Digital Asset Reference Pack

www.gsr.io

Brian Rudick, Senior Strategist
Matt Kunke, Research Analyst

With the cryptosphere heating up, we provide a reference pack with brief, fundamental overviews of various digital assets topics and subsectors.

With notable developments like the recent approval of US spot Bitcoin ETFs, Solana's rise from the depths, experiments around new blockchain architectures, and newfound innovation on Bitcoin, the cryptosphere is heating up. As such, we provide an overview of various digital asset topics and subsectors as a reference for the experienced and an introduction for the newly initiated. For those preferring shorter-form overviews with more exhibits, please see our GSR Crypto Holiday Series Twitter thread of threads, which covers all below topics and subsectors in Twitter thread form. And without further ado, we present our GSR Digital Asset Reference Pack. Enjoy.

GSR Crypto Holiday Series Thread of Threads

Source: Twitter, GSR.

Table of Contents

GSR

Topics & Concepts

Bridges

- Different blockchains have different rules, consensus mechanisms and token standards, so one simply cannot send tokens from one to another. Bridges enable the transfer of tokens and data from a source chain to a destination chain, and must do three primary tasks in doing so: data transmission, verification, and interpretation. Bridges may be constructed in various ways, which have different tradeoffs between trustlessness (does the bridge inherit the security of the connected chains or not?), extensibility (is it easy to connect many chains or does each path require a bespoke implementation?), and generalizability (can the bridge send arbitrary data/messaging, or can it only do cross-chain swaps?). Bridges also represent a large attack vector, and are often judged by the number of chains supported, daily active users, and total value locked.
- The three mains ways bridges execute cross-chain transactions are:
    - Lock & Mint: These bridges lock up native tokens in a smart contract originating from the origin chain and subsequently issue an equivalent amount of wrapped tokens to the user on the destination chain. The wrapped tokens act as IOUs that can be later burned to get back the original tokens on the origin chain. Such bridges are collateral efficient as they don't require excess collateral or liquidity, but they fragment liquidity on the destination chain with multiple wrapped versions of an asset and they pose systematic risk to the destination chain if compromised and wrapped tokens on the destination chain become unbacked.
    - Cross-Chain Liquidity: These bridges act as cross-chain AMMs by having LPs provide liquidity to facilitate low-slippage swaps. They are liquidity inefficient, but only deal in native tokens, so risk is confined to LPs.
    - Burn & Mint: These bridges burn native tokens on the origin chain and mint the equivalent canonical tokens on the destination chain. Since they don't wrap tokens or utilize an AMM, they don't fragment liquidity or introduce slippage. But, the bridge must have authority to mint native tokens on multiple chains which is often only the case with real world assets (Circle's CCTP is an example).
- Bridges must come to consensus that the assets on the origin chain are locked or burned before minting on the destination chain. This is done in three ways:
    - Native Verification: The bridge runs a light client of the origin chain as a smart contract on the destination chain to verify. This inherits the security of the

connected chains, but light clients must be custom built for each unidirectional bridge.

- External Verification: This bridge uses its own validator set to reach consensus, which may be a centralized entity, a multisig, or a decentralized group of stakers (typically using PoA or PoS). These bridges are less secure, and are essentially blockchains themselves but without social consensus.
- Local Verification: Locally verified bridges act as central limit order book-based P2P matching platforms and involve a two-party interaction to cryptographically verify counterparties. They are secure and easy to set up between multiple chains, but can only do asset swaps.
- Optimistic Verification: A hybrid of the above and similar to optimistic rollups where it assumes the block headers submitted on the destination chain are valid unless proven otherwise during a challenge period.

Cryptography

- Cryptography is the study of the techniques for securing communication and data in the presence of adversaries. Together with cryptanalysis, it is part of the larger discipline of cryptology.
- Cryptography uses various encryption algorithms referred to as a cipher to secure communication, where a cipher and a secret key transform input data known as plaintext into encrypted output known as ciphertext. Cryptography may be split into symmetric cryptography, asymmetric cryptography, and cryptographic hashing functions.
- Symmetric cryptography uses the same secret key for encryption of the plaintext and decryption of the ciphertext. It is generally more simple and less computationally intensive than asymmetric cryptography, but requires a way to securely share the secret key and requires separate secret keys for each pair of users in a network. Examples include various ciphers (eg. Caesar cipher) and the data encryption standard (DES).
- Asymmetric cryptography (aka public-key cryptography): uses mathematically linked public and private keys to eliminate the need to share a secret key, and is therefore better for large/expanding/active networks. Public keys are freely shareable and created from private keys, which serve as one-factor authentication mechanisms and should be kept strictly confidential. The public and private keys are mathematically related, and while it is easy to calculate the public key from the private key, it is mathematically infeasible to go the other way. This provides the ability to prove that one knows the private key without revealing it, and enables one to encrypt messages to a recipient's public key that can then only be decrypted by the recipient's private key (providing encryption), and the sender's public key can be used to verify that the sender is the holder of the private key without the need to reveal the private key (providing authentication). Examples include DH, RSA, and Elliptic Curve Cryptography, which is used by Bitcoin, Ethereum and others.
- Cryptographic hash functions create a digital fingerprint of any arbitrary amount of data by splitting the data into pieces and running many rounds of local operations on them, losing info as it goes, to ultimately convert the data into a numeric string of fixed length. Hashing functions are one-way (one can't derive the input from the output) and deterministic (returns the same output for a given input). Bitcoin uses the SHA-256 hashing function throughout the protocol.

