CRYPTOASSET MARKET COVERAGE INITIATION: TECHNICAL UNDERPINNINGS

Summary

The cryptoasset market has expanded from 14 coins with a combined market capitalization of $1.3B in 2013, to over 1,500 coins with a combined value of over $240B today. Beginning with Bitcoin and its initially proposed use case of value transmission and remittance, alternative networks have emerged with novel applications.

We believe that growth of this market is only set to accelerate as applications of the networks develop and materialize, although meaningful size and liquidity currently remains concentrated within a few specific coins.

We are initiating research coverage on the cryptoasset market space, and through a series of upcoming notes we will deliver a comprehensive understanding of the space.

This initial report will focus on Technical Underpinnings of cryptoasset networks and associated distributed ledger technologies:

- Distributed Ledger Network Architectures, both Public and Private
- Consensus Algorithms
- Hashing Algorithms
- Mining, Hardware, and Attack Vectors

Future reports will be released in sequence, covering the following topics:

- Network Creation – Smart contracts, network beginnings and structures, and ICO market landscape and quality.
- Market Composition – Network statistics, applications and performance by sector.
- Valuation – Fundamental and technical/trend-based.
- Custody & Trading – Custodial offerings and trading venues.

Satis Group Crypto Research will eventually move to a password protected subscription model. To be sure you can continue to access our research and inquire about pricing please contact: sales@analysthub.com.

This report was prepared by the Satis Group research team led by Sherwin Dowlat with assistance from Michael Hodapp.

Please note, Satis Group Crypto Research is powered by Analyst Hub and their robust institutional compliance program. Please contact them for more details.

Market Update

Name	Market Cap ($MM)		Launch Year	Price	ATH	Days Since ATH	% from ATH
	Current	2050 Implied*					
BTC	$104,883	$128,561	2009	$6,127	$20,089	192	(69.5%)
ETH	$43,709	$64,022	2015	$436	$1,432	165	(69.6%)
XRP	$18,444	$46,978	2013	$0.47	$3.84	174	(87.8%)
BCH	$12,229	$14,913	2017	$711	$4,330	189	(83.6%)
EOS	$7,115	$11,593	2018	$7.94	$22.89	59	(65.3%)
LTC	$4,588	$6,732	2011	$80	$375	190	(78.7%)

** Refers to Market Capitalization estimate, calculated using 2050 estimated supply using respective network inflation schedules.*

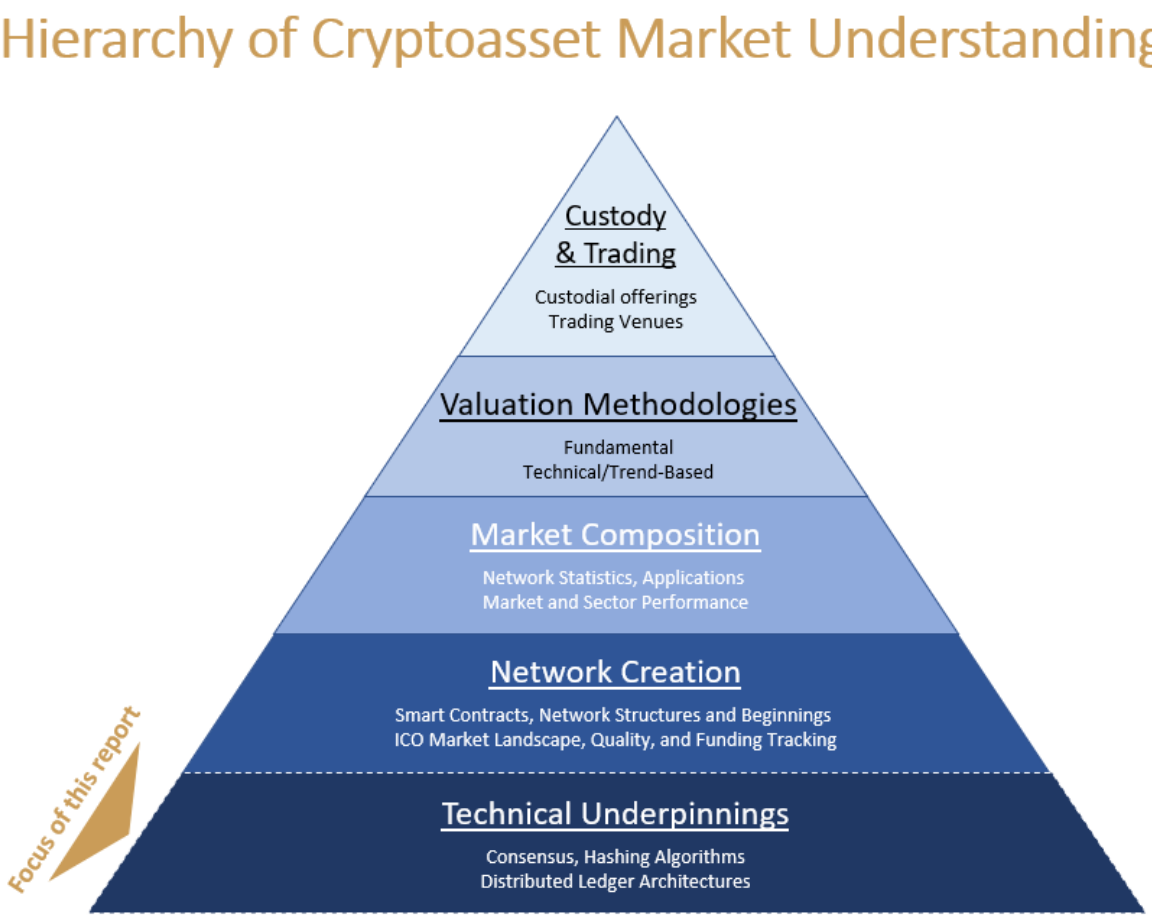
Intro

For decades, detractors of the modern financial system had far more complaints than answers. The nature of these complaints varied, but typically focused on gripes with the centralized bodies that control monetary policy, lack of transparency, debt that dilutes value, and the risks posed by a system that relies entirely on blind faith. Investors that wished to hedge traditionally would look towards gold and other non-cash assets as an alternative because of three key traits: usefulness, scarcity, and ability to hold value over time.

In 2009, a transparent and auditable peer-to-peer digital payment network called Bitcoin was released to the public. Created by a person (or group of persons) writing under the pseudonym Satoshi Nakamoto, Bitcoin delivered on the need for a secure way to transfer value without interfacing with the legacy finance world and the inefficiencies ingrained in it. While many in the beginning expected Bitcoin to remain a novelty, situations where its underpinning technology could be utilized were soon recognized. One of those scenarios materialized as citizens in the Republic of Cyprus faced uncertainty over taxes and the stability of their financial system amid a financial crisis. In their attempts to secure a bailout, the government initially proposed a one-time capital levy (haircut) on all money held in banks. The appeal of an alternative technological currency like Bitcoin, safe from retroactive government taxes, quickly became apparent, and was referred to by some as a safe haven store of assets. Others catalysts for adoption include millennials looking for an easy way to store their savings digitally (accessible at any time and only by them), rather than holding physical gold. Some seeking privacy in the wake of large scale global spying disclosures likely prefer to hold Bitcoin (or other specialized privacy-centric coins) rather than storing assets in a traditional financial institution subject to the reach of governments, which can arbitrarily restrict the movement of assets.

