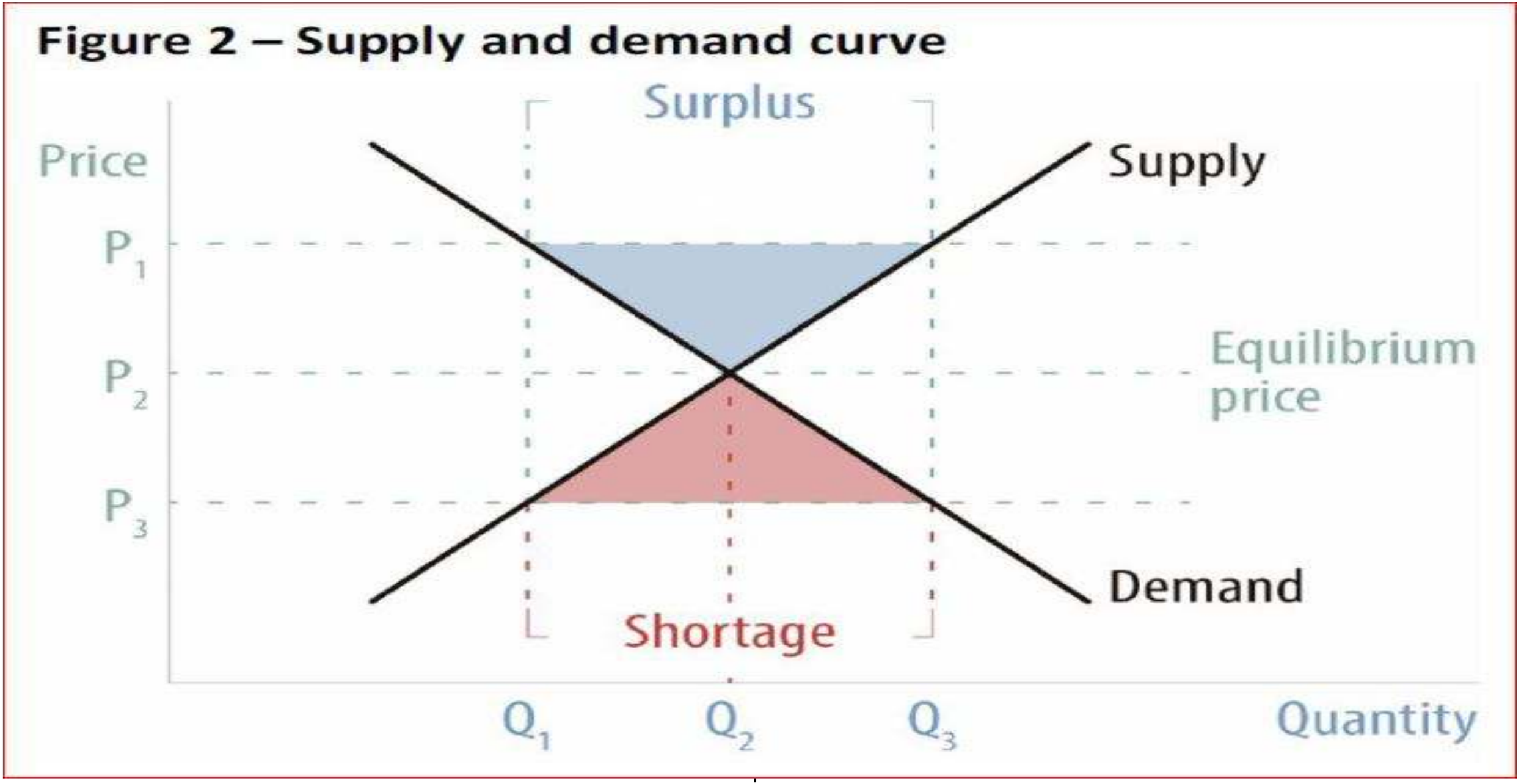
Crypto Macroeconomics:

- Timing, quantity of token creation and allocation of token
- Decision makers act as virtual central banker
- Democratization of monetary policies - market design & economic regulations were previously coordinated by policy designers, central bankers & economists

Crypto Microeconomics:

- Value proposition of tokens, e.g. how will these tokens generate value?
- Economic interactions enabled by the token
- Incentives of agents/token olders to participate in the respective token economy
- Token economy ensuring fairness and promoting honest behavior

Crypto Supply and Demand



0

Monetary Policy

CENTRALIZED

- FED Monetary Policy Mechanisms:
  - Discount rate
    - Interest rate charged by FEDs to depository institutions on short-term loans
  - Reserve requirements
    - Portions of deposits that banks must maintain either in their vaults or on deposit at a FED
  - Open market operations
    - FED purchases and sales of financial instruments
  - Interest on reserves

DECENTRALIZED

- Crypto Monetary Policy Mechanisms:
  1. Token Supply
  2. Token Release
  3. Maximum issuance of tokens
- Token Supply Management:
  - Release mechanisms for tokens help manage the supply of tokens in circulation.
  - Escrow accounts can hold tokens that were not issued in the ICO. Such escrowed tokens may be released for future issuance to finance future projects of the issuer or support operational financing.
- Impact: Maximum token issuance in combination with controlled token supply releases can result in small increases in demand driving token prices higher
- Avoidance of token price crash:
  - Token escrow accounts can provide usage and access controls that assure investors that escrowed tokens will not be issued at a discount
  - Lockup of escrowed tokens for phased releases.

Fiscal Policy

CENTRALIZED

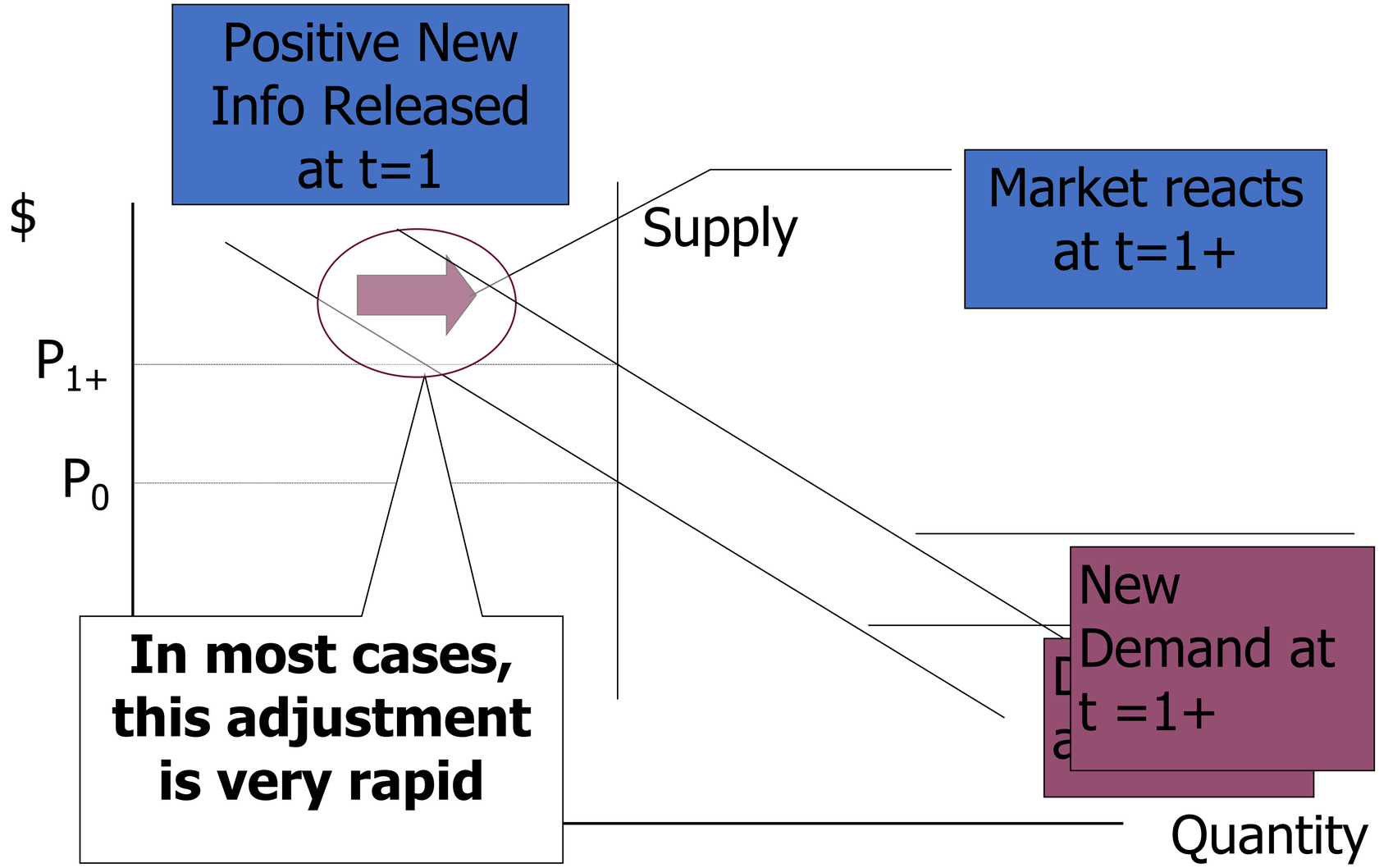
Fiscal policy tools:

- Government spending policies
  - To increase business activity in an economy, it can increase the amount of money it spends, often referred to as "Stimulus" spending (as opposed to "deficit spending")
- Government tax policies
  - Stimulate economy by lowering taxes
  - By increasing taxes, governments pull money out of the economy and slow business activity

DECENTRALIZED

- Quasi fiscal policy tool of <u>adjusting commercial benefits of tokens</u>:
  - Increase in commercial benefits associated with a token heightens aggregate demand of the given token supply.
  - Commercial benefits associated with a token issuance can help offset depreciated supply scarcity, e.g. the effects of a large issuance / supply of a given token in circulation.
- Commercial benefit adjustment as quasi fiscal policy to control the flow of tokens in a given issuance through indirect economic incentives
  - Adjustments in commercial benefits can help manage operational cost changes for the issuer and the external competition with other token issuers experienced by the issuer, among other factors.
  - Adjusting the commercial benefits associated with a given token issuance avoids more drastic monetary policy intervention by way of emergency sales or building token reserves or a decrease or increase of token supply in circulation.

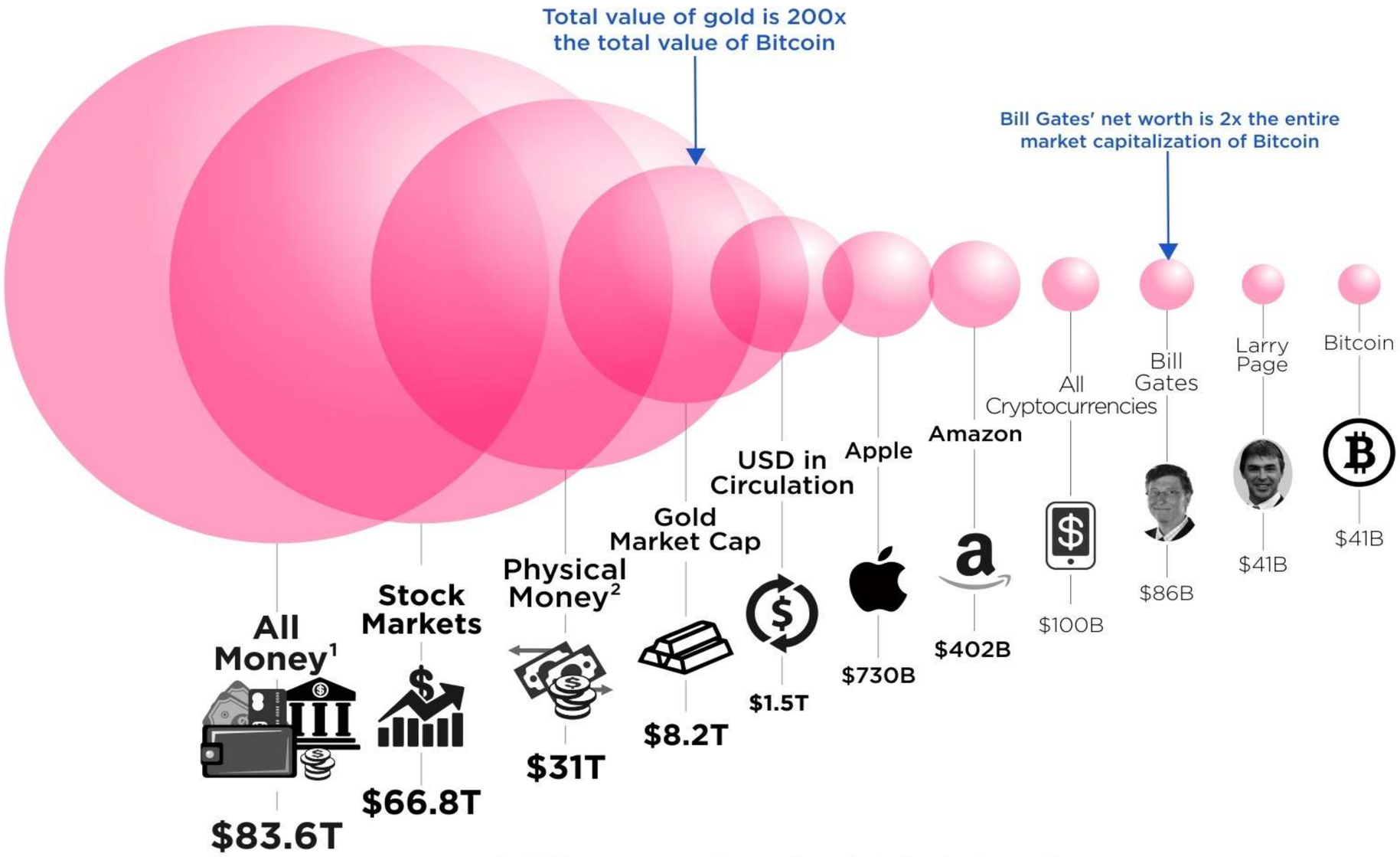
Efficient Capital Markets Hypothesis Applicable?



ECMH in Crypto?