Custody

- Digital asset custodians store and secure the owner's cryptographic private keys which enables the holder to sign digital asset transactions. Keys are stored in a crypto wallet, which may be hot (connected to the internet; sacrifice security for speed, liquidity, automation) or cold (not connected to the internet; safer but slower and manual).
- Custodians safeguard keys on behalf of the user, while custody technology providers provide tech solutions to enable safe and efficient self-custody by the end user. Custodians assume more risk, are subject to more regulation, and have higher customer service, but offer fewer assets/functionality, introduce counterparty risk, and are slower.
- Core custody technology solutions include:
    - Hardware Security Module (HSM): is a tamper-resistant, government certified physical device that secures cryptographic processes and is not connected to the internet. HSMs are difficult to breach, but constitute a single point of failure.
    - Multisig: require multiple keys to authorize a digital asset transaction, typically requiring a majority of the keys associated with an asset to sign the transaction (eg. 3 of 5). Multisigs alleviate the single point of failure of HSMs, but may not be supported on all blockchains, may result in higher transaction fees or reduced privacy, and introduce smart contract risk.
    - Multi-Party Computation (MPC): is a process that splits a private key into key shares that can be distributed across multiple devices. MPC is flexible, enables complex signing rules, can be changed later or have signer shares revoked, allow a mix of hot and cold wallets, and generate a standard signature, but is newer, less-tested technology and cannot be used with HSMs.
- Custody solutions are administered by various providers (egs. crypto-native specialized providers, traditional financial institutions, cryptocurrency exchanges, prime brokers), may focus on retail or institutions, and often offer additional services like trading, borrowing/lending, staking, wrapping, governance participation, and/or a secure network of customers.

Decentralized Autonomous Organizations (DAOs)

- Decentralized autonomous organizations (DAOs) are blockchain-based organizations managed by a set of automatically enforceable rules that allow for bottoms up decision-making and the organization of communities around shared goals. DAOs are collectively managed and owned by their members, with no hierarchical structure and governance codified into smart contracts. DAOs are essentially coordination mechanisms, offering trustless management and organizational transparency, participatory decision making and borderless collaboration, and novel funding and ownership mechanisms. They are being used to govern protocols, fund grants, distribute creative work, direct investment, unite members socially, and serve other DAOs.
- Membership of a DAO is commonly determined by ownership of the DAO's token, which is typically freely obtainable and allows any holder to table and vote on governance proposals such as how to spend treasury funds. Additionally, a number of DAO frameworks have popped up to automate DAO creation, including Aragon, DAOstack, Moloch, and Colony.
- The most famous DAO is The DAO, a community-directed venture capital fund created in 2016 to invest its treasury based upon member votes. The DAO amassed 14% of all outstanding ETH at the time before $60m was hacked from its treasury and disagreement on whether to restore the funds led to the network splitting into Ethereum and Ethereum Classic.
- DAOs are heavily relied upon for DeFi protocol governance, such as with Uniswap, Compound, and Aave. And more recently, DAOs have been set up as art collectives (PleasrDAO), social communities (Friends With Benefits), and to purchase items (ConstitutionDAO). The largest DAOs are Optimism, Arbitrum, Mantle, and Uniswap (data here).
- DAOs have the potential to one day improve civic engagement, streamline business creation and fundraising, give way to shared financial and social capital, enable unconstrained and self-defined work, better match products/services with demand, and improve meritocratic, contribution-driven ownership and reward. However, DAOs have thus far not lived up to initial hype and are frequently criticized for low voter participation and the potential for coercion, a lack of privacy, and over-influence by large token holders.