Because of its coincidental price increase during times of global macro-economic uncertainty and turmoil, Bitcoin has been perceived to be a hedge against quantitative easing. As central banks around the world have enacted policies that serve to increase the total supply of money as well as inflation after economic contraction through 2007, investors have yearned for an asset class with a provably finite supply - for Bitcoin, that is 21,000,000 coins minted - and is enforced by a transparent set of rules. Additionally, in a global low-yield environment, this nascent risk-bearing asset class with low correlation to others has driven further investment speculation.

In the cryptoasset space, Bitcoin has solidified its standing as the dominant store of value, as others have worked to create coins that focus on privacy, ease and speed of exchange, ownership of physical assets, and other novel use-cases. While Bitcoin was the first to bring digital currencies to a mainstream audience, the low cost of creating alternatives (forking - copying and branching off of previous code or writing entirely new code) has spawned many others. Early use cases and perceptions around the technology underpinning Bitcoin assumed the main application would be as a currency, but many more token-operated networks have been created and are beginning to demonstrate alternative applications (with their native cryptoassets acting as operational units within the network itself). Whether or not the proposed applications of the newer networks are utilized immediately or ever, fundamental understanding of the entire asset class is needed since the underpinnings may appear to be similar but have the slightest technological differences that impact their network effects and ability to become adopted and ultimately valuable. Additionally, we believe a strong catalyst for adoption could be the tokenization of real assets (where the token is backed by a real asset and/or a stream of cash flows), which will be built primarily on public token-operated networks for security and integrity. The industry is not a winner takes all space; there is room for a handful of winners, each with advantageous features depending on the networks goals and technical differences.



Source: Satis Research

We believe that as this fundamental shift in technological and economic innovation continues to expand and mature, significant economic value will be created within multiple distinct application sectors. Through this series of notes, we hope to deliver a comprehensive understanding of the pillars that comprise the cryptoasset universe.

Distributed Ledger Architectures

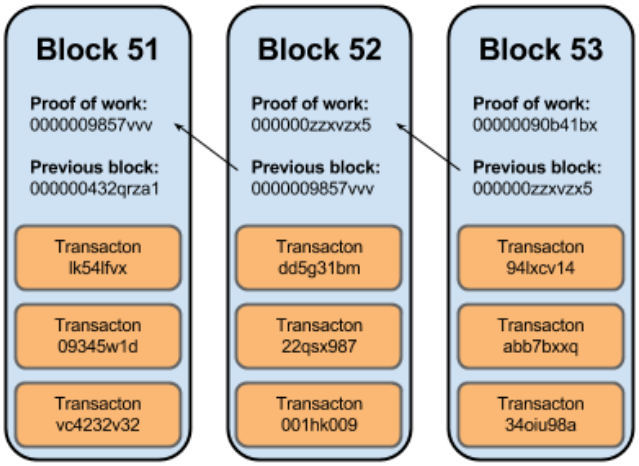
Unlike incumbent databases, which store data in a centralized area with central points of access and storage, decentralized networks aim to replicate data across members of the network to mitigate the risks associated with centralized attack vectors. Inherent in the ability to have members of the network reach consensus on common truths, each member carries a record of the historic truth by distribution of the ledger; a distributed ledger architecture. While networks that use distributed ledger technology (DLT) share a common goal, to allow decentralized communities to come to agreement on an accurate ledger, there are multiple distinct architectures that exist.

Although the Blockchain is the most commonly known data structure in the cryptoasset space, Directed Acyclic Graphs (DAG's) have recently emerged followed by fewer instances of the use of Hashtree structures. Additionally, Private Blockchain structures used in commercial settings have been in the process of testing for years.

Public Ledgers

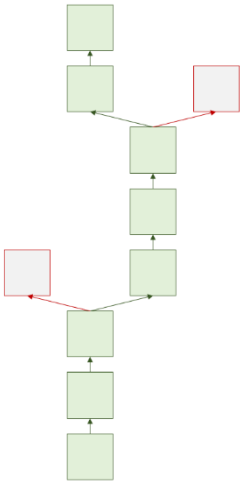
A **Blockchain** is the most well-known distributed ledger architecture, known for its use in the Bitcoin network. A Blockchain stores transaction data in batches - which are called blocks. Within each individual block, transaction data is stored, along with the hash of the block (a unique fingerprint), as well as the hash of the previous block. Since every block on the network is linked by the hash (as illustrated below), modifying the transaction data in any block would require every future block to be modified also. Due to the large amount of computing power active on the Bitcoin network, as well as the difficulty of producing (or mining) each block (which means a block takes 10 minutes to produce), attacks are enormously expensive, time consuming, and easily detectable.

Figure 1: Individual Block Data



Source: Yevgeniy Brikman

Figure 2: Blockchain

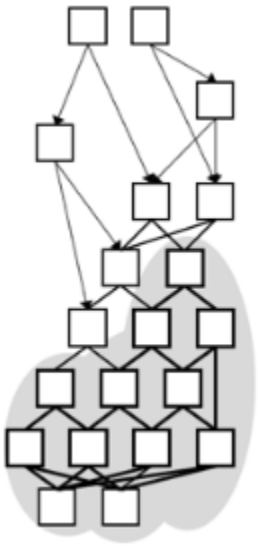


Source: Patrick Schueffel

Advantages	Disadvantages	Networks
✓ High security ✓ High energy use (depending on consensus mechanism)	× High energy use (depending on consensus mechanism) × Low transaction throughput (requiring novel solutions to improve scale)	Bitcoin (BTC) Ethereum (ETH) Bitcoin Cash (BCH) Eos (EOS) Litecoin (LTC) Stellar (XLM)

A Directed Acyclic Graph (DAG) is an alternative to the traditional crypto record keeping system, the blockchain. In a DAG system, there are no blocks and no constraints on the number of transactions. The concept of a DAG has a long history in mathematics. The first publicly reported effort to describe and implement DAG as a consensus model in a cryptocurrency was by Sergio Demian Lerner, who described *DagCoin* in a September 2015 blog post. Subsequently, Byteball and IOTA, the most well-known adoption of DAG technology, were announced. In a DAG model, every new transaction confirms at least one prior transaction, allowing the network to function quickly and efficiently. In a normal blockchain, the "chain" is modified on a block by block basis (creating a bottleneck) – whereas with a DAG, modifications occur on a transaction by transaction basis. Some DAG implementations (such as IOTA) use partial Proof of Work for spam prevention purposes, though this is not necessary.