- Illiquidity
- ECMH without crypto disclosure framework?
- Main driver without disclosure – use cases
  - Currency market
  - Token use cases – adjusting commercial benefits (quasi fiscal)
- Lack of reliable information - Crypto volatility
- Volatility mitigation

Putting the World's Money into Perspective

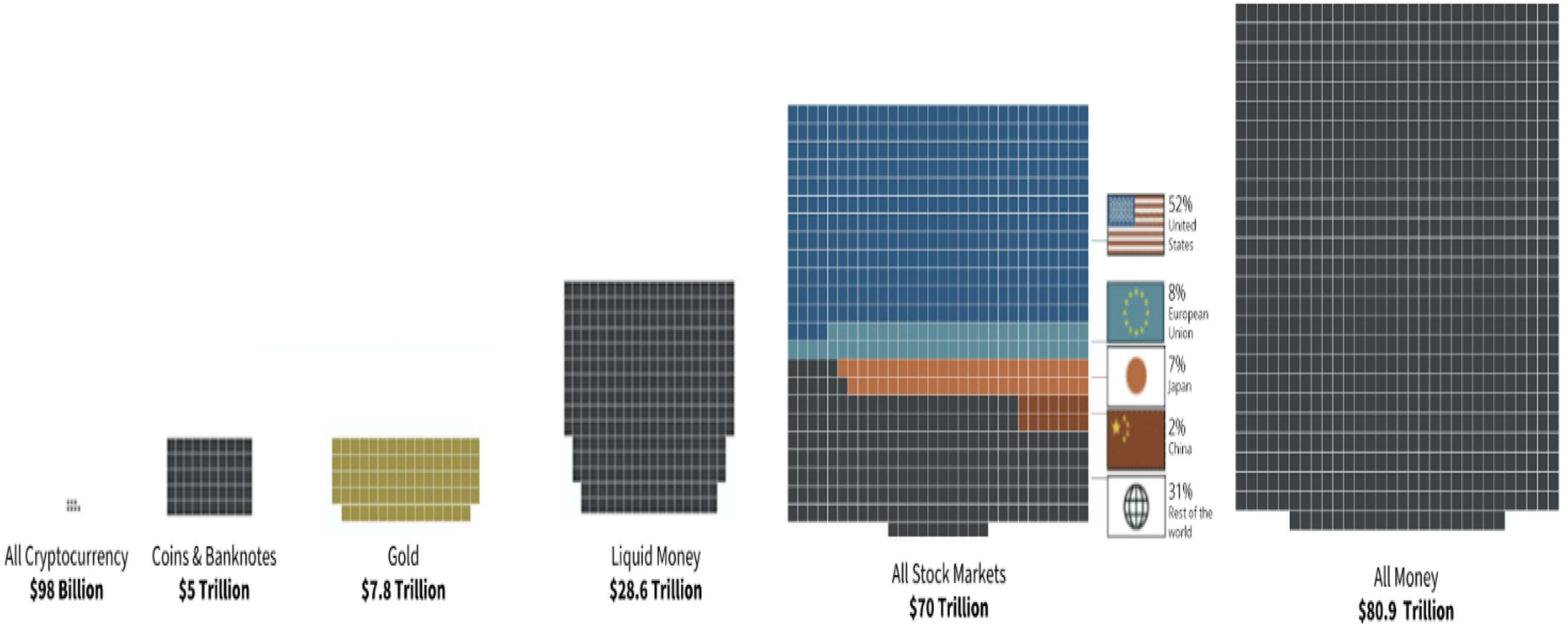


Sources:
https://howmuch.net/articles/worlds-money-in-perspective
https://coinmarketcap.com
https://www.forbes.com
https://www.federalreserve.gov
https://www.cia.gov

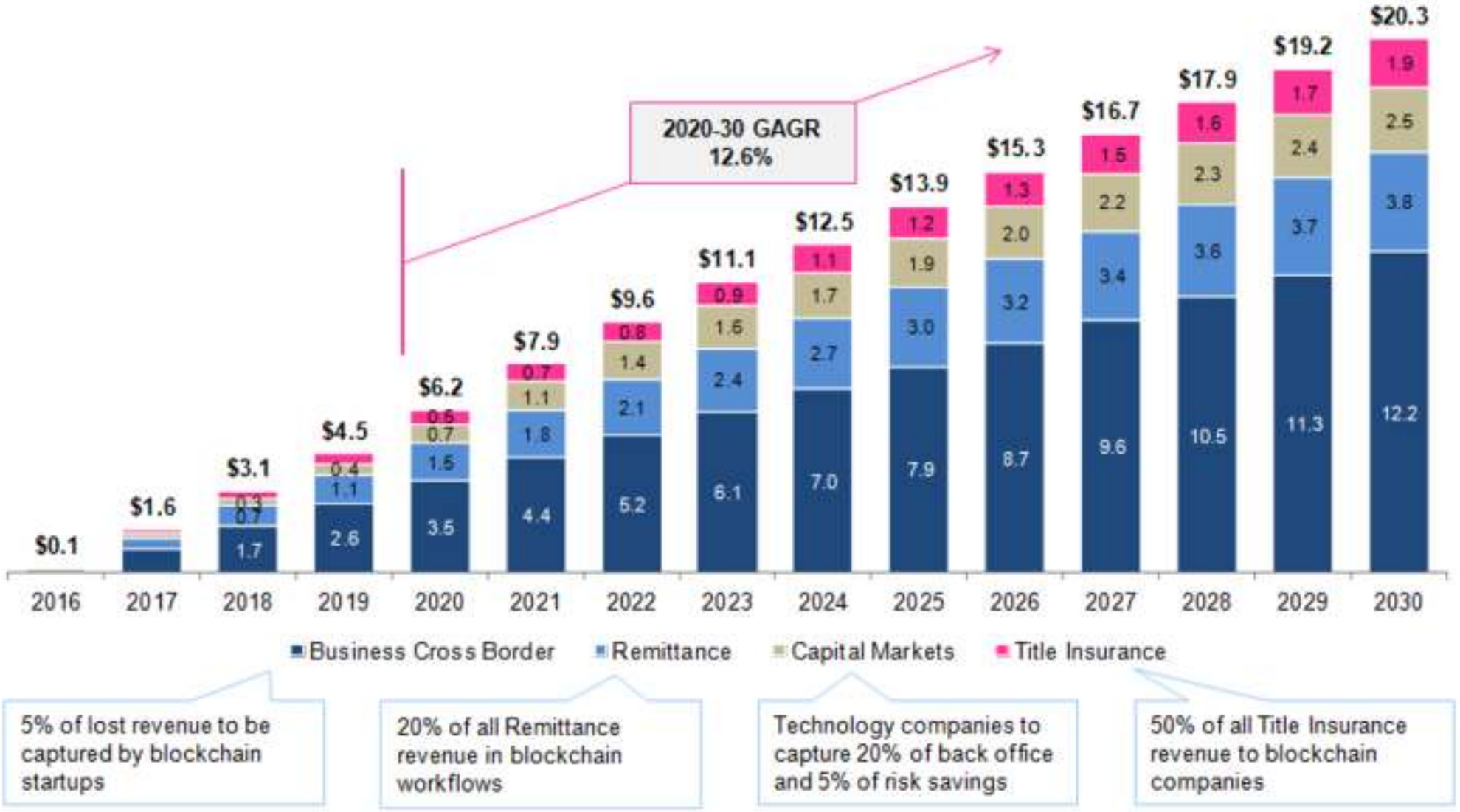
[1] All Money = money in any form including bank or other deposits as well as notes and coins.
[2] Phisical Money = money in forms that can be used as a medium of exchange, generally notes, coins, and certain balances held by banks.

howmuch.net

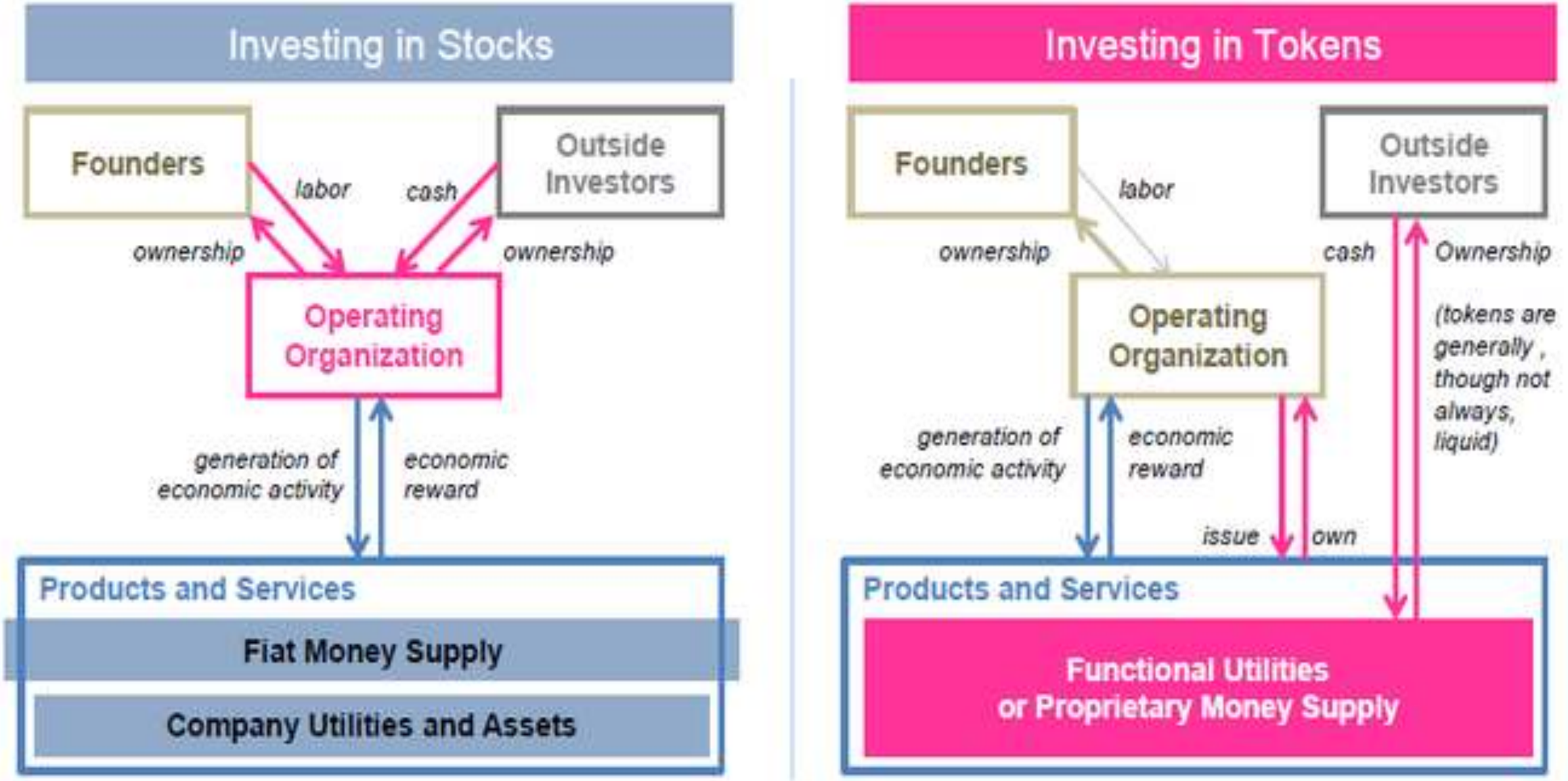
Market Background - Comparative Size



Blockchain Technology Revenue Pool ($ billions)

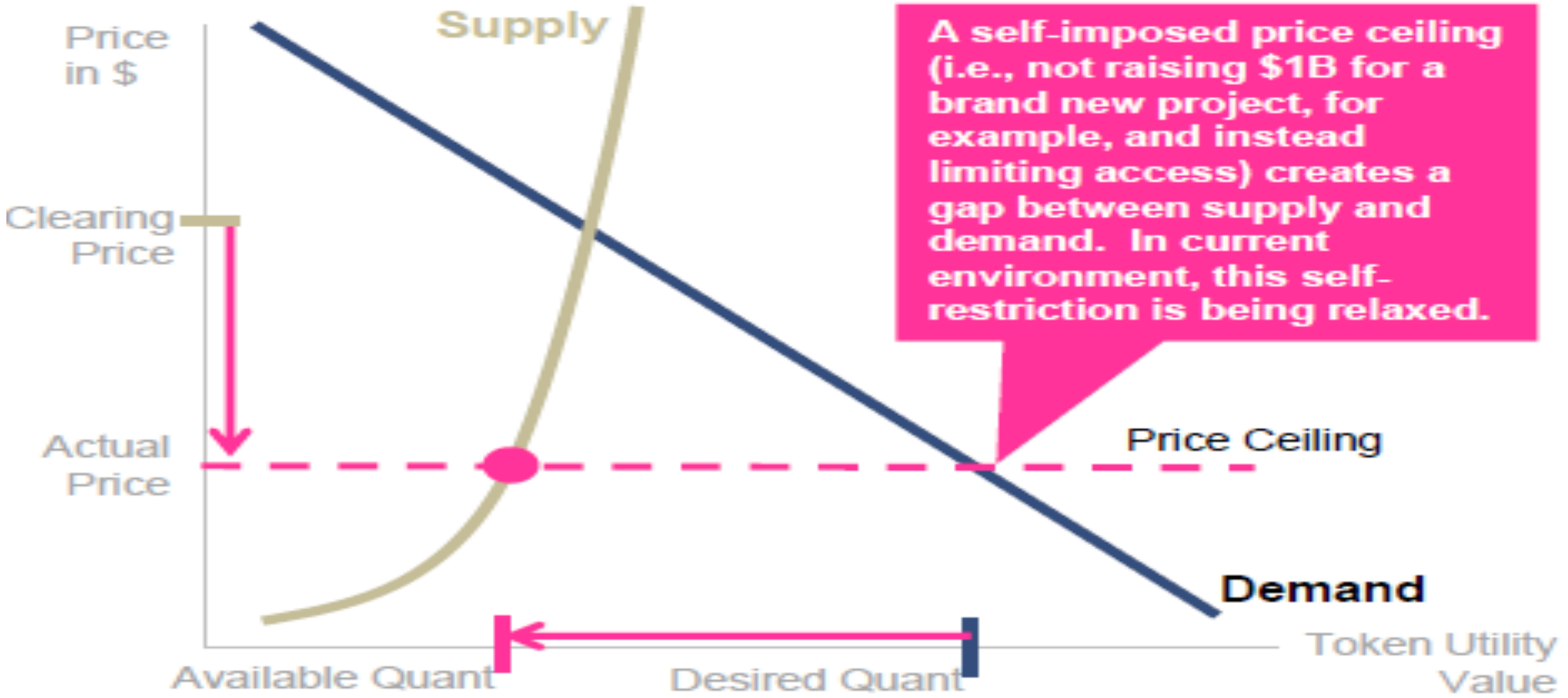


Source: Autonomous Research, Ate Group



Source: Autonomous NEXT

Aggregate Supply / Demand in Digital Tokens



Source: Autonomous NEXT, Vitalik Buterin

TOKEN MODELS

1. Dataset: Top 100 Coins (n=100) by Market Cap
2. Token fundamentals defined
3. Data trends from top 100 tokens by market cap
4. Market Cap vs. Net Realizable Value (NRV)

RESEARCH TEAM

Wulf Kaal

Wulf Kaal is a leading expert at the intersection of law, business, and technology. His research focuses on Distributed Ledge Technology (DLT), crypto economics, innovation, DLT applications, smart contracts, ICOs, and the crypto evolution, including 4th generation crypto infrastructure products. Before entering the academy, he was associated with Cravath, Swain & Moore LLP, in New York, and Goldman Sachs in London, UK.