Decentralized Finance (DeFi)

- Decentralized Finance (DeFi) is a form of finance that uses blockchain technology, smart contracts, and decentralized applications (dApps) to offer typical financial services such as lending, trading, and investment without intermediaries and in an open and transparent way.
- Protocol developers typically release their dapp as smart contract code deployed to a blockchain such as Ethereum. Dapps commonly start off centralized, but often work towards progressive decentralization and ultimate control by a decentralized autonomous organization (DAO). Dapps typically issue a token to coordinate and incentivize behavior, reward value contribution, and enable exchange.
- By utilizing smart contract code deployed to decentralized, public blockchains and creating peer-to-peer networks, DeFi is both trustless, as programs execute autonomously, and rent-removing, as centralized intermediaries don't exist. DeFi also inherits general blockchain properties such as transparency, openness, and immutability, and introduces new paradigms around ownership, governance, and incentives.
- DeFi activity can be measured by active users, the number of dapps, or total value locked (TVL), which is the total amount of assets locked in DeFi smart contracts at a particular time. Most DeFi activity occurs on Ethereum or its layer twos, given large network effects, however other blockchains like Solana and Avalanche have active DeFi ecosystems and offer advantages over Ethereum such as speed/scalability. Popular dapps include Uniswap (spot DEX), dYdX (perps DEX), Aave/Compound (borrow/lend), Lido (liquid staking), and Maker (collateralized debt position / DAI stablecoin). Data is here.
- DeFi began to flourish in the summer of 2020 – known as DeFi Summer – when borrow/lend platform Compound started incentivizing activity on its dapp with its COMP governance token in a process called liquidity mining.

Derivatives

- Derivatives are financial contracts whose value is dependent on an underlying asset, group of assets or a benchmark, and are used to hedge risk or for speculation purposes. Derivatives prices fluctuate based on changes in the underlying asset, and derivatives may trade on an exchange with standardized terms or bilaterally with more bespoke terms in the over-the-counter market.
- While derivatives in traditional finance also include forwards and swaps, the most common derivatives in crypto include calendar futures, perpetual futures, and options.
    - Calendar Futures: Calendar Futures are financial contracts obligating the buyer to buy and the seller to sell the underlying asset at an agreed upon price at a future date. Futures contracts are standardized, trade on exchanges, and can be settled physically or in cash. Standard crypto futures are mostly comprised of CME's futures products and represent less than 5% of all futures volumes when including perps (ie. most futures trading is done via perps).
    - Perpetuals (Perps): Perps are similar to futures except they don't expire. Whereas futures prices converge to spot prices as expiration nears, perpetuals use a funding mechanism to tether contracts to their underlying spot price. Specifically, when the perp price is greater than the spot price, the funding rate is positive and longs pay funding to shorts and vice versa (the funding rate is also based on the magnitude of the dislocation between the perp and underlying price to incentivize traders to balance demand and tether the perp price to the spot price). Perps improve market efficiency versus standard futures by concentrating liquidity from various listed expiries to a single exchange-traded instrument. Binance dominates perps market share, with OKX and Bybit major perps exchanges. Just 2% of perps volume occurs onchain, with dYdX the clear leader.
    - Options: Options give the holder the right, but not the obligation, to buy (a call option) or sell (a put option) an asset for a specific price called the strike price on, and sometimes before, a predetermined future date. Option prices are determined by the price of the underlying asset, the strike price, the time to expiration, the volatility of the underlying asset, and interest rates. Options traders often monitor risk measures called the Greeks, which measure the change in option prices in response to changes in underlying variables, such as the underlying asset price (called delta), the change in delta due to the change in the underlying (gamma), the change in volatility (vega), and the change in time remaining (theta). Adoption of crypto options has been muted relative to perps and liquid options markets have failed to materialize beyond BTC and ETH. Deribit commands 80-90% of crypto options volumes while Paradigm is an OTC communication/RFQ network that accounts for ~one third of Deribit volume. DEXs represent just 1% of total options trading volume with Ribbon/Aevo, Lyra, and Dopex leading.

Market Making

- Market making is the act of providing two-sided bid and ask quotes along with quote sizes for an asset on an exchange. It increases liquidity for buyers and sellers, where they otherwise may see worse pricing and lower market depth.
- Market makers use proprietary software called an engine or bot to show two-sided quotes to the market, with the engines constantly adjusting bids and asks up and down based on price changes and evolving volume dynamics.
- Traditionally, market makers earn the bid-ask spread – eg. buy for $100 and sell for $101 – in exchange for taking on the risk that the global price moves against them while they hold an asset, ie. price risk. Given the high prevalence of trending markets and one-way order flow, which make it difficult to capture the bid-ask spread, market making in crypto often works via a loan+optionality or a retainer model.
- Differentiators among market makers include liquidity provided, technology and software, history and experience, transparency and reporting, reputation, exchange integrations, the ability to provide liquidity on CEXs and DEXs, and value added services.
- Specific market making KPIs include bid-ask spread, the percentage of volumes, the percentage of top of book (having best bid / ask), and uptime.
- Market making offers vital benefits to projects and exchanges such as greater liquidity and market depth, reduced price volatility, improved price discovery, and dramatically reduced slippage. And perhaps most importantly, tokens play a vital role in decentralized applications, so liquidity is what makes the technology work.