Figure 3: DAG

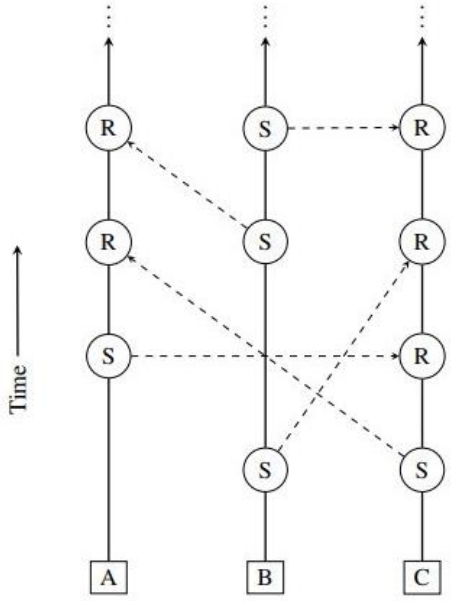


Source: Patrick Schueffel

Advantages	Disadvantages	Networks
✓ Rapid transaction confirmations ✓ Improved scalability and latency – more transactions translate to faster speeds ✓ No reliance on miners ✓ Transaction fees small or nonexistent ✓ Transaction finality possible in some implementations (Byteball)	× Initially requires some element of centralized-risk – a witness, or a coordinator	IOTA (MIOTA) Byteball (GBYTE) Dagger (XDAG) Hashgraph (N/A)

A **Block Lattice** is an architecture where each individual user has an individual blockchain, with balances transferred between accounts using send and receive blocks. Block lattice architectures use non-shared asynchrony, which means that there is no globally shared state of the blockchain like most networks, resulting in higher efficiency and transaction throughput.

Figure 4: Block Lattice

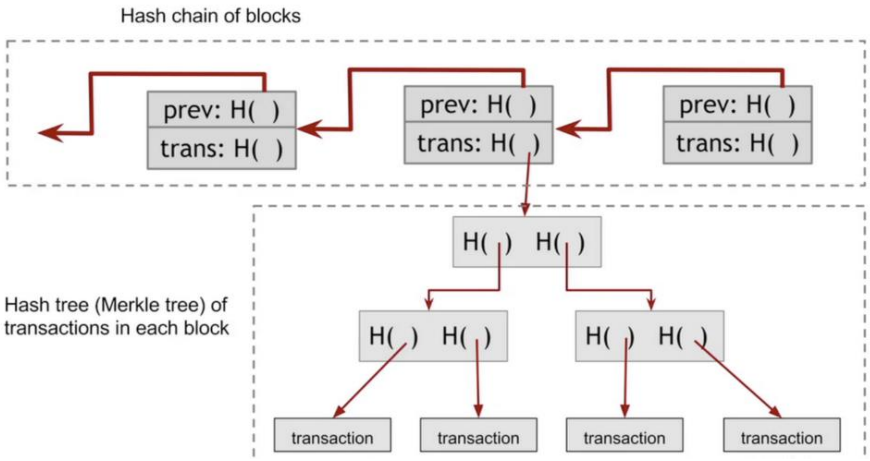


Source: Nano Whitepaper

Advantages	Disadvantages	Networks
✓ High transaction throughput ✓ High efficiency, low fees	× Unproven technology	Nano (XRB)

Hashtree is a less commonly used architecture primarily utilized by Ripple Labs' XRP. The hash tree uses a group of trusted, known validators to participate in consensus - similar to asking people in a room whether they agree on a stated opinion to determine if it is fact. Validators follow deterministic rules, while proposing and using an "avalanche" model to reach consensus. Though XRP uses a consensus mechanism it is not a standard blockchain and does not contain blocks.

Figure 5: Hashtree



Source: Ahmed Rashwan

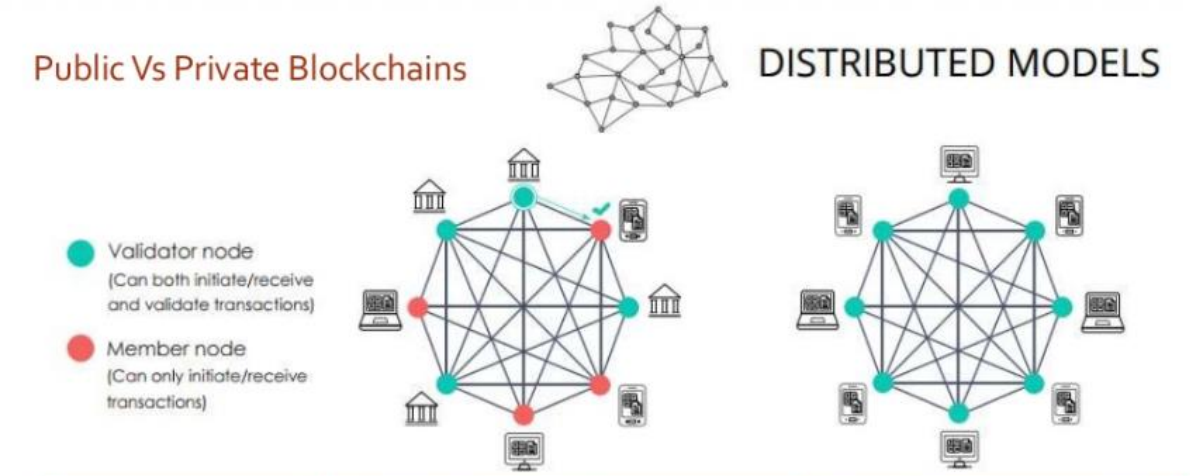
Advantages	Disadvantages	Networks
✓ Fast confirmations ✓ High throughput	× Centralized validators	Ripple (XRP)

Private Ledgers

Permissioned ledgers, also called **Private Blockchains**, attempt to transfer the value of traditional public blockchains to an internal, distributed system - a ledger that requires permission from a centralized authority(s) to access and/or modify. These systems can appeal to governments, financial institutions, and large corporations. Rather than value being created by the economic activity generated (and paid out in the native token/coin of the network) between users of a network and validators, in a permissioned network value is achieved through cost savings of data validation (since a token/coin doesn't exist on it) by members on the network hoping to achieve the same security of a public chain without paying for it.

In comparison to public architectures like public Blockchains, DAG's, and Hashtree's, Private Blockchains suffer their own set of trade-offs. Governance is centralized, and censorship concerns can exist due to a lack of transparency. Additionally, in a private ledger that lacks a native token—a free-floating, market-pricing based reward for participation and enforcement of the network—there exists - less economic incentive exists to maintain the integrity of the network. Thus, permissioned systems may be inherently less secure than a traditional, permissionless blockchain.

Figure 6: Public vs Private Blockchains



	Permissioned Blockchain (Private)	Permissionless Blockchain (public)
How do you get access to the network?	Authorized access	Open access
How are their approach to laws and regulations?	Aims to follow financial regulations such as AML/ KYC	Aims to create censorship resistant, anonymous transactions, outside current legal framework
Who are the validators?	Pre-selected, trusted validators	Anonymous, fully decentralized validators
What can it be used for?	Enterprise-level systems	Permissionless innovation, open-access applications

Source: M.Tech (IS)

Permissioned chains are appealing to:

- Government Institutions: who may want to restrict access to and audit certain parties.
- Financial Institutions: who may not want to give away control of internal governance and oversight.
- Large Corporations: who may not want to stockpile blockchain-native assets and deal with price fluctuation/market risk, in order to pay fees for using various blockchain platforms.