Samuel Evans

Sam Evans is a blockchain consultant, researcher, educator, and graduate of the University of St. Thomas School of Law. There, he gained a deep understanding of blockchain, private investment fund regulation and tax law. For the last few years, he has worked under Wulf Kaal doing blockchain research and has been published in various scholarly journals.

Daniel Dosch

Dosch is a blockchain consultant, researcher and graduate of the University of St. Thomas School of Law. His undergraduate background in Intercultural Studies and Organizational Leadership piqued his interest in ecosystems and governance, for which he received law school honors. Dosch's exposure to venture capital, fintech, and developing world entrepreneurship shape his skill, strategy and passion for sustainability.

Stephanie Jones

Jones is a blockchain researcher and law graduate passionate about the intersection of racial and access equality, law, economics, and business. Her technical background began with a coding emphasis in undergrad and continued under Wulf Kaal's blockchain courses. With a passion to travel, Ms. Jones hopes to connect like-minded individuals around the world to work together materializing research into practical blockchain projects.

Hayley Howe

Howe is a research assistant and incoming 1L at the University of St. Thomas School of Law. She holds a B.S. in Mathematical Economics and minors in French and Dance. Howe's interest in blockchain began with smart contracts and her background in technical and systematic analysis. Howe is particularly interested in decentralized exchanges for fraud prevention.

Top 100 Token Categories

TECHNICAL CORES	TOKEN MODELS	CONSENSUS PROTOCOLS
Blockchain-native token Implemented on the protocol level of a blockchain. *Example: Bitcoin*	**Currency** Intended to be a pure currency *Example: Bitcoin*	**Proof of Work** Block validation work is performed by the first miner to solve a hash problem and is rewarded with some amount of the native token. *Example: Bitcoin*
ERC20 token Implemented in a cryptoeconomic protocol on the Ethereum blockchain. *Example: Binance Coin*	**Stablecoin** Pegged to some external value, generally to promote consistent trading utility *Example: Tether*	**Proof of Stake** Like PoW, but miners may only process a volume of transactions correlated to their holdings/stake of the native token. *Example: Peercoin*
Other, non-native protocol token Implemented in a cryptoeconomic protocol on another blockchain *Example: Komodo*	**Utility** Enables specific functions in a network or application. *Example: Basic Attention Token*	**Delegated Proof of Stake** Block producers are elected by native tokenholders, who possess voting power in proportion to their holdings. *Example: Bitshares, EOS, Steem*
dApp token Implemented on the application level of a blockchain. *Example: Dether*	**Usage** Provides access to a digital service (similar to an API key). *Example: Ether*	**Proof of Activity** Block headers are won via a PoW miner and completed via PoS validators. The rewards are split between the miner and validators. *Example: Decred*
	Work Grants right to contribute to a system with a possibility of reward. *Example: Augur Reputation Token*	**Proof of Capacity** Miners are only allowed to validate a volume of blocks correlated to their respective amounts of available device storage space. *Example: Burstcoin*
	Asset-backed Functions as a claim on underlying physical or digital property. *Example: LAToken*	**Proof of Burn** Miners are only allowed to validate a volume of blocks correlated to the volume of non-native, previously-mined tokens they burn (like Bitcoin). *Example: Slimcoin*
	Security Intended or legally classified as a financial investment instrument under. *Example: The DAO*	**Proof of Elapsed Time** A random waiting period is established and miners “go to sleep.” The first to wake wins, validating the block and claiming the reward. *Example: Hyperledger Sawtooth*

TOKEN CHARACTERISTICS

UX and Interoperability

User-facing	Ecosystem participants handle the token directly.
Layered	Operates underneath another token, platform, chain, or etc.
Interoperability	Whether a token is 1) fundamentally restricted for use in a given ecosystem or 2) allows or intends inter-system functionality.

TOKEN CHARACTERISTICS

Underlying Value

Inherent	Proposes to be valuable independently (e.g., manufactured scarcity).
Permission to use	Enables access to services or functionality on a platform.
Permission to work	Entitles and enables holder to contribute to the system in exchange for a reward.
Asset	Represents ownership of digital or physical asset.
”Share" in enterprise	Entitles holder to revenue, voting rights and/or other traditional equity values.

TOKEN CHARACTERISTICS

Governance

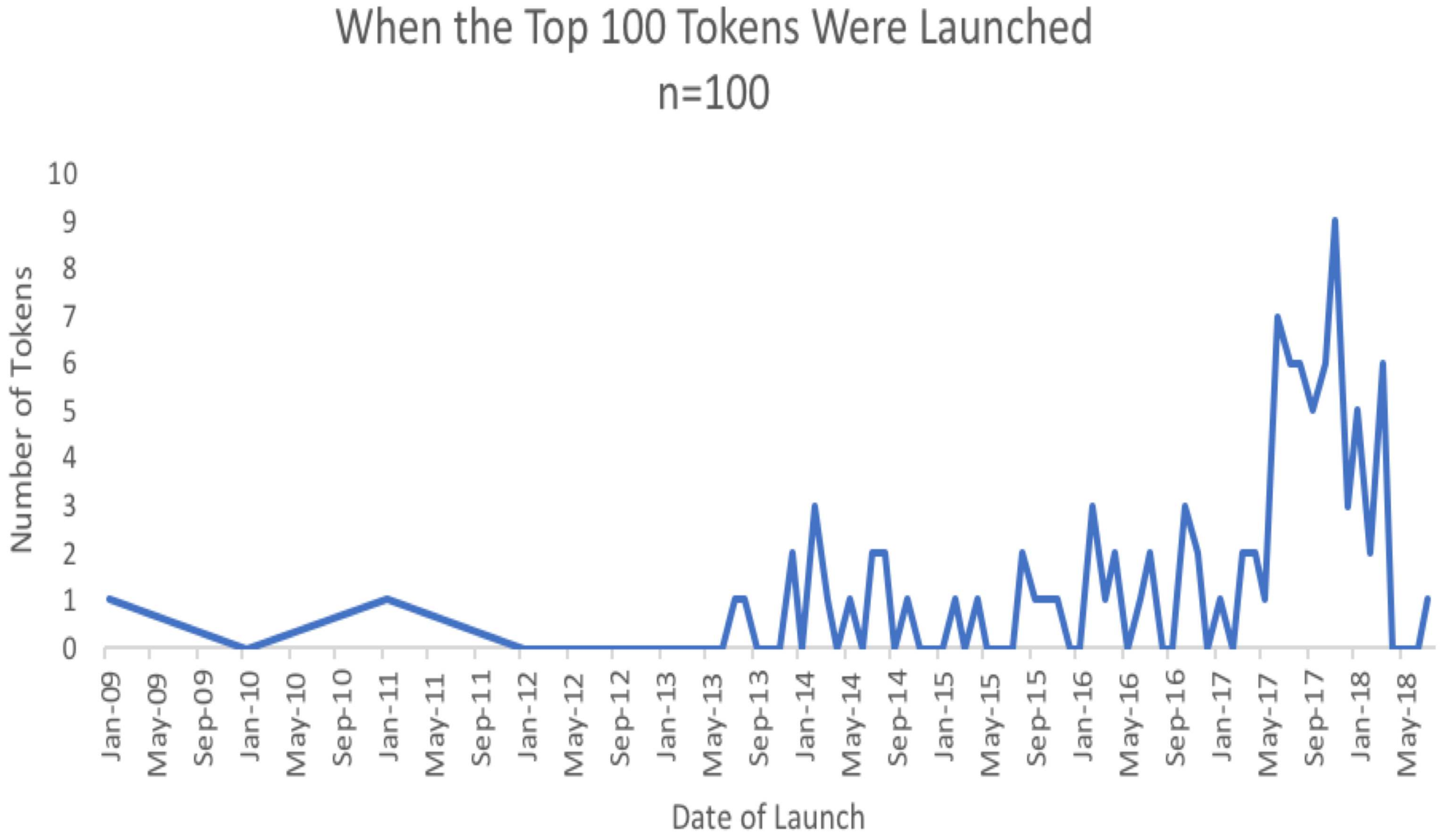
Hard Forking	Protocol changes are fundamental such that there is no backwards compatibility; the old chain is a different chain. Old and new communities compete for prominence.
Soft Forking	Protocol changes ensure interoperability between the old and new chains. Hosting organization cultivates interoperable changes and individual miners opt in or out.
Masternodes	Protocol changes are made by a subset of the tokenholders determined according to customizable criteria (e.g., holdings, activity, KYC, etc.)