Market Structure

- Crypto market structure has many unique attributes relative to traditional finance, including: 24/7/365 trading, the ability to self-custody, centralized exchanges playing multiple roles including those of the brokerage/exchange/custodian, settlement occurring near-instantly, mixed regulatory oversight, fragmented liquidity, stablecoins used as a base asset, a still-evolving derivatives market, the ability to transact both on and off-chain, and enhanced transparency (for onchain activity).
- Crypto markets offer many key benefits relative to traditional finance, including fewer intermediaries, instant settlement, lower costs, improved efficiency, and greater access.
- Crypto market structure gives rise to several key challenges and risks. First, legal and regulatory oversight is mixed, with many regulatory regimes still in development. Second, there are heightened risks around security (smart contract risk, hacks, scams), custody (lost keys, poor access control), and counterparties (misappropriation, anonymous teams). Lastly, there is widespread capital inefficiency due to fragmented liquidity across venues and across on/off-chain, a lack of full service crypto prime brokers, limited cross-margining, and the required pre-funding of trades.
- Trading can occur on centralized or decentralized exchanges or via over-the-counter (OTC) markets. While some spot trading is done via DEXs (~15% of the total), little derivatives trading happens onchain (~2-3%). Perpetual swaps are by far the most popular trading instrument, followed by spot, with relatively little trading occurring in options or calendar futures.
- Crypto prices exhibit high volatility given their nascency and for structural reasons, though crypto assets have also shown a low correlation with traditional assets. Bitcoin is highly correlated with increases and decreases in global liquidity, and over the short-term tends to move with the macro as well as crypto-specific catalysts and risks. Over the long-term, we expect prices will move with fundamentals, including adoption, usage, development, talent, and capital.

Maximal Extractable Value (MEV)

- Maximal Extractable Value (MEV) is a measure of profit that a miner or validator can extract from block production beyond the block reward and transaction fees by including, excluding, and changing the order of transactions in a block.
- Transaction information, including the transaction's base fee and priority tip collectively known as gas, are typically broadcast to a blockchain network and placed in a pending transaction queue known as the txpool or mempool. Miners/validators may choose which transactions to include in their proposed block as well as the transaction order, and historically they would select transactions from the mempool with the highest gas price and order them by gas spend. However, pending transaction info can be used malevolently by bots looking to front run pending trades, and it quickly became apparent that vanilla transaction ordering based on priority fees was not the profit maximizing strategy relative to a more sophisticated ordering. For example, miners or independent third parties called searches may use sophisticated, bot-based trading strategies to arbitrage price differences between DEXs, wrap a pending DEX trade with its own buy and sell orders (known as a sandwich attack), or execute liquidations for decentralized lending protocols.
- While validators are in prime position to capitalize on such transactions, as they control which transactions are included & in what order, the majority of MEV is extracted by highly sophisticated independent parties called searchers (although most of this accrues to validators). The Ethereum validator role is designed to be as simple as possible w/o requiring specialization, but maximizing transaction fees in this MEV paradigm is very complex and computationally challenging compared to earlier years when miners simply ordered transactions by fees paid. As a result, validators typically do not build their own blocks today (although they still can!), but they typically receive blocks from a mutually trusted relay that intermediates block builders and the block proposer (the validator). Flashbot's MEV-Boost software facilitates this handoff. In this setup, block production is outsourced to a market of specialized builders that aim to maximize MEV, and these builders bid to the block proposer (validator) to propose their block to the network. The validator's role becomes as simple as selecting the highest bid block. Due to the competitive nature of this bidding process, the majority of MEV revenue is paid from the builders/searchers that find it back to the validators that actually have the ability to propose the block that harvests it.
- While some types of MEV, such as CEX / DEX arbitrage ensuring users pay the same global market price and exchange liquidations ensuring loans are paid back, are beneficial, MEV produces a number of negative externalities. These include worse execution and higher prices for traders that are sandwiched as well as broader network centralization concerns given the specialization required to compete.
- Two very important MEV competition vectors include private order flow and latency. All else equal, more transactions are always better from a searcher's PoV, so any searcher/builder that receives private order flow directly instead of it going through the

mempool is advantaged. Additionally, CEX/DEX arbitrage is the largest form of MEV by a wide margin today. And since the price on most DEXs only adjusts on a block-by-block basis (12 secs) while CEX prices are constantly fluctuating, having the lowest latency to get the last bid in is advantageous. This is particularly notable when the real market price of an asset moves sharply within a 12 second slot, enabling the lowest latency actors to provide the most competitive bids right before the auction ends.