Tradeoffs and benefits:

× Centralized Governance: governance is confined to a small group of trusted validators, with restricted admission and access to the vulnerability of censorship. Much of the reason public blockchains have succeeded in usage is their transparency and availability for participation from the public, which is hindered in a permissioned system.

× Less Security: validators have little incentive to properly run and ensure integrity of the network, since there is often no free-floating, market-based price for a unit of operation/coin to participate in the network or any sort of mining/staking to benefit from transaction activity. The less aligned incentives are for validators, the more vulnerable the network will be.

✓ Clear Governance Structure: governance and code forks can be planned and implanted according to defined rules, without requiring agreement of majority of operators.

✓ Speed: as a result of abbreviated and centralized consensus, transactions are quicker.

Hyperledger Fabric is a platform maintained by The Linux Foundation, that takes a modular approach allowing different consensus and smart contract (automatically executing computer protocol) implementations. At the core, there are different node types responsible for creating transactions, updating the ledger, and verifying transactions, in contrast to something like Ethereum, where all nodes are identical in function. In order to deal with disagreements between nodes, a consensus algorithm is implemented. The consensus algorithm used will depend on the goals of the operator. Smart contracts and tokens can also be implemented.

R3CEV is a consortium of more than 200 firms seeking to create distributed ledger technologies for the financial world. Their flagship product, Corda, is designed to facilitate complex financial transactions while restricting access to some confidential or proprietary data. Consensus in Corda is achieved using *Notary Nodes* – nodes, or groups of nodes, that work by verifying that any input requested by a transaction has not already been spent, signing legitimate transactions and rejecting any transactions that attempt to double spend an input. In addition, validity is also ensured by checking to determine whether each party has signed the transaction. Smart contracts are supported, but without a currency or token. R3 and their Corda platform has been largely criticized by much of the crypto community, in part due to its lack of blockchain technology - including the lack of a token. A number of power players initially involved have left the consortium in order to pursue their own blockchain ambitions, including JPMorgan Chase, Goldman Sachs, Morgan Stanley, and Santander. Recent reports indicated the company may be struggling financially[1].

Quorum is a private blockchain built by J.P. Morgan that was forked from Ethereum and designed to address the specific needs of the financial sector. Unlike Ethereum (a public blockchain), Quorum is permissioned, requiring a third party's approval to participate. Transactions and smart contracts, which can each contain confidential and proprietary data and information, can be kept confidential. Consensus is achieved through a voting mechanism called QuorumChain, which allows for a far higher transaction throughput than Proof of Work (PoW), blockchains.

Common pushback from major users/providers of private, permissioned chains stems from issues of privacy. They argue that regulated access may be warranted around the sensitive data that the networks will be used to transact with. Major privacy innovations within the public blockchain space are underway and being improved upon, with technology such as:

- **Zero-Knowledge Proofs**: Notably implemented first in Zcash (ZEC), ZK-Proofs allow users within consensus-enforced networks to prove that some element of data is true without actually knowing what the underlying data contains.
    - **ZK-SNARKS** (Zero-Knowledge Succinct Non-Interactive Argument): The first iteration of zero-knowledge cryptography within the ZEC protocol, allowing users to verify information without knowing the details of the information and without interacting with the information counterparty.
        - Deployment: ZEC (current), ETH (current)
    - **ZK-Starks** (Zero-Knowledge Scalable Transparent ARgument of Knowledge): A ZK-proof that relies on fewer assumptions around public key cryptography than ZK-SNARKS. Computation can take as little as seconds to calculate (compared to nearly 30 min for ZK-SNARKS) and just over 1MB (compared to ~20GB for ZK-SNARKS).
        - Deployment: ZEC (EOY 2018, est), XMR (n/a)
- **Mimblewimble:** Mimblewimble aims to achieve a similar goal as ZK-SNARKS but for Bitcoin: anonymous transactions where details are unknown to all. When compared to ZK-SNARKS, Mimblewimble is quicker and computationally efficient. Though its original goal was to be a sidechain of Bitcoin, it is now rumored to be introducing its own coin and chain.
        - Deployment: GRIN (n/a), BTC (n/a)

[1] http://fortune.com/2018/06/07/blockchain-firm-r3-is-running-out-of-money-sources-say/

- **Ring CT** (Ring Confidential Transactions): Known for its use in Monero (XMR) but under development in other projects, Ring CT allows for hidden transaction amounts and transactors (from/to) more efficiently than its prior version called ring signatures. Ring signatures essentially create a group of signatures in a transaction by using the sender's keys as well as others from the blockchain, making it incredibly difficult to trace transaction information.
    - XMR (current)
- **Bulletproofs:** Also known for use in Monero, bulletproofs replace a prior mathematical method used to hide transaction details (called range proofs), allowing transactions sizes to decrease ~80% (since it can scale logarithmically with parameters in the transactions, including number of outputs, rather than linearly like the current range proofs).
    - XMR (3Q18, est)

Consensus Algorithms

In a traditional, centralized database, administrators are entrusted with the responsibility of maintaining the integrity of the data and ensuring that the information contained therein is accurate and up to date. In a decentralized database such as Bitcoin - which revolves around a network that holds distributed ledgers of historic and proposed future truth - the integrity of the database is maintained by network participants (which can be outside validators and/or users, depending on the network structure). These networks rely on Public Key Cryptography, which allows users to prove ownership/authorship of publicly visible code through the use of a private key that they alone control. There are a number of different approaches to maintaining *Consensus*, where all nodes agree upon the accuracy of past and future transactions, of the ledger.

Figure 7: Market Share and Value of Networks, by Consensus Algorithm

Consensus Algorithm	**Network Share***	**Value of Networks ($MM)**
Proof of Work**	61.3%	$164,856
Hybrid PoW/PoS	9.4%	$1,714
Proof of Stake	6.6%	$7,984
Delegated Proof of Stake	6.6%	$16,741
Custom (DAG)	1.9%	$4,201
Del Byz Fault Tolerance	1.9%	$2,745
Fed Byzantine Agreement	2.8%	$59,455
Proof of Importance	0.9%	$1,895
Proof of Burn	0.9%	$29
Proof of Reserves	0.9%	$35
Other	6.6%	$5,787
Total	**100.0%**	**$265,442**

** Network Share is the share of total number of networks that use it.*
*** Includes coins built on top of other networks, such as Ethereum (using the ERC-20 standard).*
Source: Satis Research