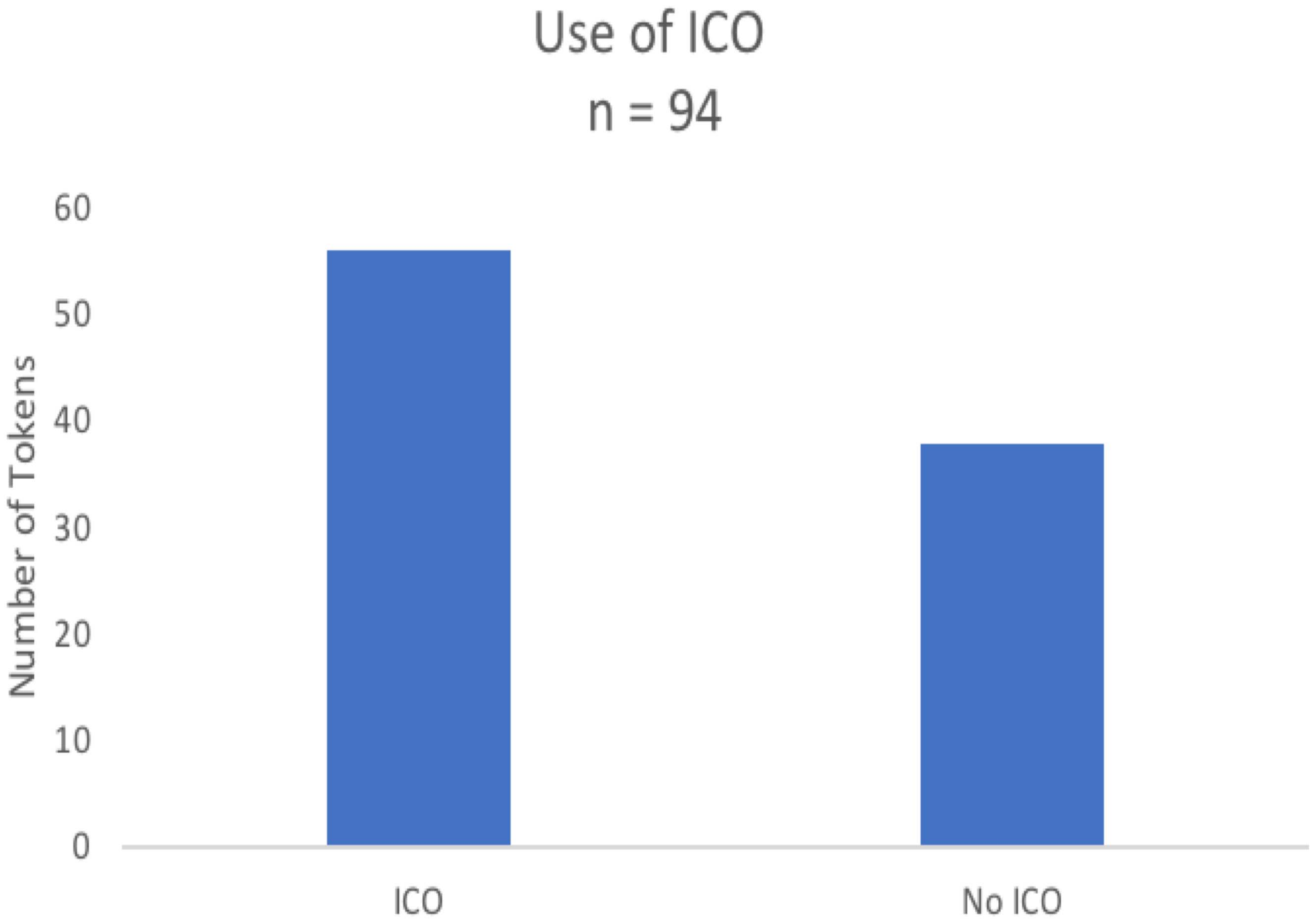
TOKEN CHARACTERISTICS

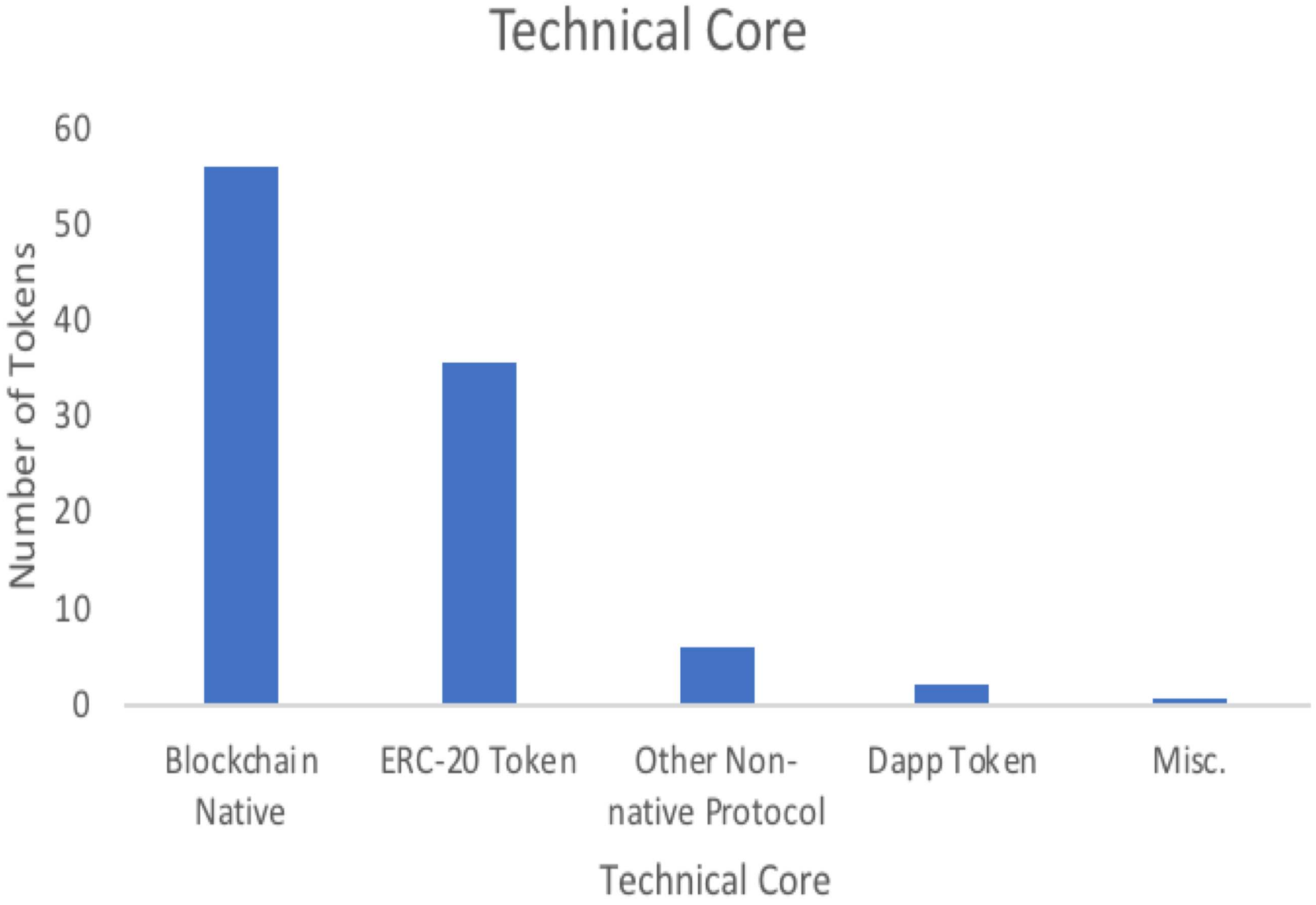
Supply and Valuation Trajectories

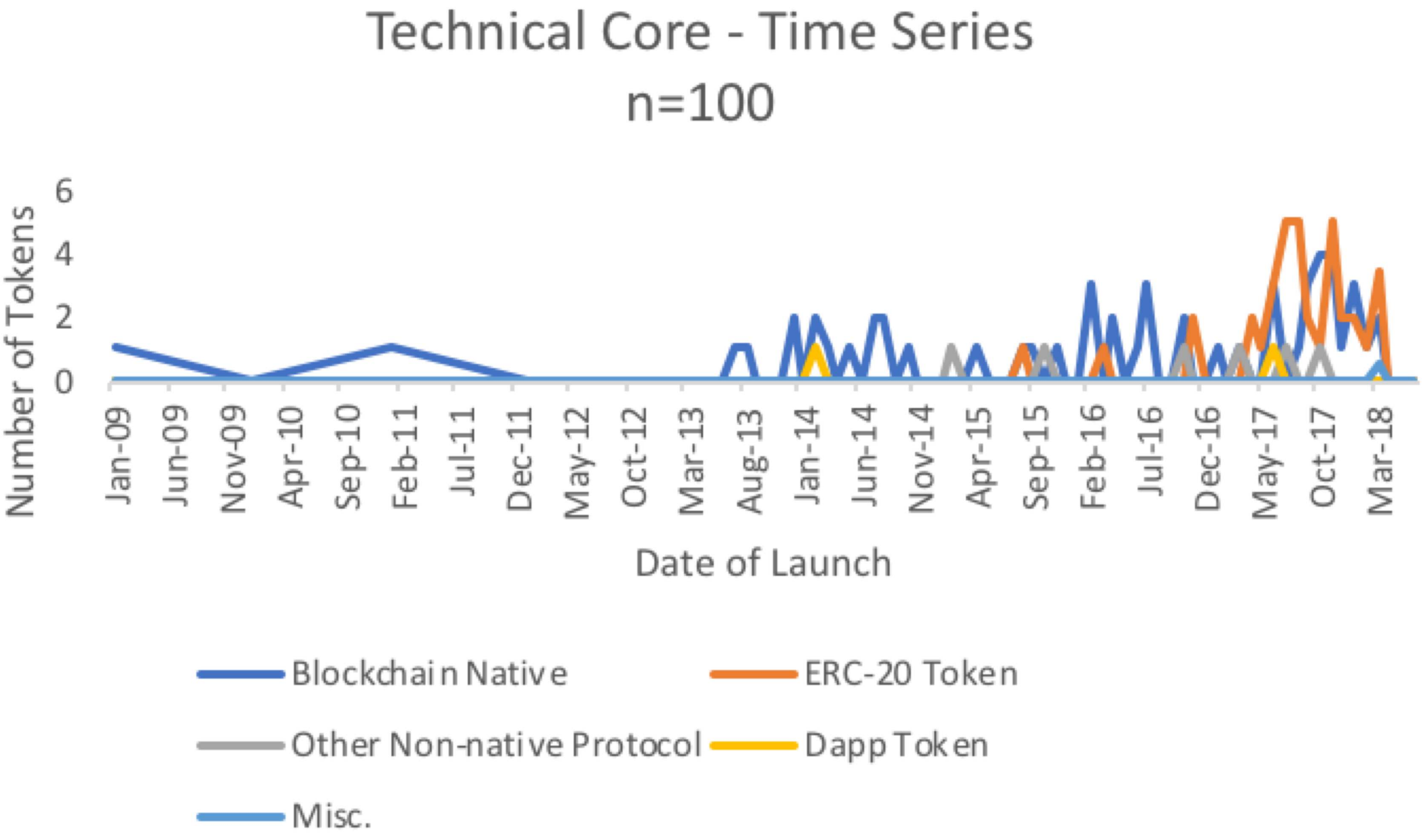
SUPPLY
Fixed: Limited ultimate supply with varying mint/release procedures.
Inflationary minting: No ultimate limit. Minting/releasing procedures vary according to project aims.
Mint-and-burn: No ultimate limit. In addition to minting, protocol destroys tokens to regulate supply.
Pegging: Minting and/or burning tightly correlate supply to correlate with some external marker (e.g, USD, Bitcoin, some specific price).

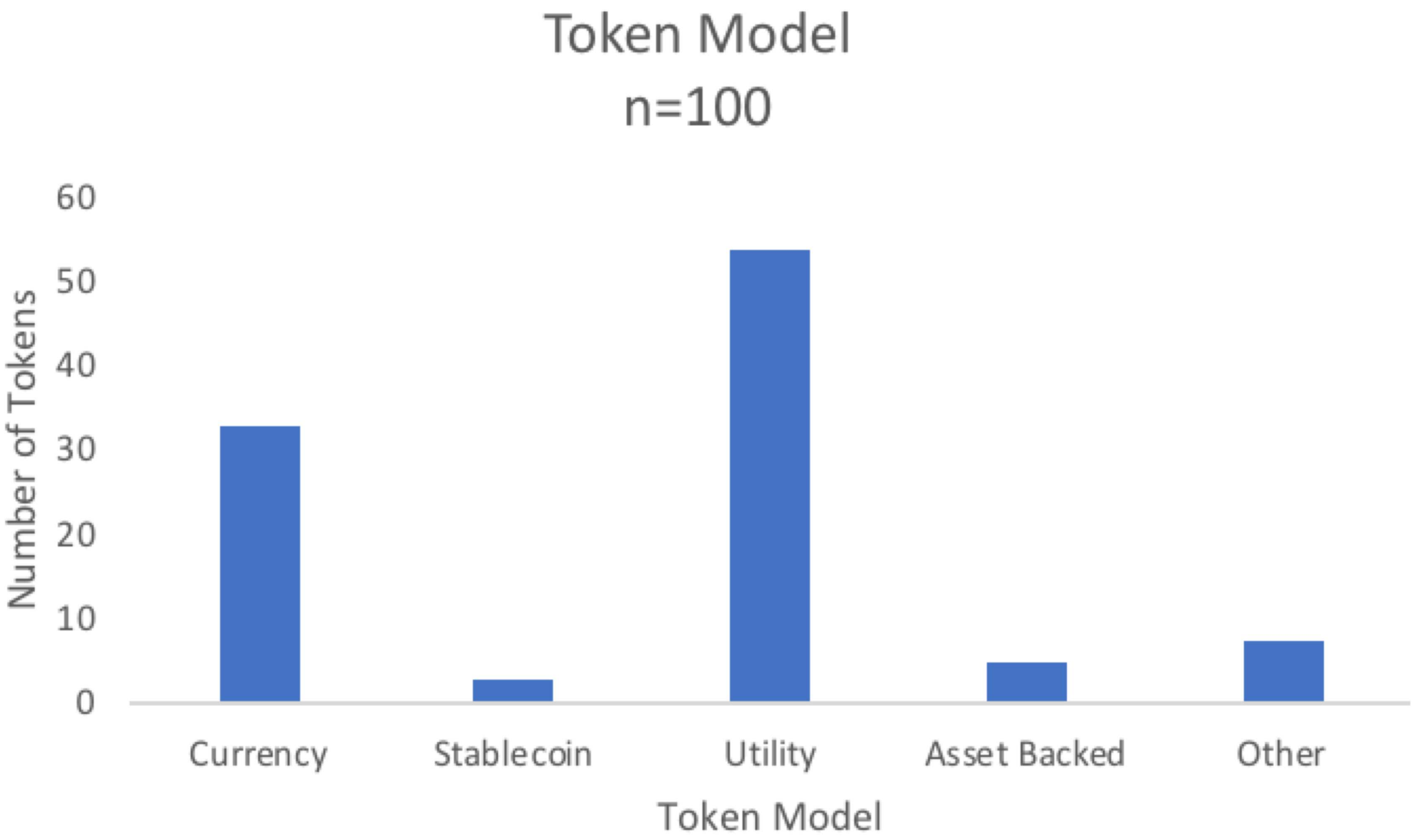
VALUATION TRAJECTORY
Inflationary: Price expected to decrease incrementally or is regulated according to minting/releasing procedure.
Deflationary: Price expected to increases because of fundamental scarcity.

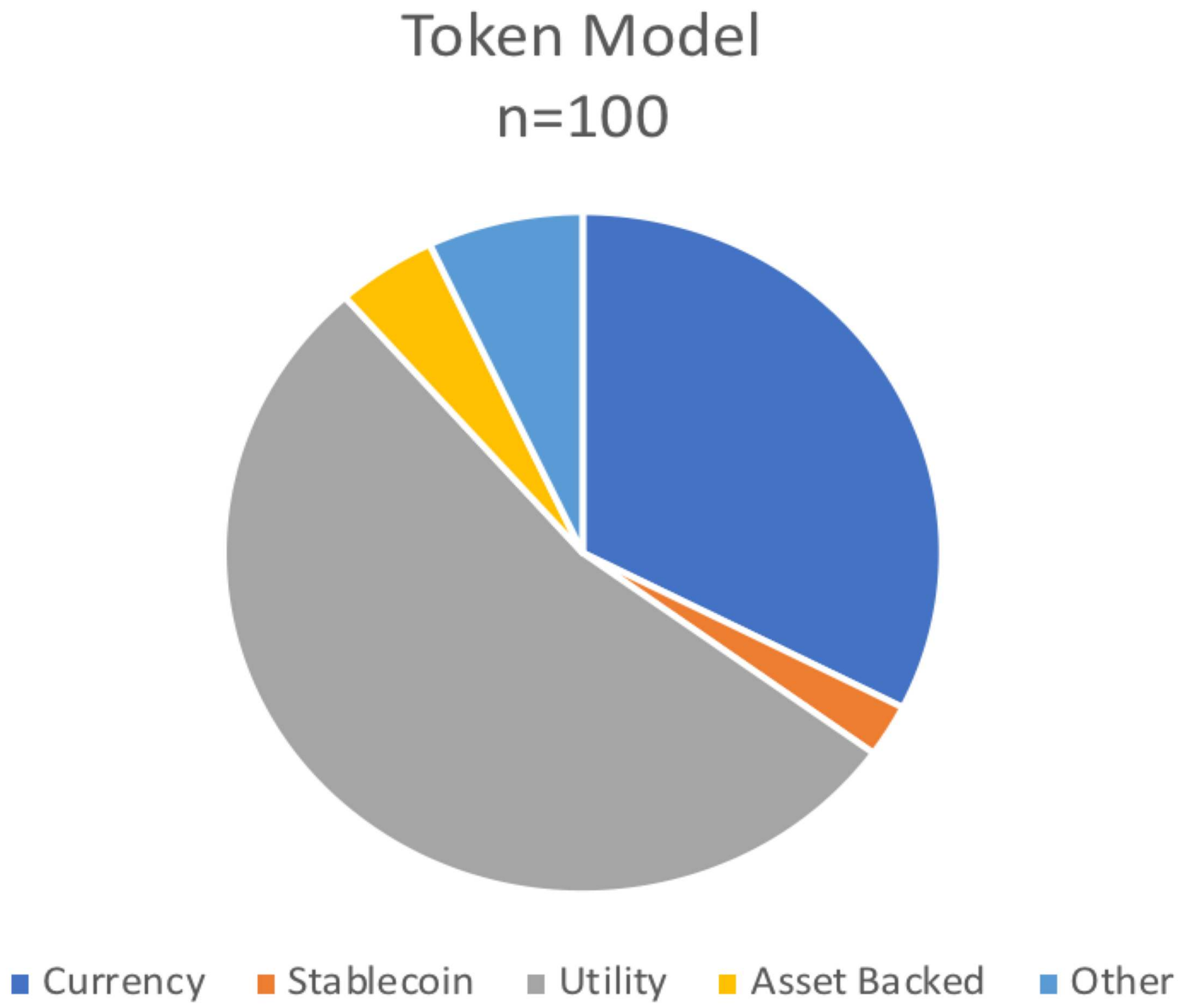

When the Top 100 Tokens Were Launched
n=100
Number of Tokens
0
1
2
3
4
5
6
7
8
9
10
Jan-09
May-09
Sep-09
Jan-10
May-10
Sep-10
Jan-11
May-11
Sep-11
Jan-12
May-12
Sep-12
Jan-13
May-13
Sep-13
Jan-14
May-14
Sep-14
Jan-15
May-15
Sep-15
Jan-16
May-16
Sep-16
Jan-17
May-17
Sep-17
Jan-18
May-18
Date of Launch