- There are various companies and strategies for reducing the negative externalities of MEV, with the most well-known being Flashbots, a research organization seeking to illuminate and democratize access to MEV. After successful products such as Flashbots Auction and MEV-Boost, Flashbots is now working on its SUAVE solution to decentralize block building itself.

Mining

- The Bitcoin blockchain is a network of unrelated computers called nodes that agree on and record valid transactions using cryptography and a consensus mechanism. Special nodes called miners organize pending transactions into blocks and compete to be the first to solve a mining puzzle to add their block to the blockchain and receive the block reward (and related transaction fees). By requiring miners to spend something of value - here computational and energy resources - to solve the mining puzzle, Bitcoin encourages miners to participate honestly, despite the potential presence of bad actors.
- Miners organize pending transactions into a proposed block, and, including a random number called a nonce, will hash their proposed block in an attempt for the hash output to be below the target (a hashing function is a deterministic, one-way algorithm that converts an arbitrary amount of input data into a fixed length, numeric output - see the cryptography section for more). If the hash is below target, the miner broadcasts the winning block to the network, which is verified by other miners and added to the blockchain, and the winning miner will receive the block reward and block transaction fees. If the miner does not solve the mining puzzle, it will change the nonce (and/or transactions) and hash it again, repeating this until it or another miner solves the puzzle, when the process begins anew. Miners typically use rigs with special circuits called ASICs, and each rig model has its own hashrate (the number of hashes the rig can do per second…eg. A Bitmain S19J Pro can do ~100 TH/s, or 10^14 hashes/s) and efficiency (the amount of power used per hash; joules per terahash).
- Bitcoin is pre-programmed to have a maximum supply of 21m bitcoin, which it accomplishes by halving the block reward every four years (the current block reward is 6.25 BTC, which will be halved in April 2024). Moreover, the network adjusts the mining puzzle target up or down roughly every two weeks such that it takes the network (and its then-current amount of hashrate) roughly ten minutes to solve the mining puzzle. Thus, the Bitcoin network produces one new block roughly every ten minutes that when combined with the 6.25 BTC block reward, means the network is distributing 900 new BTC per day (6.25 BTC block reward * 6 blocks / hour * 24 hours / day).
- The odds that any one miner solves the mining puzzle is directly proportional to its hashrate market share (the miner's hashrate relative to the network hashrate). For example, if a miner produces 4 EH/s (4*10^18 hashes/s) while the total network hashrate was 400 EH/s, then that miner would have a 1% hashrate market share and would be expected to receive 1% of all bitcoin block rewards, or 9 BTC / day. This setup encourages a hashrate arms race amongst the miners. Also note that to smooth out revenue and reduce the impact of luck, miners join mining pools to band together hashrate and have block rewards distributed to all pool members in proportion to hashrate contributed, in exchange for a small fee).

- Mining occurs around the world, but miners flock to geographies with strong rule of law and cheap electricity costs. China was the leading geography given its cheap hydro power until it banned mining in May 2021, and now the US is the top geography for mining. Note that Bitcoin mining is often criticized for its high electricity use, though opponents often conflate usage with emissions (mining is over-indexed to renewables, as it's often the cheapest electricity source) and mining can actually encourage renewables development by serving as a flexible base load for otherwise-non economical renewables projects.
- The largest miners include Marathon (26 EH/s), Core Scientific (16 EH/s), CleanSpark (10 EH/s), RIOT (9 EH/s), Bitdeer (8 EH/s), and Cipher (7 EH/s), per The Miner Mag's December 2023 realized hashrate.