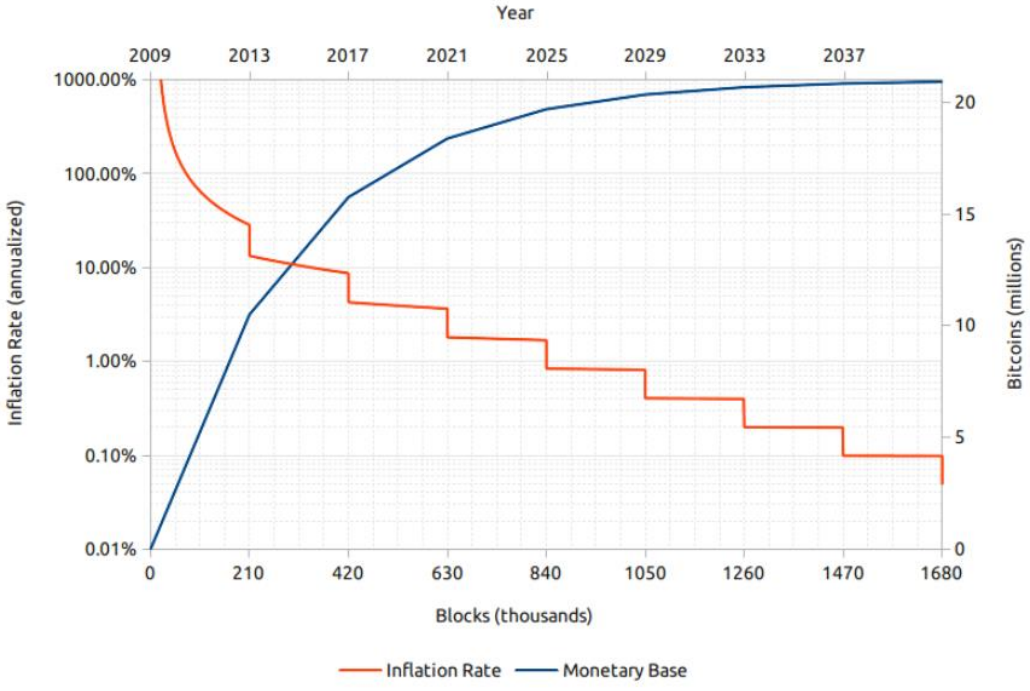
Although Proof-of-Work is the most commonly used, more mechanisms have arisen from the need for energy-efficient alternatives.

The **Proof-of-Work (PoW)** consensus mechanism underpins many distributed ledger architectures. Originally proposed as a solution to curb oversized resource requests (notably DDoS attacks and email spam) in 1992, Adam Back's HashCash in 1997, and most notably its implementation in the Bitcoin protocol in 2009.

Miners engage in hashing, or the transformation of a large string of characters into shorter amounts that can be traced back to the original, to make sure that the original data and the data used to generate the hash are the same. The network proposes a difficulty level to emulate the handicap of "work", hence the name Proof-of-Work. The difficulty sets a target hash that must be equal to or lower than the current target in order for the network to accept the new block; the lower the hash target, the greater the difficulty. The network aims to add one block every 10 minutes, so once every 2016 blocks (or roughly two weeks at the current rate), the difficulty is either increased (if the blocks took under two weeks to find) or decreased (if the blocks took over two weeks to find).

Miners are essentially solving a puzzle with a dynamic handicap, based on competing network power, with the ultimate goal of forming blocks, confirming transactions and being rewarded for their work by receiving a "block reward" (an amount of coins the network releases to the winning miner) and a slice of transaction fees (which are small; on the BTC network the fees account for ~2% of total rewards). Depending on the codebase, block rewards (aka miner incentives to secure the network and continue to create and place blocks) are adjusted over time through a controlled supply algorithm. For example, on the Bitcoin network, the amount of BTC given as a reward per block halves every 210,000 blocks (or ~four years) until eventually the network will be entirely reliant upon transaction fees to incentivize miners (est. ~2140), as can be seen in Figure 8 below. Different networks will deploy various versions of this controlled supply schedule, with some having perpetual inflation and keeping the block reward while others mimic Bitcoin's reward inflation cap.

Figure 8: Bitcoin Inflation vs. Time



Source: Matt Whitlock

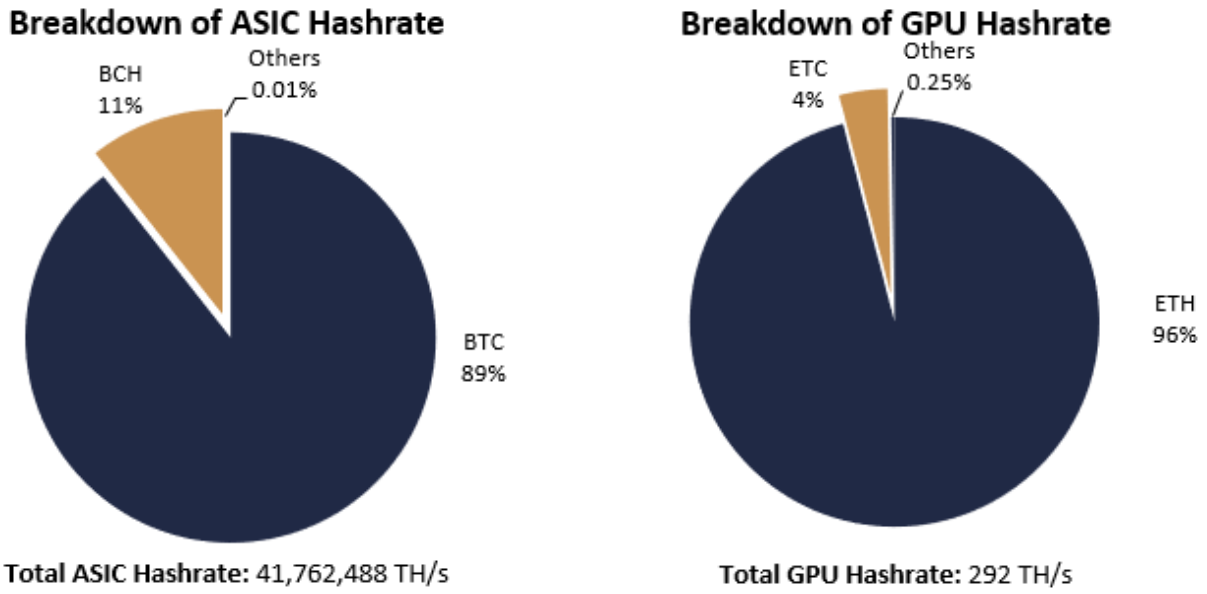
Mining

In cryptocurrency networks with PoW consensus protocols, hardware miners use certain chips to work through the necessary computations permitted within the network to solve complex algorithms for their reward and the ability to add transactions within the blocks to the ledger. Although in early days of Bitcoin mining CPU's (Central Processing Units) were sufficient and profitable for mining, GPU's (Graphics Processing Units) and ASICs (Application-Specific Integrated Circuits) have taken over as the picks and shovels of the cryptocurrency mining revolution. Integrated circuits perform tasks on a scale that varies by scope and performance; the more specified the initial instruction set and rigid the chips' ability, the higher the performance. Where a CPU may be the critically-thinking project-manager, the GPU is the workhorse that's prepared to repetitively perform a certain (but programmatically alterable) type of task, and the ASIC is a workhorse that has been manufactured specifically to do one repetitive task. Naturally in cryptocurrency mining, where scope is narrowed around a specified hashing algorithm and little need for flexibility beyond it, general-purpose hardware (like CPU's and even GPU's) has fallen behind and the ASIC has dominated.