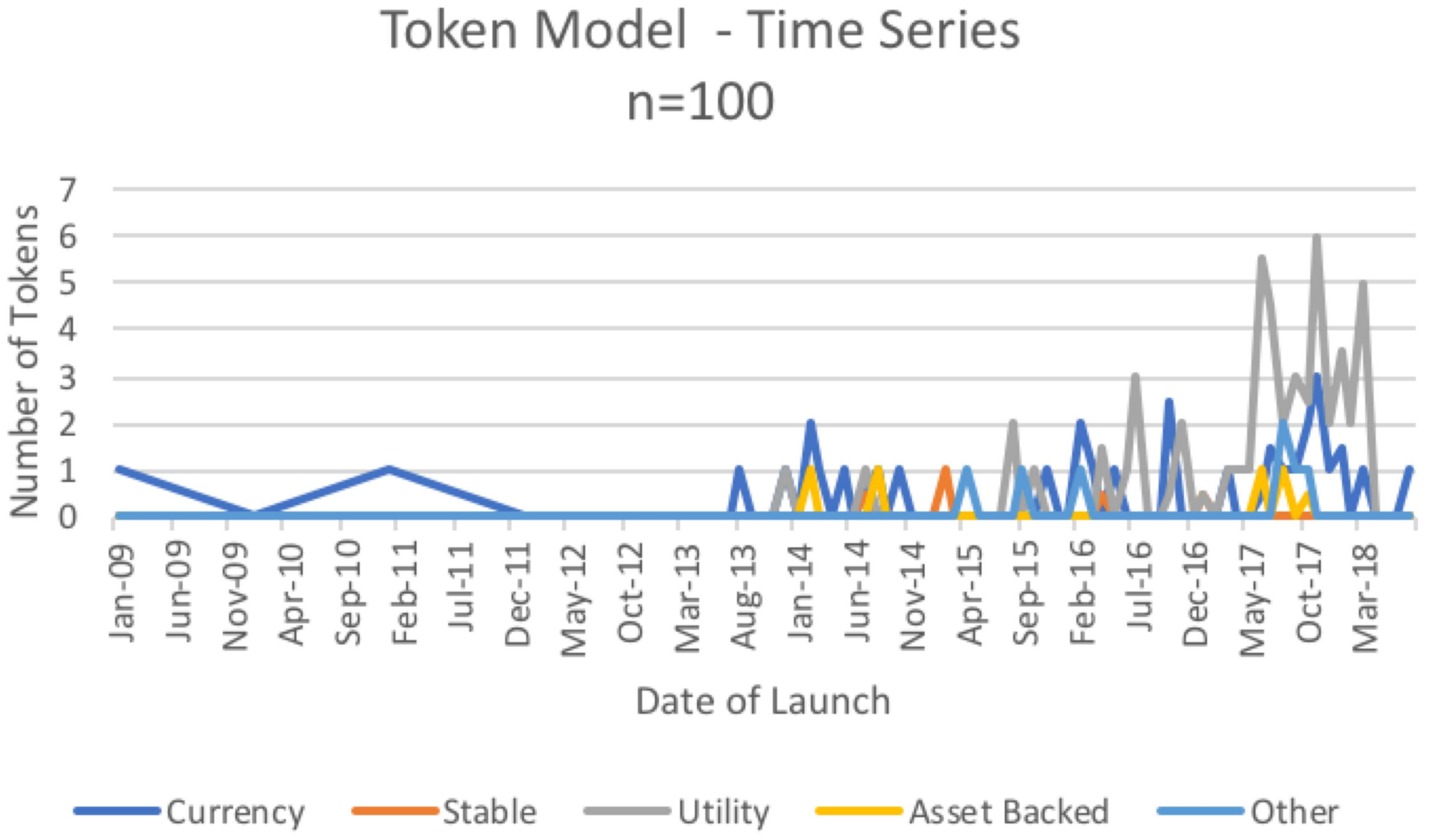

Use of ICO
n = 94
Number of Tokens
60
50
40
30
20
10
0
ICO
No ICO

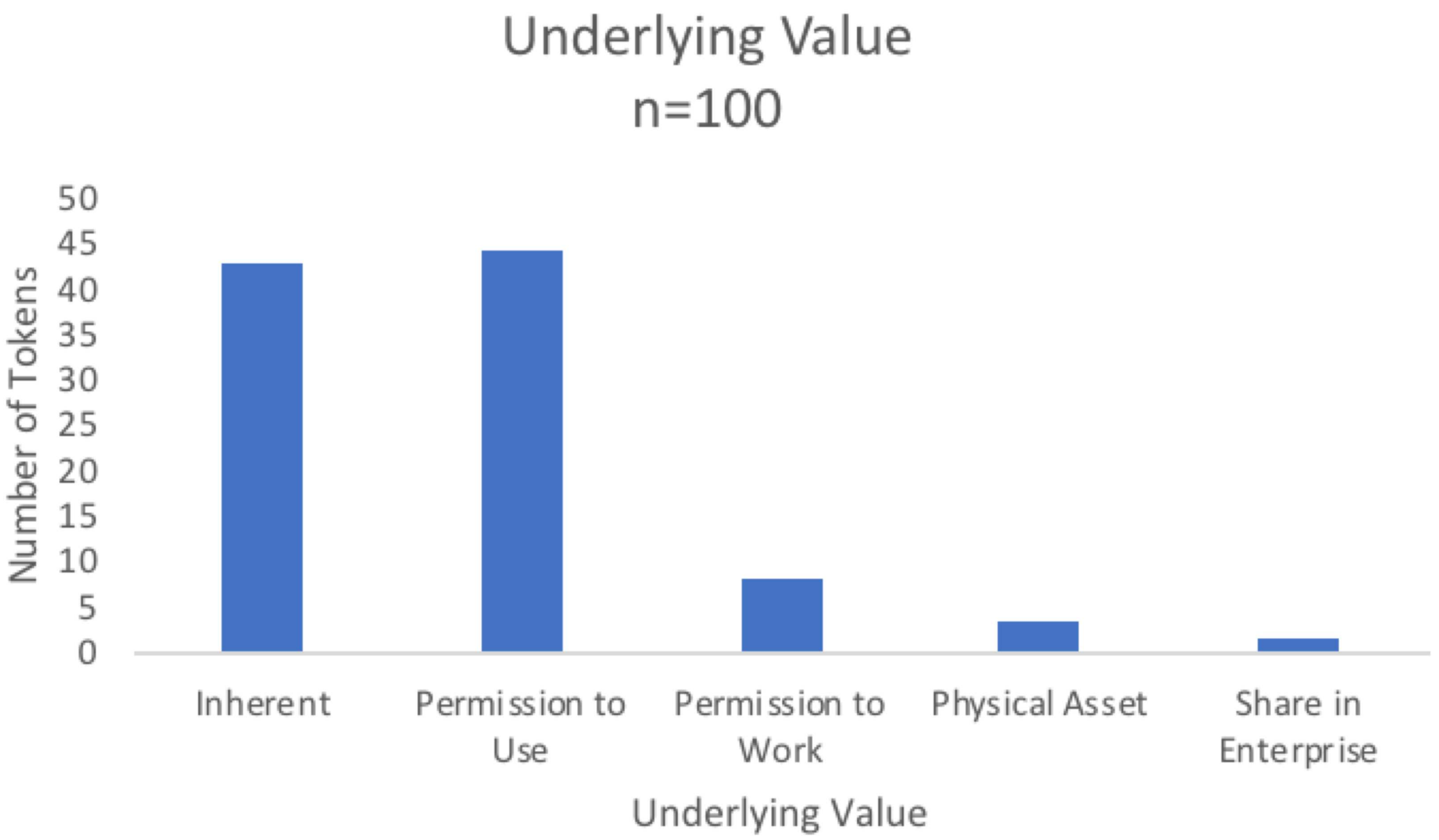

Technical Core
Number of Tokens
60
50
40
30
20
10
0
Blockchain Native
ERC-20 Token
Other Non-native Protocol
Dapp Token
Misc.
Technical Core

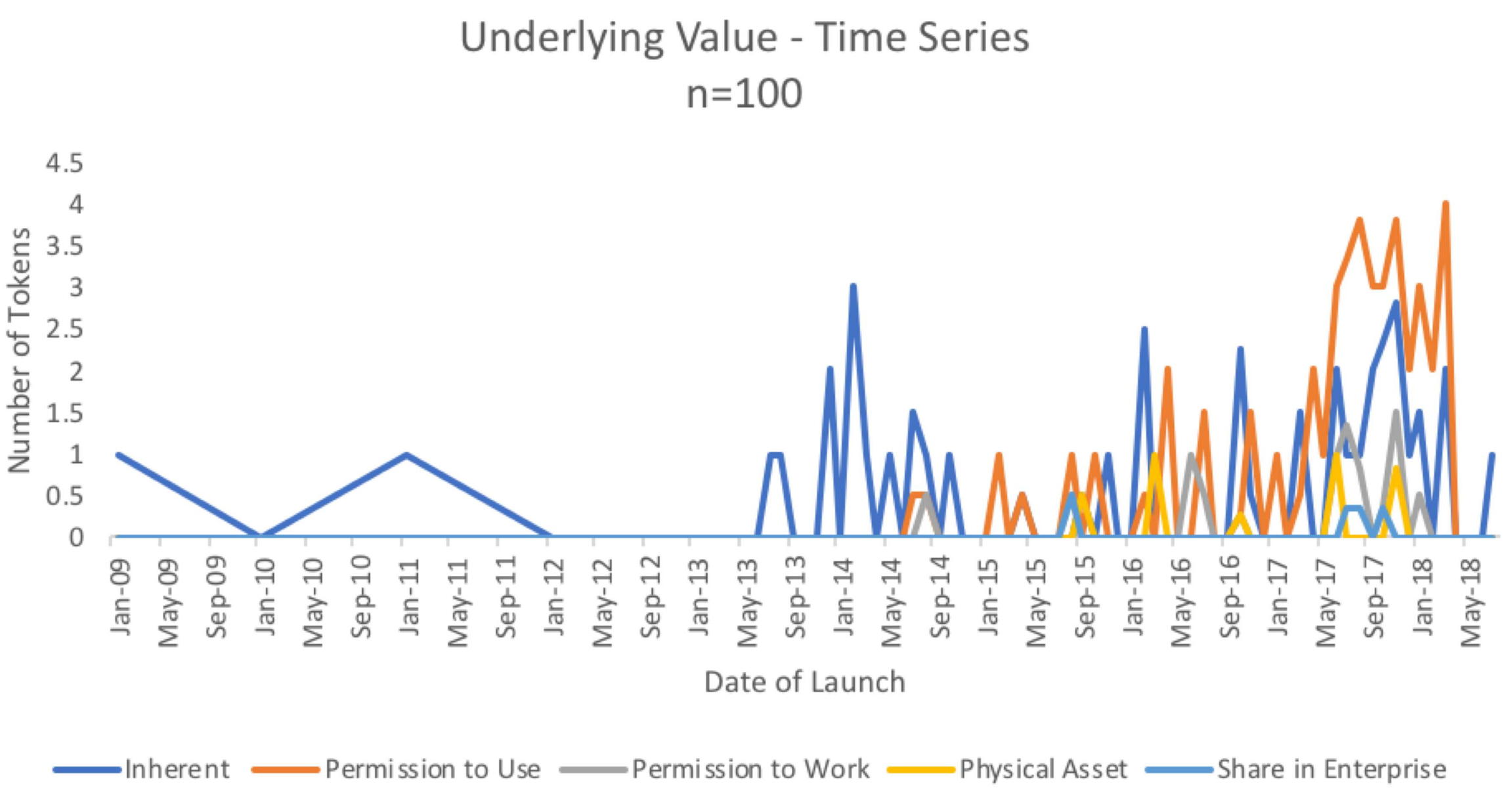

Technical Core - Time Series
n=100
Number of Tokens
0
2
4
6
Jan-09
Jun-09
Nov-09
Apr-10
Sep-10
Feb-11
Jul-11
Dec-11
May-12
Oct-12
Mar-13
Aug-13
Jan-14
Jun-14
Nov-14
Apr-15
Sep-15
Feb-16
Jul-16
Dec-16
May-17
Oct-17
Mar-18
Date of Launch
Blockchain Native
ERC-20 Token
Other Non-native Protocol
Dapp Token
Misc.