Modularity

- Blockchains perform four basic functions in execution, consensus, settlement, and data availability. Traditionally, all four functions were performed by the layer one blockchain, which is referred to as monolithic architecture. However, this led to trade-offs along The Blockchain Trilemma, which states that it's impossible for a blockchain to be decentralized, secure, and scalable at the same time (to see why, a blockchain could increase block size, for example, to increase speed, but that would lead to a larger blockchain and make it prohibitively expensive for some nodes to keep a full copy, ultimately reducing decentralization). However, a new breed of protocols is separating out and optimizing each function, likening their efforts to what Henry Ford did with the Model T and specialization, and allowing each component of the modular stack to be optimized for a more decentralized, secure, and faster blockchain. This concept is known as a modular blockchain or modular architecture.
- In more detail, the four functions of a blockchain are:
    - Execution: Performing computations. This involves taking the beginning state, running the transactions, and transitioning to the ending state.
    - Consensus: The process of agreeing on transactions and their ordering.
    - Settlement: Validating transactions and providing a finality guarantee. For modular chains, this includes verifying/arbitrating proofs and coordinating cross-chain messaging.
    - Data Availability: Ensuring transaction data has been published so anyone can recreate state.
- Examples Include: Ethereum, which has chosen to improve scalability by outsourcing execution to layer two networks. While Ethereum can still operate as a monolith, it is moving towards performing consensus, settlement, and data availability while utilizing layer two scaling solutions for off-chain execution. Celestia is another example, which provides transaction ordering and data availability using data availability sampling and erasure encoding to prove that sufficient data was made available to replicate the blockchain's state, and allows other modular components to plug into Celestia's network to quickly spin up interoperable, customizable, highly performant blockchains. Others include Fuel (a modular execution layer), Tezos (a layer one with an enshrined rollup), and Avail and EigenDA (data availability layers).
- Different constructions may be used to design modular chains, and different solutions may be used for different functions. For example, Solana performs all four blockchain functions and is a monolithic blockchain. A smart contract rollup, by contrast, uses Ethereum for consensus, settlement, and DA, and a smart contract rollup for execution. A validium may use Ethereum for consensus and settlement, off-chain DA through a Data Availability Committee (DAC), and the validium for execution. While a sovereign rollup may use Ethereum for data availability and consensus, with execution and settlement occurring on the sovereign rollup.

- There are many challenges with modular chains, such as their development still being in process, rollup sequencers still being centralized (ie. each rollup currently decides its transactions / transaction ordering and may censor), and fragmented liquidity across disparate execution layers.

Non-Fungible Tokens (NFTs)

- As opposed to fungibility, where two items are the same and interchangeable such as with US dollars or airline points, non-fungibility refers to the property of being solely unique and therefore not freely interchangeable such as with an original painting or plot of land. NFTs are non-fungible (wholly unique) digital assets stored on a blockchain, and may be thought of as blockchain-based digital representations of ownership. Note that NFTs are actually typically not stored onchain for cost reasons, but rather an ID number is stored onchain that points to the URL of a JSON metadata file (Autoglyphs are one of the few counterexamples). Also note that blockchains have token standards defining fungible tokens such as Ethereum's ERC-20, and non-fungible tokens like Ethereum's ERC-721.
- NFTs bear typical cryptocurrency benefits, such as immutability, provable scarcity and provenance, standardization and interoperability, and programmability, and they make digital assets as real and as permanent as objects in the physical world. NFTs can represent ownership in unique items of value like digital art, domain names, intellectual property, and event tickets, and they can be employed in a variety of use cases like collectibles, gaming, media, music, and finance.
- Prominent examples of NFTs include: colored coins on Bitcoin in 2012; CryptoPunks in 2017 (a collection of 10,000 punks with different rarity characteristics, and the first NFTs on Ethereum); CryptoKitties in 2017 (a digital cat NFT collecting and breeding game that clogged Ethereum); Beeple's Everydays NFT sale (sold for a record $69m); and 2021's NBA Top Shot (digital NBA trading card game).
- NFTs historically traded on various NFT marketplaces, with some occupying specific niches, before OpenSea took a 95% market share during the bull market in late 2021. More recently, however, Blur used token incentives and increased trading functionality to unseat OpenSea as the dominant marketplace. Overall, NFT trading volumes, much of which were "PFP" profile pic NFTs, are down ~95% and prices are down 80%+ from peak.
- Despite the severe decline in volumes and prices, many believe the importance of NFTs cannot be understated and that they will ultimately become ubiquitous as new functionality such as programmability and composability improve, new use cases like tokenization and gaming continue to develop, new paradigms around ownership and business models emerge, and as the world becomes increasingly digital.