While networks like BTC have been open to ASIC mining for quite some time, other networks (often with substantial hashrate, like ETH) have tried to maintain ASIC-resistance (through means of alternative hashing and consensus algorithms) but recently ASIC manufacturers like Bitmain have discovered ways to design around their memory-hard algorithms and are shipping their first ASIC's in the coming months.

Although BTC holds ~89% total cryptoasset market network hash rate, ETH's rise to popularity among miners in the past few years drove incremental gains for GPU designers like AMD and NVDA, with ETH holding ~96% of all GPU-powered network hash rate. Now, with the emergence of ASICs designed for previously assumed-to-be ASIC-resistant networks like ETH, impact to AMD and NVDA will gradually be realized since their crypto-targeted market of much smaller networks will shrink as large GPU-powered networks (like ETH) will transition to a different chip architecture. Additionally, ETH's impending switch to PoS (which will supposedly move entirely off of hardware mining, to the less-computationally intensive Proof-of-Stake consensus algorithm – explained further below) will impact mining and chip revenue which we will walk through in our next report on ETH and scaling.

Figure 9: Hashrate Composition



Source: Satis Research

Figure 10: Hardware Trade-Off Comparison

	Microprocessor	FPGA	ASIC	GPU
Example	ARM Cortex-A9	Virtex Ultrascale 440	Bitfury 16nm	Nvidia Titan X
Flexibility during development	Medium	High	Very high	Low
Flexibility after development[1]	High	High	Low	High
Parallelism	Low	High	High	Medium
Performance[2]	Low	Medium	High	Medium
Power consumption	High	Medium	Low	High
Development cost	Low	Medium	High	Low
Production setup cost[3]	None	None	High	None
Unit cost[4]	Medium	High	Low	High
Time-to-market	Low	Medium	High	Medium

[1]E.g. to fix bugs, add new functionality when already in production
[2]For a sufficiently parallel application
[3]Cost of producing the first chip

Source: ResearchGate

While hardware innovations can significantly increase efficiency, they can create difficult circumstances for the health of the network. In addition to advancements in chip architecture, design efficiencies within ASICs have also been utilized and caused contention within the networks. In the past, large manufacturers have developed technologies that allow for steps in the process of mining to be done more efficiently. Since many PoW networks are separated by validators and processors of transactions (the miners, who use the equipment) and submitters (the users transacting, who use the coin), changes to the network can come with disagreement since validators hold voting power while users don't directly. Miners, which hold voting power and are economically incentivized by mining rewards and transaction fees, may be less inclined to allow network upgrades that benefit users and could negate their innovative mining advantages.

Pushback on critical changes, from advantageous players with large mining and possibly chip production share, can be detrimental and hostile to the advancement of the network. Additionally, certain networks like Monero (XMR) and Ethereum (ETH) have implemented ASIC-inefficient elements within their protocols, to deter concentration caused by miners who build more efficient and powerful ASICs to attempt to gain control of the network hash power (aka hash rate) through size and efficiencies. These networks have come under considerable pressure recently, with Monero attempting to hard-fork (which is a change in the code that implements non-backwards compatible features) to avert this. The vulnerability in this situation was clear, when the network forked and lost a significant amount of the network hash rate (~50% of the TTM power went offline), lowering the cost of an attack where over half of the hash rate is controlled by a malicious actor.

When attempting to project the future path of cryptocurrency-related mining and associated revenues (to chip designers and producers), it is important to understand the role that the native cryptoassets play in the incentive structure. Recall that miners are separate from users. Miners expend variable computational energy and sink capex into depreciable hardware, in order to prove digital work and be rewarded by shares of network fees and/or codebase-defined rewards (aka block rewards, which grant miners network native coins as a reward for working on the blocks). On the other side, users are incentivized to transact through networks that have substantial miner backing and security; it is presumed that the more hashrate or computational power there is behind a network, the more difficult it will be to outspend to overthrow and compromise transaction and coin integrity. Entrants without substantial competitive advantages in variable costs (electricity), computation efficiencies (like ASICBoost), and supply-chain efficiencies (i.e. like Bitmain, which can mine at-cost since they produce the equipment), are

hamstrung to the market price of the coin in relation to the difficulty to mine on the network. The less profitable it becomes to mine on the network, in relation to their respective breakeven cost, the more likely they will be to hop off and secure/mine another chain. Because multiple chains use the same hashing algorithms, switching costs for miners are extremely low. Since the risk of double-spending attacks and the integrity of the ledger are more likely compromised, users may be averse to holding value on that network.

In Figures 11 and 12 we show the estimated costs of taking over 50% computing power of the various networks in their current forms. In Figure 11, we assume the attacker is new and held no previous hashrate (and therefore must match the power of the network, to gain majority power). In Figure 12, we assume the attacker held ~25% hash rate power previously on the network.

Figure 11: Cost of Attack Relative to Market Value (New Miner)

Cost of a 51% Attack	BTC	ETH	BCH	LTC	DASH	ETC	ZEC	ETH	XMR	ETC	ZEC
Hardware Type	ASIC	ASIC	ASIC	ASIC	ASIC	ASIC	ASIC	GPU	GPU	GPU	GPU
# Units needed	2,692,516	1,488,421	320,170	609,006	115,972	59,058	58,075	8,837,500	5,807,500	350,659	967,917
Hardware Cost ($MM)	$2,019	$2,792	$240	$281	$36	$111	$49	$5,303	$2,323	$210	$726
Electricity Cost per Day ($MM)	$6.7	$2.3	$0.8	$0.5	$0.2	$0.1	$0.0	$2.5	$2.3	$0.1	$0.3
Total Cost per Day ($MM)	**$2,026**	**$2,795**	**$241**	**$282**	**$36**	**$111**	**$49**	**$5,305**	**$2,325**	**$210**	**$726**
Market Cap ($MM)	$104,883	$43,709	$12,229	$4,588	$2,112	$1,412	$818	$43,709	$2,113	$1,412	$819
Attack % of Market Cap	**2%**	**6%**	**2%**	**6%**	**2%**	**8%**	**6%**	**12%**	**110%**	**15%**	**89%**

Figure 12: Cost of Attack Relative to Market Value (Old Miner)

Cost of a 51% Attack	BTC	ETH	BCH	LTC	DASH	ETC	ZEC	ETH	XMR	ETC	ZEC
Hardware Type	ASIC	ASIC	ASIC	ASIC	ASIC	ASIC	ASIC	GPU	GPU	GPU	GPU
# Units needed	1,999,393	1,105,263	237,750	452,232	86,118	43,855	43,125	6,562,500	4,312,500	260,391	718,750
Hardware Cost ($MM)	$1,500	$2,073	$178	$209	$27	$82	$37	$3,938	$1,725	$156	$539
Electricity Cost per Day ($MM)	$5.0	$1.7	$0.6	$0.3	$0.1	$0.1	$0.0	$1.9	$1.7	$0.1	$0.2
Total Cost per Day ($MM)	**$1,505**	**$2,075**	**$179**	**$209**	**$27**	**$82**	**$37**	**$3,939**	**$1,727**	**$156**	**$539**
Market Cap ($MM)	$104,883	$43,709	$12,229	$4,588	$2,112	$1,412	$818	$43,709	$2,113	$1,412	$818
Attack % of Market Cap	**1%**	**5%**	**1%**	**5%**	**1%**	**6%**	**4%**	**9%**	**82%**	**11%**	**66%**

Although the relative cost of attacking an ASIC network is far lower than on a GPU network, the networks most prone to attack and manipulation are the networks with semi-permissioned validator networks and low transaction fees, as shown in by mining/voting and network holding balances in Figure 13.