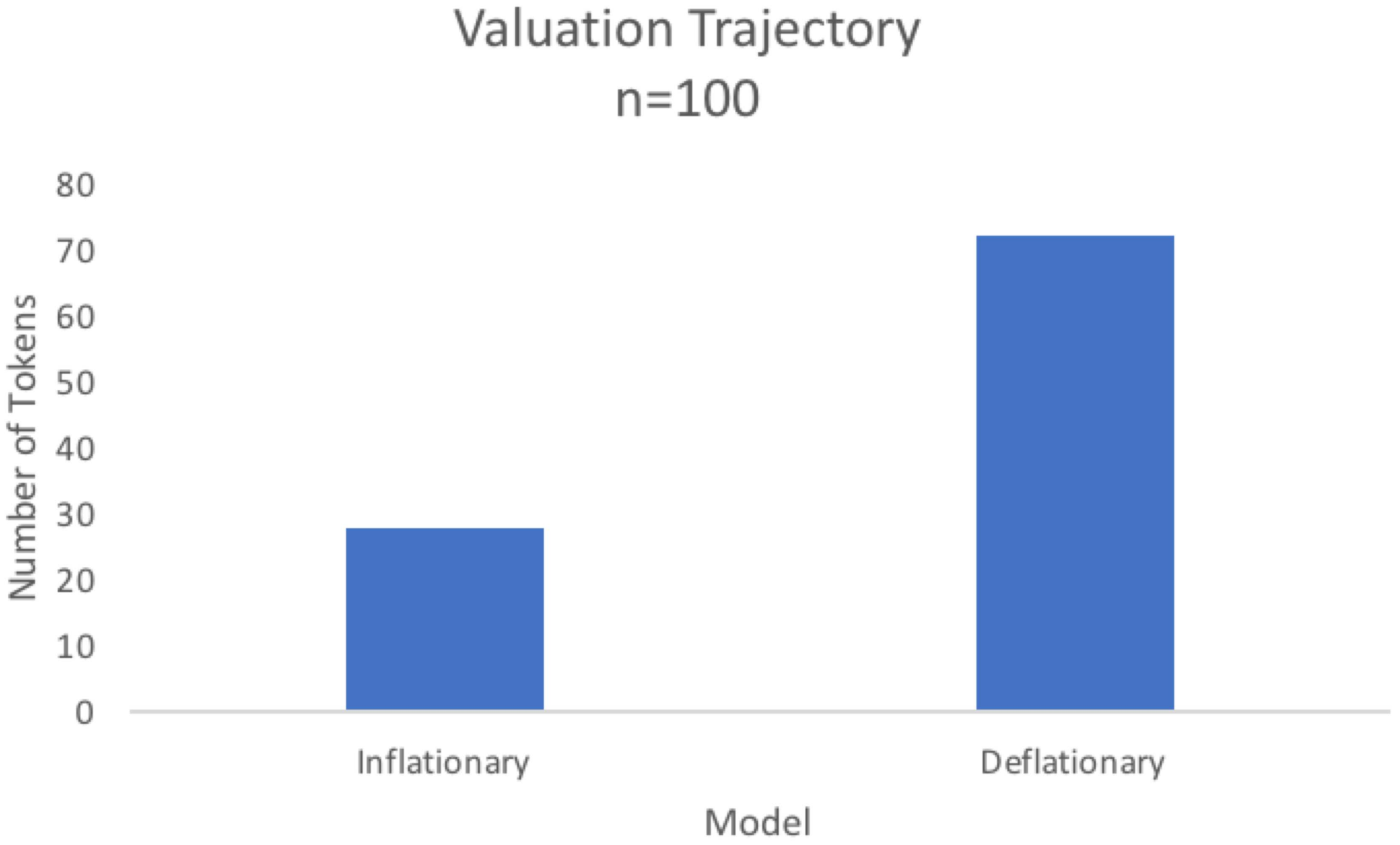

Token Model
n=100
Number of Tokens
60
50
40
30
20
10
0
Currency
Stablecoin
Utility
Asset Backed
Other
Token Model

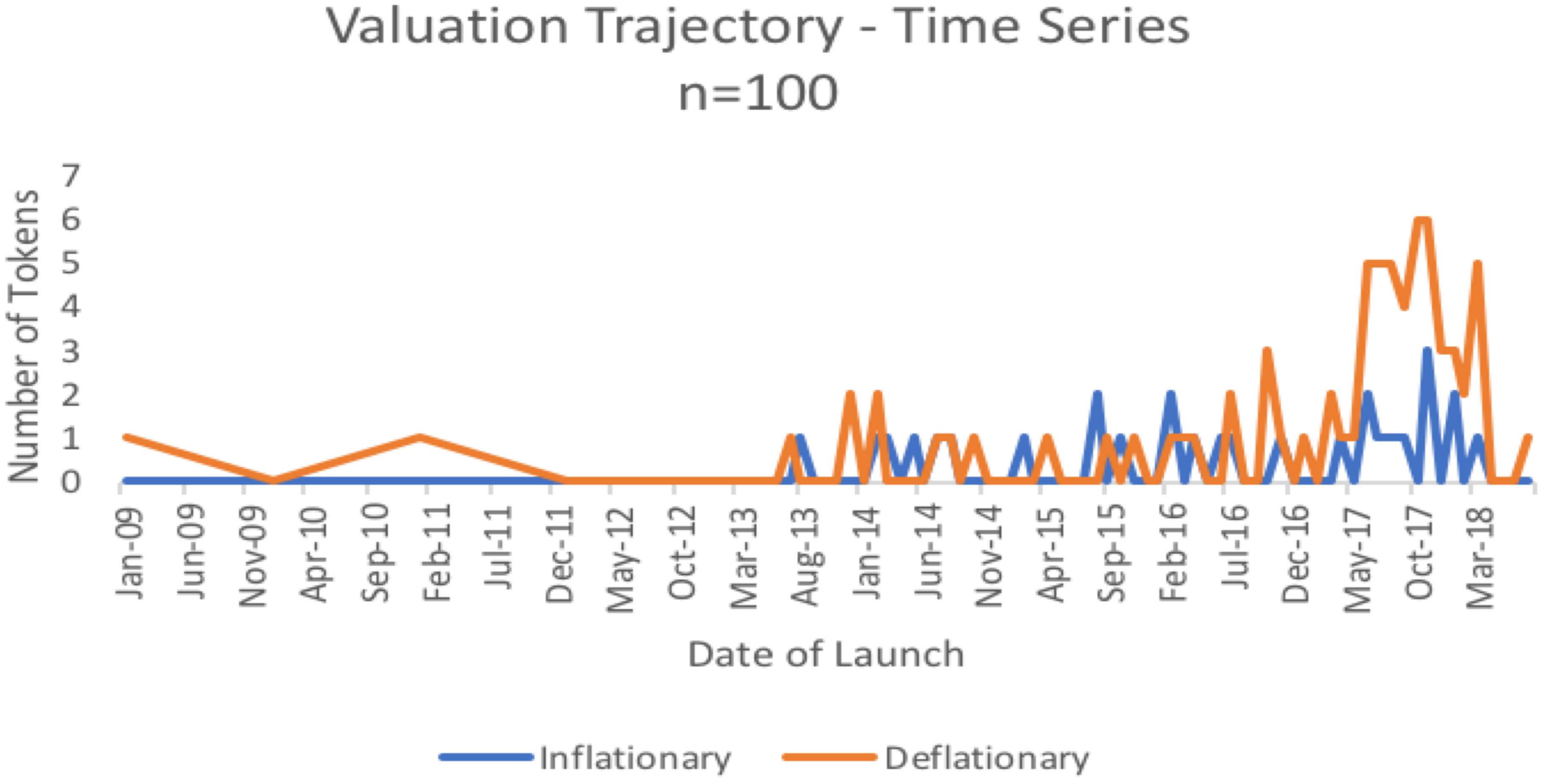

Token Model
n=100
Currency
Stablecoin
Utility
Asset Backed
Other

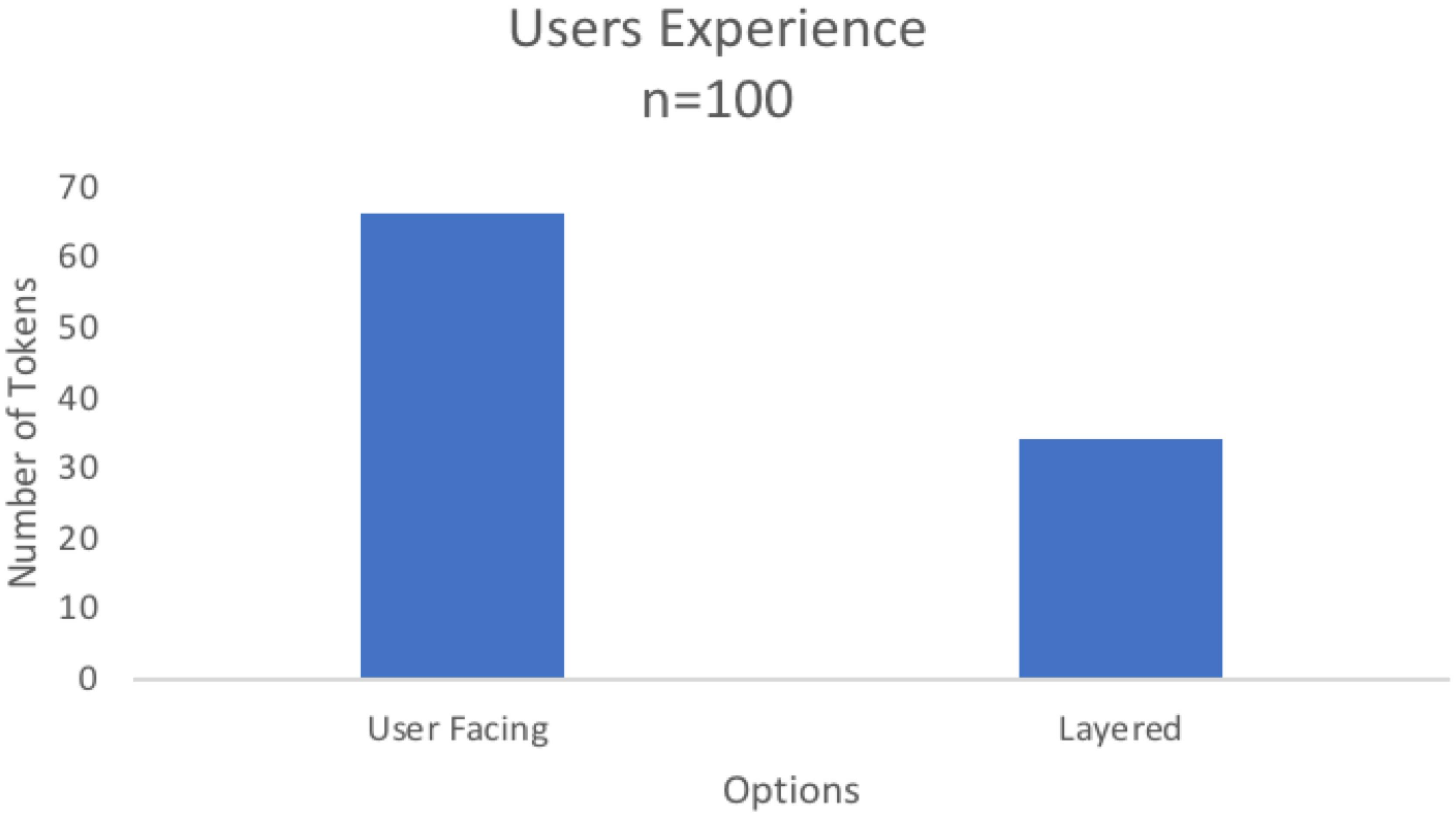

Token Model - Time Series
n=100
Number of Tokens
0
1
2
3
4
5
6
7
Jan-09
Jun-09
Nov-09
Apr-10
Sep-10
Feb-11
Jul-11
Dec-11
May-12
Oct-12
Mar-13
Aug-13
Jan-14
Jun-14
Nov-14
Apr-15
Sep-15
Feb-16
Jul-16
Dec-16
May-17
Oct-17
Mar-18
Date of Launch
Currency
Stable
Utility
Asset Backed
Other

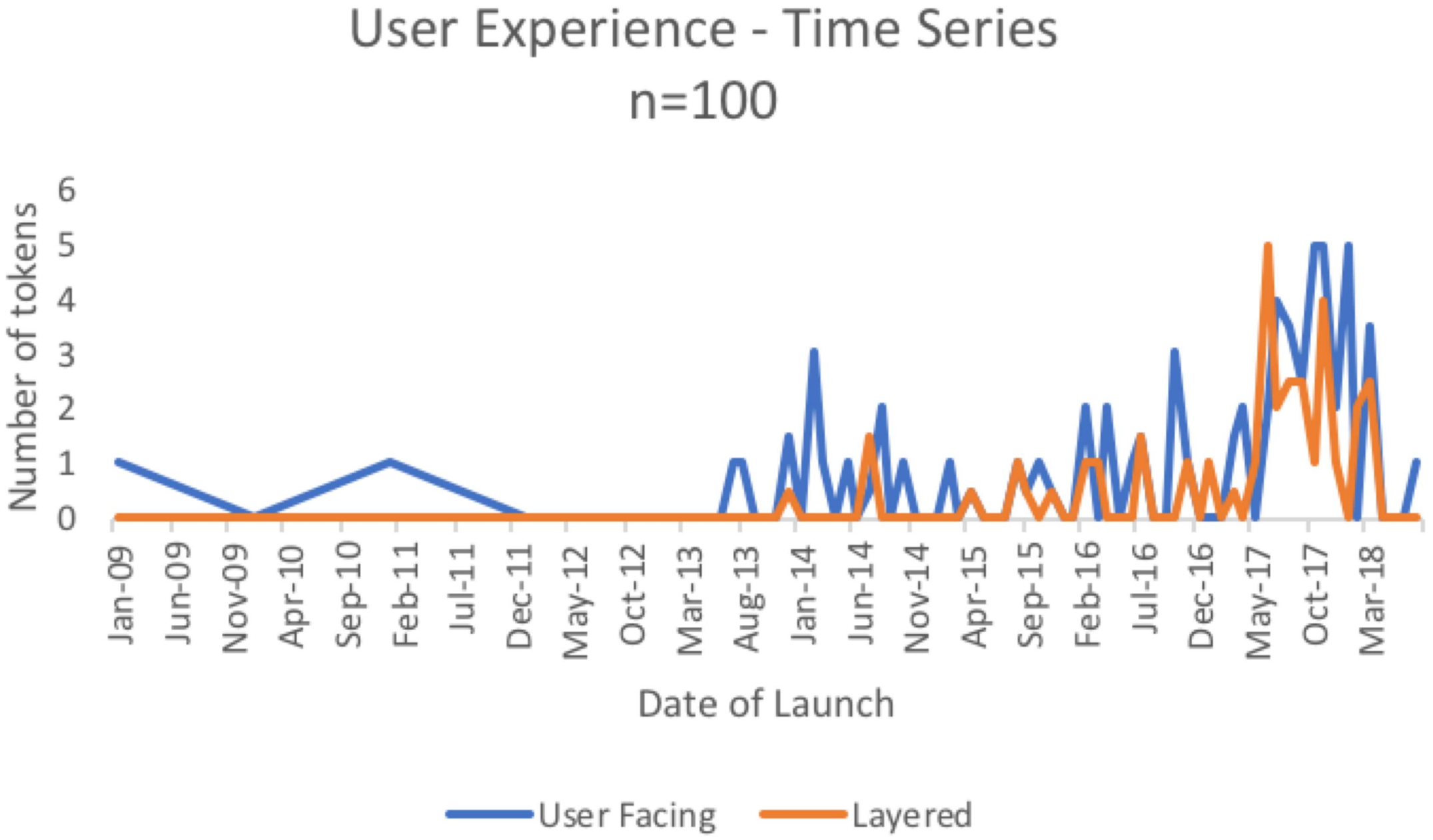

Underlying Value
n=100
Number of Tokens
50
45
40
35
30
25
20
15
10
5
0
Inherent
Permission to Use
Permission to Work
Physical Asset
Share in Enterprise
Underlying Value