Staking

- A blockchain is comprised of blocks of transactions created and validated by block producers according to pre-specified, codified rules. However, as open networks where participants may be malicious, blockchains require block producers to expend something of value to prevent bad behavior. Proof-of-stake (PoS) based blockchains like Ethereum do this by requiring block producers (called validators in a PoS system) to lock cryptocurrency into a smart contract in a process known as staking.
- Along with additional balancing mechanisms, validators are chosen at random to produce a block in proportion to their stake, and receive staking rewards derived from transaction fees and protocol emissions for the work they perform, such as proposing and validating blocks. Validators, however, may see some of their stake slashed if they intentionally or unintentionally perform their duties poorly. As such, staking is vital to the proof-of-stake consensus process and is what secures the network.
- To stake, individuals may either run a validator node or delegate tokens to a validator in exchange for a small percentage of the staking rewards. Staking rewards vary based on protocol design, the staking participation rate, activity on the network, vesting periods, and which validator is chosen (for delegators). Risks include an unbonding period as stake is typically prohibited from immediate withdrawal, the potential for slashing upon poor performance, and opportunity costs as staked tokens cannot be used for other activities.
- To get around high opportunity costs, many staking service providers distribute derivative assets known as liquid staking tokens (LSTs) that not only represent staked tokens but also accrue interest and can be used in DeFi protocols such as for loan collateral or to LP to a DEX. Lido staked ether (stETH) is the largest example.
- Many dapps and centralized digital asset service providers offer “staking” where users deposit tokens into a smart contract or centralized module to earn rewards / boosted rewards, garner governance rights, etc. While this is also known as staking, it is quite different from staking as part of a blockchain’s consensus protocol and is more often used to reduce token supply, increase token demand, and reward users.

Tokenization / Real World Assets (RWAs)

- Overview: Tokenization is the process of bringing off-chain assets, often known as real world assets or RWAs, that primarily originate outside of blockchains onchain to enable onchain tracking, trading, programming, and management. Many different types of assets may be tokenized, such as commodities, collectibles, financial instruments, intellectual property, and real estate, among others. Given the benefits and improvement over existing constructs, there is burgeoning interest from corporations, crypto-natives, and regulators alike, and the global tokenization market is expected to reach $16T by 2030, per The Block.
- Benefits: The benefits of tokenization include:
    - Asset Management and Administration: streamlined operations, reduced administrative burdens, automated and transparent record keeping
    - Market Efficiency and Liquidity: greater investor access from lower administrative costs and fractionalization, improved standardization, reduced settlement times, lowered reliance on intermediaries, improved asset efficiency from composability
    - Financial Inclusion: lower investment minimums, access to more capital sources
    - Economic Growth: improved access to capital and financing by a larger, more diverse set of participants
- Process: RWAs are brought onchain through the tokenization process, which, per The Block, includes:
    - Identification: Choose the RWA to bring onchain
    - Verification: Establish the ownership and value of the asset through legal docs or appraisals. A trusted third party like a lawyer or auditor can verify authenticity, ownership, and valuation.
    - Tokenization: Create a digital token or set of tokens to represent the asset on the blockchain. Each token typically represents a fractional ownership or specific claim on the asset, and the token's properties and functionality can be defined using smart contracts.
    - Issuance: The verified asset info and created tokens are recorded on the blockchain, with token issuance done through an ICO, an STO, or direct listing.
    - Custody / Management: Asset management and custody ensure the safekeeping of the physical asset and the management of its onchain representation, often involving both traditional asset custodians and blockchain based custody solutions.
- Examples: Stablecoins are the best known example of tokenization, with stablecoins most often tokenizing US dollars, but also other assets like gold (egs. KAU, PAXG, XAUT). The market for tokenized US Treasury bills has grown rapidly, with leaders being Franklin Templeton ($300m), Ondo's OUSG ($130m), and Matrixdock's STBT ($85m). Outside of treasuries, other debt instruments are being tokenized like private

credit (by Defyca), structured debt (Intain), debt securities (Obligate). In addition, several protocols tokenize or serve as a marketplace for less liquid tokenized products such as Centrifuge, Goldfinch, Maple, RealT, BSOS, and Re, while others are tokenizing equities and indexes like Backed and Swarm. Lastly, tokenization extends to carbon credits (Ecowatt, Flowcarbon), physical collectibles (Collector, Tangible), and even data indexing (The Graph), KYC (Shyft Network), and jobs markets (Human Protocol), though the latter are typically outside of the current tokenization / RWA narrative.

- Challenges: Despite the benefits, there are various challenges tokenization / RWAs must first overcome to reach their full potential. First, robust and clear legal and regulatory frameworks must be established. Second, standardization needs to occur around asset representation, ownership determination, and user identity. Third, interoperability needs to improve to consolidate users and liquidity across chains and applications. Lastly, data, custody, and audit processes need to improve.