Figure 13: Centralization of Networks Across both Holdings and Voting Power

Source: Satis Data

Network Centralization Considerations	BTC	ETH	BCH	DASH	XMR	XRP	LTC	XLM	NEO	ADA
Consensus Algorithm	PoW	PoW	PoW	PoW	PoW	HT	PoW	FBA	DBFT	PoS
Miners/voters Incentivized?	Y	Y	Y	Y	Y	**N**	Y	**N**	N	N
# of entities in control of >50% of voting/mining power	3	3	3	3	3	**1**	3	**1**	1	1
% of money supply held by top 100 accounts	**19%**	34%	25%	**15%**	N/A*	**81%**	44%	**95%**	70%	40%
# of client codebases that account for > 90% of nodes	1	2	2	1	1	1	3	1	2	1
# of public nodes	9,624	15,708	2,124	4,649	1,691	732	261	111	46	1

**Monero accounts are impossible to track due and it is therefore unknown what wallets hold what amounts.*

Hashing Algorithms

PoW networks use cryptographic hashing to create a monetary cost of "work" with rewards, digitally akin to the opportunity cost of labor required to mine precious metals. A hash refers to a unique "fingerprint" that can be generated by a running a string of text through specialized computer software. Imagine a full page of important financial data - when running this page through a *hashing algorithm,* a unique (short) string of characters (the data's fingerprint) is generated. If a malicious actor changes even 1 number at any point within the financial data, an entirely different hash is generated, making the malicious modification extremely easy to detect. Within Proof-of-Work networks, hashing is utilized to ensure the integrity of the ledger - in the event that one transaction was modified by a malicious actor, the hash of every future block will change and all network participants will know.

While SHA-256 is the most common hashing algorithm, it was not created uniquely for cryptoasset mining. Other novel algorithms (like ETHash and Equihash) were created specifically for their networks (created as an attempt to avert ASIC mining). Below are the most commonly utilized technical hashing parameters and functions by the largest PoW networks, along with less used alternatives:

SHA-256	Perhaps the most well-known hashing algorithm, SHA-256 creates a 256-bit signature from an input of any size. SHA-256 is commonly mined using custom-designed ASIC equipment or general-purpose GPUs. **Networks:** Bitcoin (BTC), Bitcoin Cash (BCH), Steem (STEEM), Namecoin (NMC)
ETHash (Keccak-256, previously SHA-3)	ETHash is a PoW algorithm used by Ethereum that utilizes the Keccak-256 hashing function. Though it had the original goal of being ASIC-resistant, ASIC manufacturers have recently learned to work around this and have ASICs being shipped in the next few months. **Networks:** Ethereum (ETH), Ethereum Classic (ETC)
Equihash	Equihash is another memory intensive algorithm, also intended to be ASIC resistant, though the first ASIC miner is scheduled to launch this month. **Networks:** Zcash (ZEC), Bitcoin Gold (BTG)
Blake	Variants of the Blake function are used on several popular networks, including Siacoin (Blake2b), DCR (Blake256), and XVG (Blake2s). **Networks:** Siacoin (SC), Decred (DCR), Verge (XVG)
Scrypt	Scrypt is an alternative to SHA-256 and is designed to utilize large amounts of memory, which theoretically reduces the risk of brute force attacks. **Networks:** LTC, DOGE, Blackcoin (BLK), Gridcoin (GRC)
CryptoNight	The CryptoNight hashing function, most well-known for its use in Monero alongside the CryptoNote PoW algorithm, is designed to be dependent on modern CPUs, and resistant to specialized hardware including ASIC miners. While ASIC miners have been developed, they have been successfully mitigated with forks to the code. **Networks:** Monero **(**XMR), Bytecoin (BCN), Electroneum (ETN)
X11	The X11 algorithm was introduced by the Dash developer Evan Duffield and combines 11 hashing algorithms. The goal was to prevent custom ASIC hardware from overpowering the Dash network in its inception. Because it combines 11 distinct algorithms, the network can remain secure even if a significant vulnerability is discovered in one or more of the included algorithms. **Networks:** Dash (DASH)
Curl	Only used in the IOTA protocol on a DAG architecture, the Curl algorithm is designed to be lightweight and require minimum computational power, allowing for its use in IoT connected devices, such as sensors. **Networks:** IOTA (MIOTA)

Proof-of-Stake (PoS) is the most well-known alternative to PoW. Whereas PoW requires a large sum of computing power and electricity to validate transactions and create blocks in the blockchain, PoS is a philosophy that depends on proving your wealth. The philosophy of Proof-of-Stake goes back to Wei Dai's B-Money, proposed in 1998. He suggested a group of selected users would maintain the ledger, after depositing their own holdings to a special account, which they would forfeit should they be dishonest. First proposed by BitcoinTalk.org user Quantum Mechanic in 2011, PoS has seen considerable adoption as the core technologies have developed over the following years. The first implementation of PoS, Peercoin, debuted in 2011.

In the PoS model, users "stake" or deposit their currency using a contract to post collateral on the integrity of future transactions they are validating. Generally, the more currency deposited, the higher the probability of creating a new block. In order to disincentivize malicious activity, some PoS protocols implement a penalty mechanism which will seize coins from attackers on the network. PoS means that anyone can become a validator – without having to make a significant investment in specialized computing hardware. The only requirement is to own a minimum threshold of coins.

Some PoS coins also use Masternodes, or Bonded Validator Systems, which make decisions for the network and may be able to vote on important network decisions, including development and use of funds. Masternodes are complex to operate and require a significant minimum stake. DASH, the first token to utilize Masternodes, requires 1,000 DASH (~$270,000 at current prices). This large stake incentivizes the operator to not act maliciously. While their functions vary from currency to currency, Masternodes often facilitate privacy, instant send, currency exchange, contracts, or other services.