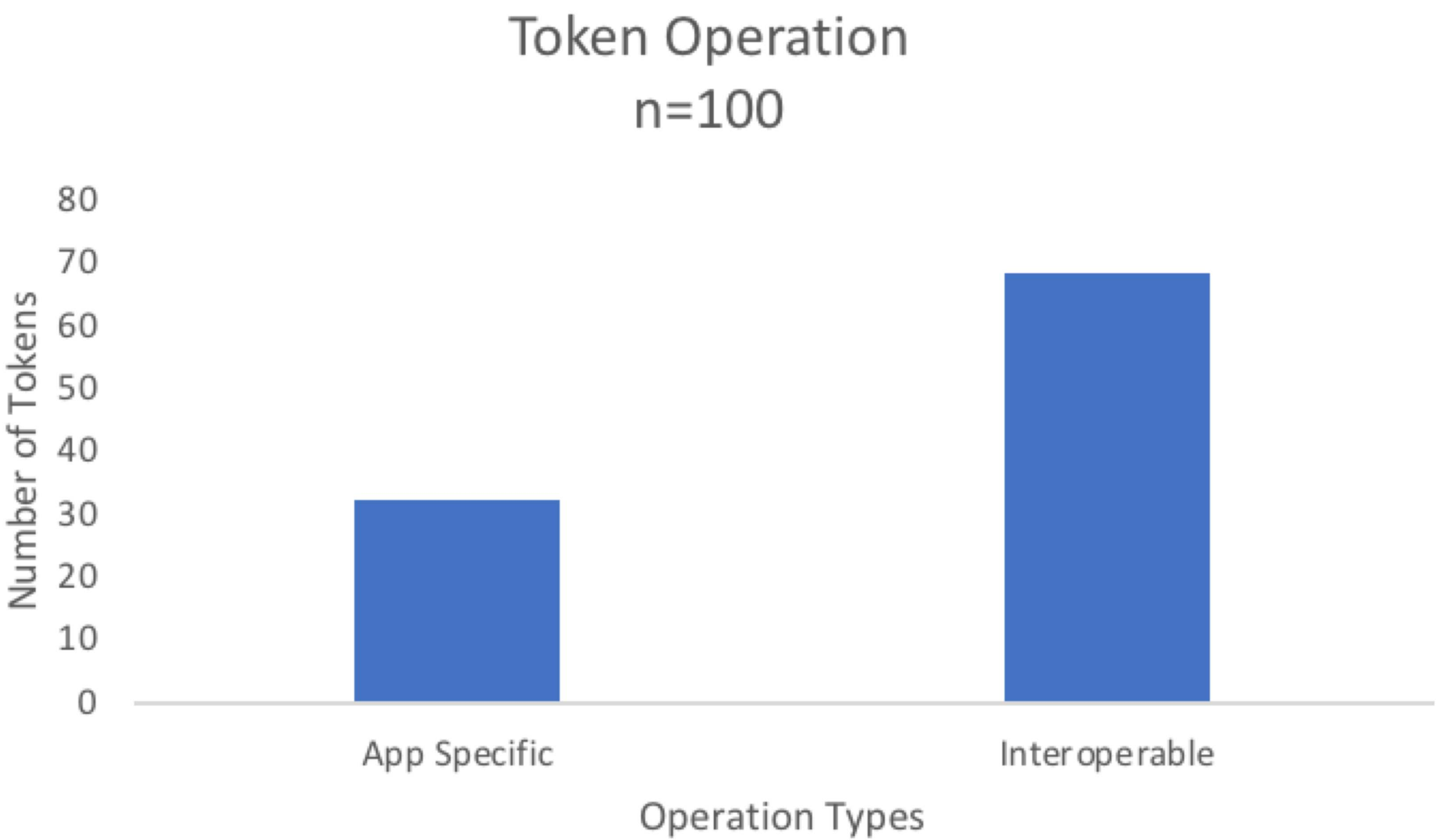

Underlying Value - Time Series
n=100
Number of Tokens
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Jan-09
May-09
Sep-09
Jan-10
May-10
Sep-10
Jan-11
May-11
Sep-11
Jan-12
May-12
Sep-12
Jan-13
May-13
Sep-13
Jan-14
May-14
Sep-14
Jan-15
May-15
Sep-15
Jan-16
May-16
Sep-16
Jan-17
May-17
Sep-17
Jan-18
May-18
Date of Launch
Inherent
Permission to Use
Permission to Work
Physical Asset
Share in Enterprise

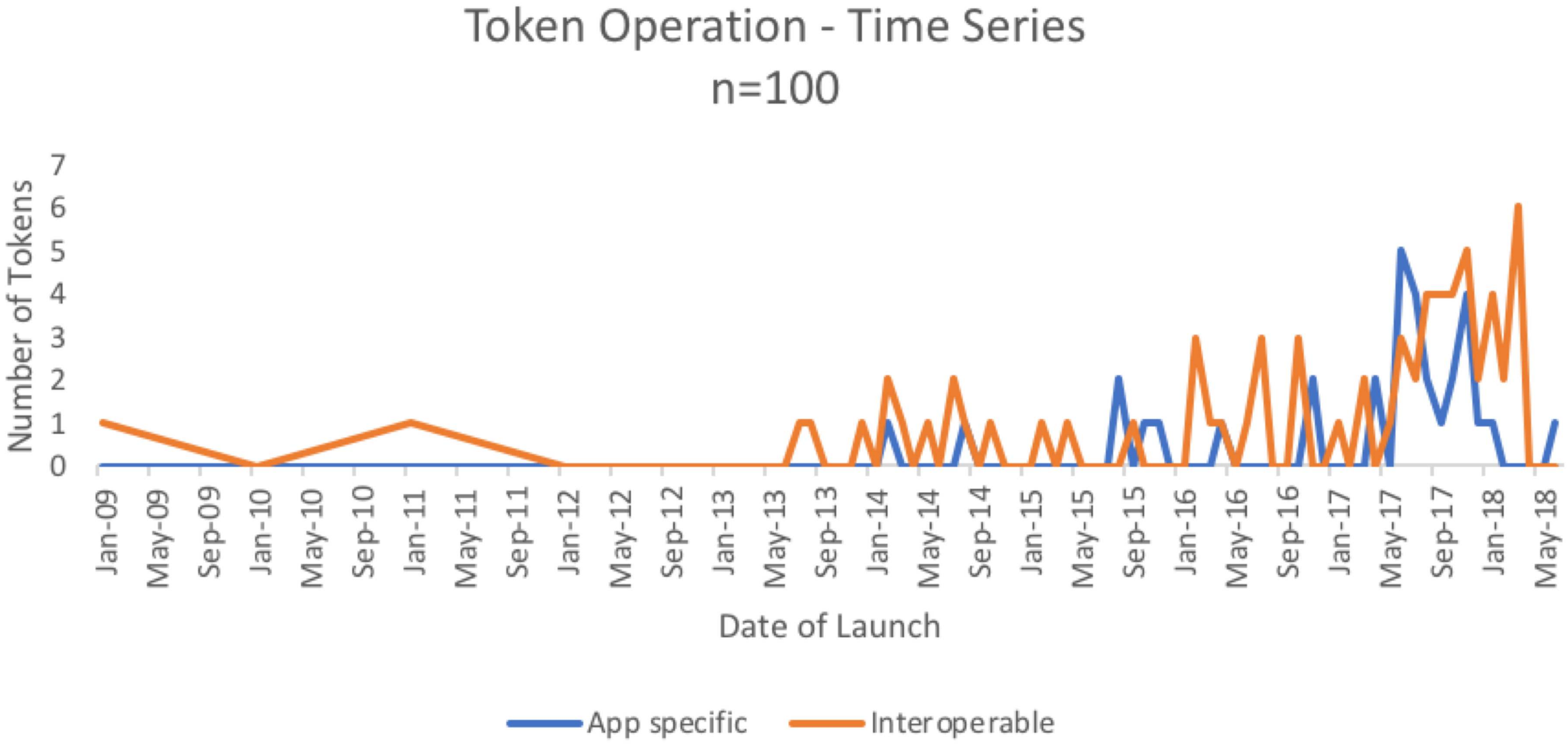

Valuation Trajectory
n=100
Number of Tokens
80
70
60
50
40
30
20
10
0
Inflationary
Deflationary
Model

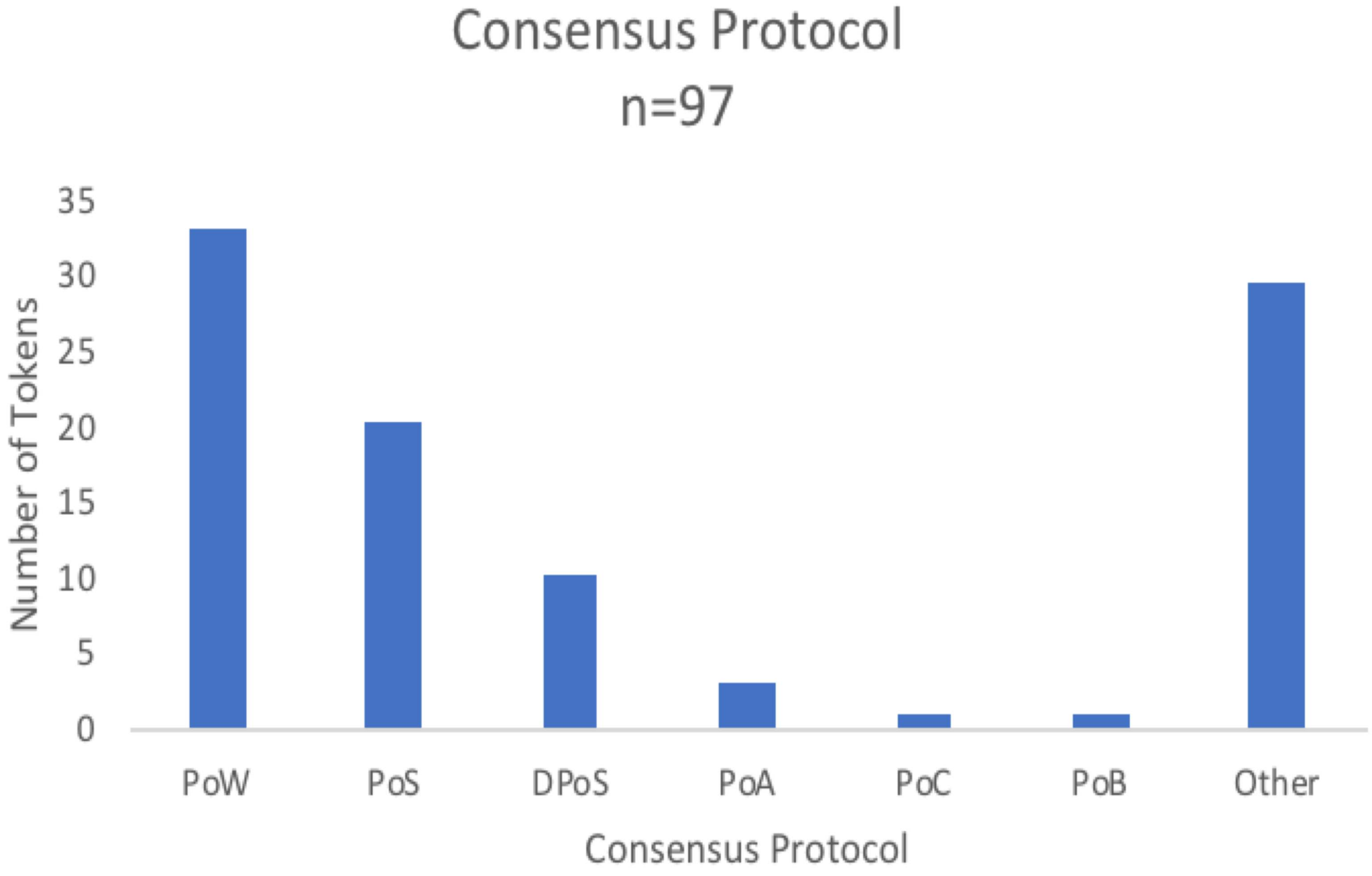

Valuation Trajectory - Time Series
n=100
Number of Tokens
0
1
2
3
4
5
6
7
Jan-09
Jun-09
Nov-09
Apr-10
Sep-10
Feb-11
Jul-11
Dec-11
May-12
Oct-12
Mar-13
Aug-13
Jan-14
Jun-14
Nov-14
Apr-15
Sep-15
Feb-16
Jul-16
Dec-16
May-17
Oct-17
Mar-18
Date of Launch
Inflationary
Deflationary