Advantages
✓ Energy efficiency since, unlike PoW, PoS networks use validator ownership of network assets to validate transactions (and not costly mining hardware and electricity)
✓ Reduces centralization due to lack of economy of scales that benefit the wealthy disproportionately
✓ Could significantly increase the cost of 51% attacks if the network value has grown large enough, since attackers must own over 50% of the network assets to control it

× **Disadvantages**
× Since staking is a passive activity that requires no additional investment and action on the part of holders, unlike mining with PoW networks, the custody of the coins determines the ability of stakers to vote on various changes to the network. With an increasing amount of liquidity and custody through exchanges and funds, votership will eventually become concentrated in the hands of very few (similar to how active managers hold high voting power with equities). As a result, concentrated (and potentially thin) voting power could sway voting decisions.
× The cost to attack a network may be less than a PoW network (depending on the maturity and size), since an attacker would need 50+% of the system currency to hold control of the network in a PoS network while they would need 50%+ of computational power to control a PoW network.

Networks
NEO (NEO) Cardano (ADA) Factom (FCT)

Delegated Proof-of-Stake (DPoS) builds upon the PoS model by allowing token holders to cast their votes, weighted by their ownership of the token, for others to become the block producers (maintainers) of the network. This leads to a more democratized model, that allows the community to choose who they trust, even if that trusted party does not own a significant portion of outstanding tokens. Block producers are incentivized to act appropriately as any malicious action would lead to the community rescinding their position.

Advantages	Disadvantages	Networks
✓ High scalability ✓ High efficiency	× Voter apathy × 51% attack by scheming delegates × Concentration of validators	Ripple EOS **(**EOS) Nano (XRB) BitShares (BTS) Lisk (LSK)

In **Proof-of-Burn (PoB)** consensus, users demonstrate their commitment to the network by sending coins to an unrecoverable address - thus "burning" them and permanently removing the tokens from circulation. By burning valuable coins, users demonstrate their commitment to the long-term value and integrity of the network, expecting that rewards and confidence in the network will create higher value than the coins they discarded. PoB implementations vary, with some coins requiring users to burn Bitcoin, and others requiring burn of the coin itself.

Advantages	Disadvantages	Networks
✓ Long-term commitment to network value	× Favors the rich - rich get richer scenario	Counterparty **(**XCP) Slimcoin (SLM) Triggers (TRIG)

Proof-of-Capacity/Space (PoC) is based off hard-drive capacity, rather than raw computing power. In a PoC system, the "work" is done ahead of time, and a user's hard-drive is plotted with possible mining solutions - akin to a lottery. The larger a user's hard drive, the larger chance that they will create the next block.

Advantages	Disadvantages	Networks
✓ High efficiency ✓ Highly decentralized	× Malware potential	Burstcoin (BURST) Chia Network *(Launch ETA: EOY 2018)*

In **Proof-of-Elapsed-Time (PoET)**, every implementation uses an Intel hardware-based, lottery method in which the users of a computer, using a secure portion of their CPU, select a random waiting time. The user who randomly selects the lowest wait time wins.

Advantages	Disadvantages	Networks
✓ More efficient than PoW ✓ Cheaper than PoW	× Reliant on specialized hardware from one vendor (INTC)	Hyperledger Sawtooth

Proof-of-Activity (PoA) is a hybrid approach, combining PoW and PoS. PoW is used to mine new blocks, while PoS is used to sign and validate the block. Miners and validators then split any transaction fee earned.

Advantages	Disadvantages	Networks
✓ High resistance to 51% attack	× High power consumption × Double spending vulnerability	Decred (DCR) Espers (ESP)

Proof-of-Importance (PoI) was introduced by XEM and is designed as a variant to the classic PoS model. While PoS relies on the number of coins staked, PoI considers the number of coins in addition to other variables - namely the number of transactions by an address as well as the amount of currency transferred. This system is designed to give additional weight not just to those who are able to stake a large number of coins, but those who actively utilize the network.

Advantages	Disadvantages	Networks
✓ Incentivizes network participation ✓ Energy efficiency	× Potential to concentrate wealth	NEM (XEM)

Conclusion

In the expanding cryptoasset universe, core technology components among the distributed networks vary. We have described some key elements behind the architectures, methods of consensus, and hashing algorithms that are used within a variety of distributed systems.

In the next note, we will build off this knowledge and expand on the Creation of cryptoassets; how certain networks can be utilized to build others, how networks are made from scratch, network structures, and a detailed overview of the composition and growth of the Initial Coin Offering (ICO) market.

DISCLOSURES AND DISCLAIMERS

Analyst Certification
The analyst, Sherwin Dowlat, primarily responsible for the preparation of this research report attests to the following: (1) that the views and opinions rendered in this research report reflect his personal views about the subject companies or issuers; and (2) that no part of the research analyst's compensation was, is, or will be directly related to the specific recommendations or views in this research report.

Analyst Certifications and Independence of Research.
Each of the Satis Group analysts whose names appear on the front page of this report hereby certify that all the views expressed in this Report accurately reflect our personal views about any and all of the subject securities or issuers and that no part of our compensation was, is, or will be, directly or indirectly, related to the specific recommendations or views of in this Report.

Satis Group (the "Company") is an independent equity research provider. The Company is not a member of the FINRA or the SIPC and is not a registered broker dealer or investment adviser. [Firm name] has no other regulated or unregulated business activities which conflict with its provision of independent research.

Limitations of Research and Information.
This Report has been prepared for distribution to only qualified institutional or professional clients of Satis Group. The contents of this Report represent the views, opinions, and analyses of its authors. The information contained herein does not constitute financial, legal, tax or any other advice. All third-party data presented herein were obtained from publicly available sources which are believed to be reliable; however, the Company makes no warranty, express or implied, concerning the accuracy or completeness of such information. In no event shall the Company be responsible or liable for the correctness of, or update to, any such material or for any damage or lost opportunities resulting from use of this data.

Nothing contained in this Report or any distribution by the Company should be construed as any offer to sell, or any solicitation of an offer to buy, any security or investment. Any research or other material received should not be construed as individualized investment advice. Investment decisions should be made as part of an overall portfolio strategy and you should consult with a professional financial advisor, legal and tax advisor prior to making any investment decision. Satis Group shall not be liable for any direct or indirect, incidental or consequential loss or damage (including loss of profits, revenue or goodwill) arising from any investment decisions based on information or research obtained from Satis Group.

Reproduction and Distribution Strictly Prohibited.
No user of this Report may reproduce, modify, copy, distribute, sell, resell, transmit, transfer, license, assign or publish the Report itself or any information contained therein. Notwithstanding the foregoing, clients with access to working models are permitted to alter or modify the information contained therein, provided that it is solely for such client's own use. This Report is not intended to be available or distributed for any purpose that would be deemed unlawful or otherwise prohibited by any local, state, national or international laws or regulations or would otherwise subject the Company to registration or regulation of any kind within such jurisdiction.

Copyrights, Trademarks, Intellectual Property.
Satis Group, and any logos or marks included in this Report are proprietary materials. The use of such terms and logos and marks without the express written consent of Satis Group is strictly prohibited. The copyright in the pages or in the screens of the Report, and in the information and material therein, is proprietary material owned by Satis Group unless otherwise indicated. The unauthorized use of any material on this Report may violate numerous statutes, regulations and laws, including, but not limited to, copyright, trademark, trade secret or patent laws.