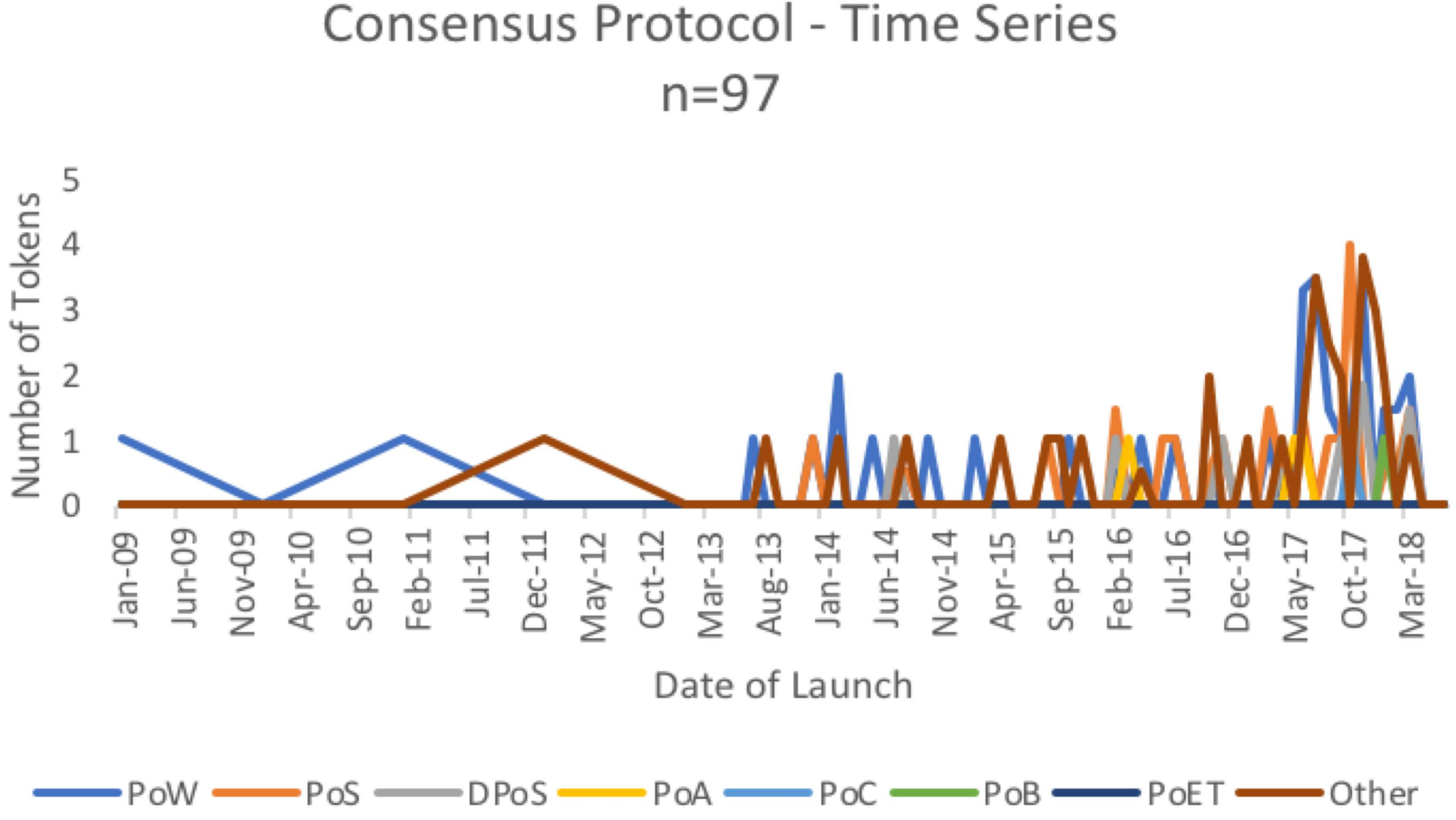

Users Experience
n=100
Number of Tokens
70
60
50
40
30
20
10
0
User Facing
Layered
Options


User Experience - Time Series
n=100
Number of tokens
0
1
2
3
4
5
6
Jan-09
Jun-09
Nov-09
Apr-10
Sep-10
Feb-11
Jul-11
Dec-11
May-12
Oct-12
Mar-13
Aug-13
Jan-14
Jun-14
Nov-14
Apr-15
Sep-15
Feb-16
Jul-16
Dec-16
May-17
Oct-17
Mar-18
Date of Launch
User Facing
Layered


Token Operation
n=100
Number of Tokens
80
70
60
50
40
30
20
10
0
App Specific
Interoperable
Operation Types


Token Operation - Time Series
n=100
Number of Tokens
0
1
2
3
4
5
6
7
Jan-09
May-09
Sep-09
Jan-10
May-10
Sep-10
Jan-11
May-11
Sep-11
Jan-12
May-12
Sep-12
Jan-13
May-13
Sep-13
Jan-14
May-14
Sep-14
Jan-15
May-15
Sep-15
Jan-16
May-16
Sep-16
Jan-17
May-17
Sep-17
Jan-18
May-18
Date of Launch
App specific
Interoperable


Consensus Protocol
n=97
Number of Tokens
35
30
25
20
15
10
5
0
PoW
PoS
DPoS
PoA
PoC
PoB
Other
Consensus Protocol


Consensus Protocol - Time Series
n=97
Number of Tokens
0
1
2
3
4
5
Jan-09
Jun-09
Nov-09
Apr-10
Sep-10
Feb-11
Jul-11
Dec-11
May-12
Oct-12
Mar-13
Aug-13
Jan-14
Jun-14
Nov-14
Apr-15
Sep-15
Feb-16
Jul-16
Dec-16
May-17
Oct-17
Mar-18
Date of Launch
PoW
PoS
DPoS
PoA
PoC
PoB
PoET
Other

DATA and TRENDS from the TOP 100

Outlier Consensus Protocols (34 total)

Market cap rank (frozen May 6)	Name
3	Ripple (XRP)
5	EOS (EOS)
8	Stellar (XLM)
9	IOTA (IOTA)
11	NEO (NEO)
14	NEM (XEM)
15	VeChain (VEN)
20	ICON (ICX)
24	Bytecoin (BCN)
27	Zcash (ZEC)
28	Ontology (ONT)
33	Siacoin (SC)
35	0x (ZRX)
40	Waves (WAVES)
42	Maker (MKR)
49	Hshare (HSR)
51	Loopring (LRC)
52	Waltonchain (WTC)
54	Aion (AION)
56	Mixin (XIN)
58	aelf (ELF)
63	Nebulas (NAS)
69	Kyber Network (KNC)
71	ReddCoin (RDD)
77	QASH (QASH)
82	GXChain (GXS)
85	Ethos (ETHOS)
88	Veritaseum (VERI)
92	Zcoin (XZC)
93	All Sports (SOC)
94	CyberMiles (CMT)
96	BnkToTheFuture (BFT)
97	Polymath (POLY)
98	Gifto (GTO)

DATA and TRENDS from the TOP 100

Outlier Consensus Protocols (34 total)

Technical Core	
Blockchain native	17
ERC20	16
Other non-native	1
dApp	0

Token Model	
Currency	13
Work	7
Network	6
Network value	6
Other	4
Usage	3
Stablecoin	1
Utility	1
Hybrid	1
Investment	0
Asset-backed	0
Share-like	0

Underlying value	
Permission to use	22
Inherent	10
Permission to work	5
Asset	3
Share	2

DATA and TRENDS from the TOP 100

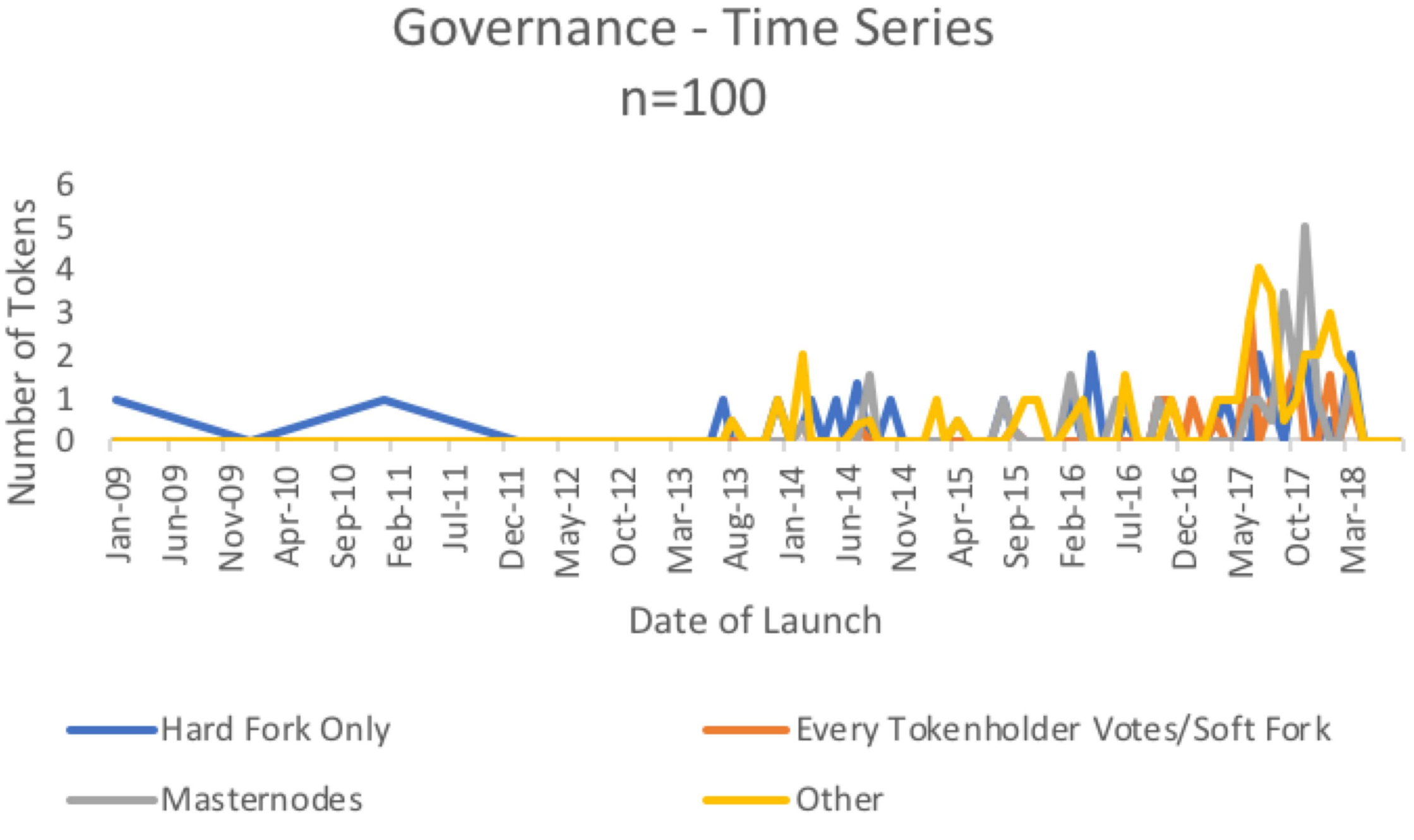
Outlier Consensus Protocols

	Top 10 Mkt Cap	Description
3	Ripple (XRP)	**The "Ripple Protocol Consensus Algorithm": subnetwork consensus** is achieved via Unique Node Lists, then aggregated. Nodes only verify their subsection of the network and their trust of other nodes.
5	EOS (EOS)	**The DPoS board of 21** can make "irreversible blocks" and other governance decisions by 2/3 majority vote (15).
8	Stellar (XLM)	**A Federated Byzantine Agreement ("FBA")** delays transaction approval until a critical mass of nodes approve (as determined by the individual authority preferences of each node in aggregate). Then, **the Stellar Consensus Protocol ("SCP") completes a nomination and ballot procedure.**
9	IOTA (IOTA)	**A "pay it forward" protocol**: validators verify blocks by PoW but their reward is getting a transaction processed by subsequent validators.

DATA and TRENDS from the TOP 100

Outlier Consensus Protocols

	Top 25 Mkt Cap	Description
11	NEO (NEO)	**Delegated Byzantine Fault Tolerance ("dBFT"):** non-validating NEO holders elect Consensus Nodes. One Consensus Node is randomly chosen as Speaker, proposing a transaction/change. Consensus Nodes validate the proposal against their constituents.
14	NEM (XEM)	**Proof of Importance**: PoS validation except that a validator's track record enhances likelihood of selection for future blocks as opposed to only holdings increasing odds in pure PoS.
15	VeChain (VEN)	**Proof of Authority**: the right to validate is only granted after a rigorous KYC process with the VeChain Foundation.
20	ICON (ICX)	**Interchain Loop Fault Tolerance**: BFT simplified by spinning. Only two steps: 1) a limited number of block generators broadcast and 2) remaining nodes only vote. Client chains retain their own protocols.
24	Bytecoin (BCN)	**Egalitarian PoW**: attempts to close gap between CPU and GPU/FPGA/ASIC miners by time-binding operations with random access to slow memory.

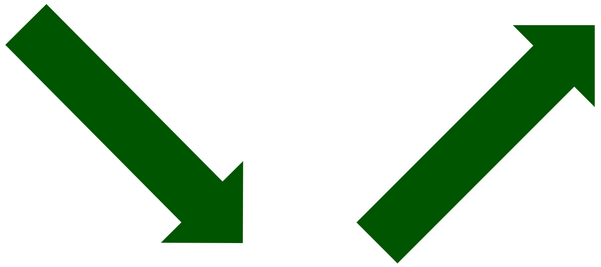

Governance - Time Series
n=100
Number of Tokens
0
1
2
3
4
5
6
Jan-09
Jun-09
Nov-09
Apr-10
Sep-10
Feb-11
Jul-11
Dec-11
May-12
Oct-12
Mar-13
Aug-13
Jan-14
Jun-14
Nov-14
Apr-15
Sep-15
Feb-16
Jul-16
Dec-16
May-17
Oct-17
Mar-18
Date of Launch
Hard Fork Only
Every Tokenholder Votes/Soft Fork
Masternodes
Other

Market Cap vs. NRV

Market Capitalization

Factors for Valuation

- Lack of expertise
- Lack of information
- Market inefficiency
- Fear
- Hype



Net Realizable Value (NRV)

- More accurate valuation
- More consistent across projects

Discounting Factors

- Development team and plan
- Technical build
- Economics
- Governance
- Availability of info

Market Cap vs. NRV

Adjustment Factors

- Development team and plan
- Technical build
- Economics
- Governance
- Availability of info

≈

Whitepapers

- Development team and plan
- Technical core
- Token model
- UX & interoperability
- Consensus protocol
- Governance
- Supply & valuation trajectory

Market Cap vs. NRV

Whitepapers

- Development team and plan
- Technical core
- Token model
- UX & interoperability
- Consensus protocol
- Governance
- Supply & valuation trajectory

- **Rank** elements by importance
- **Quantify** elements into numerical discount functions

Evaluate given whitepaper for:

- Missing elements
- Weak elements
- Strong elements

Apply discount functions

= Net Realizable Value (NRV)

Thank You

Join the Conversation!


wulf@semada.io


Wulf Kaal


Wulf Kaal


@wulfkaal


medium.com/@wulfkaal


Facebook.com/wulf.kaal


wulfkaal.com

wulfkaal