Tokenomics

- Tokenomics is the economics of a protocol's tokens and encompasses various supply and demand characteristics.
- Tokens play a vital role in decentralized entities by coordinating and incentivizing behavior, rewarding value contribution, and enabling exchange. As such, strong tokenomics may support protocol objectives, create/enhance a sustainable economic model, and accelerate long-term protocol growth and value creation.
- Tokenomics design starts with the goals of the protocol in mind and then examines how a token can help. Tokenomics is not about reducing supply to increase price, but more about matching supply and demand. There are many tokenomics frameworks, but studying supply and demand is perhaps the most popular.
- Supply: Token supply is often codified into smart contracts and is more formulaic than demand. Several notable items around token supply include:
    - Supply Definitions: There are various definitions of token supply including: Circulating supply is the number of tokens currently circulating and immediately available for sale; Total supply is the number of tokens that were created minus burned (and includes tokens locked in smart contracts); and, maximum supply is the hard-coded limit on the total tokens that will ever exist, indicates remaining inflation.
    - Supply Metrics: A token's current and future supply is impacted my many different components. These include emissions schedule (many protocols have a built-in increase in their circulating supply to incentivize and reward activity), allocation (tokens may be created and allocated via a fair launch or pre-mine), vesting (pre-mined tokens may be subject to vesting schedules to restrict significant supply from hitting the market at once), and distribution (who currently holds the tokens and in what amount, where the presence of a few large holders presents a risk).
    - In general, a token with most of its max supply already out or with steady, predictable inflation encouraging its usage, that was fair launched or pre-mined with gradual, lengthy vesting schedules, with a high community token allocation, and with a well-diversified distribution with no overly large-holders is generally in a good place to steadily absorb demand as it develops over time.
- Demand: Token demand is based on fundamental and speculative characteristics, and is driven by the benefits the token provides.
    - Demand Creation Mechanisms: Token demand may emanate from various sources, such as for use within the protocol (egs. value exchange, governance, access discounts, etc.), protocol revenue sharing with token holders or the potential thereof, moneyness, and speculative demand.
    - Demand drivers are not created equal. Governance rights are generally of low value, per low voter participation. Speculative demand cuts both ways, with it able to both help and hurt token prices. And revenue sharing is a strong

potential benefit and demand driver, but is tough to do in the current regulatory environment. Overall, protocols should focus on providing and growing real use cases/utility to drive demand for their token, and then meet this demand with supply.

Zero Knowledge Proofs (ZKPs)

- A zero-knowledge proof (ZKP) is a method that allows one party (known as the prover) to prove to another party (the verifier) that a statement is true without revealing any other information. To illustrate, lets say your friend has on a blindfold, and is holding a green ball and a red ball. You want to prove to your friend that the balls are different colors without revealing any information about the balls. You ask your friend to put the balls behind his back and either switch hands or not, and then to show you again, at which point you can tell him whether he switched the balls or not. With one round and one right answer, your friend may start to believe you, but not fully as you would have had a 50% chance of guessing correctly. But with each subsequent round and correct response, the probability that you're simply guessing moves towards zero and your friend will eventually become convinced that the balls are different colors without you revealing any information about the balls or anything else.
- ZKPs are used in blockchain mainly for privacy and scaling purposes. Examples of the former include hiding transaction information and minimizing information sharing, while an example of the latter include zero knowledge rollups, which scale a layer one blockchain like Ethereum by processing transactions off of Ethereum mainnet before batching, compressing, and posting to the layer one state data along with a zero knowledge proof (known as a validity proof) that proves the computation was correctly executed. Future use cases include cloud-scale verifiable outsourced computation, open third-party analytics on anonymized data, and enhanced trust, privacy, and remuneration with decentralized identity.
- ZKPs utilize arithmetic circuits to prove the validity of statements, are probabilistic (can't say for certain, can only say with a high degree of confidence), may be interactive (as in the example above) or non-interactive (which is what blockchains use), and most often take the form of zk-SNARKs in crypto. ZKPs have only recently moved from the theoretical to the practical, and are rapidly improving on key areas like prover time, proof size, verification time, and the trusted setup.
- The downsides of ZKPs are that they are in the early stages of development, are probabilistic rather than deterministic in nature, require many interactions or heavy computation, and typically have some minimal trust assumptions in the trusted setup, which is the procedure to produce the standard parameters of the proof system (though some ZKP implementations don't require a trusted setup).
- ZKPs are similar to other technologies like multi-party computation (enables multiple parties to share data for computing tasks without revealing each other's data) and fully homomorphic encryption (enables computation on encrypted data without needing to decrypt it first).
- Popular protocols featuring ZKPs include Aleo, Anoma, Mina, Tornado Cash, Iron Fish, Manta Network, Aztec, Argent, Starknet, zkSync, and Penumbra to name a few.

Subsectors

Blockchain Gaming

- Video games are increasingly utilizing blockchain technology to incorporate crypto-based payments, rewards, and ownership into games. This includes everything from facilitating in-game transactions to the creation of in-game digital assets like NFTs to validating and recording all blockchain transactions that happen in game.
- Blockchain-based games have many benefits, including:
    - Decentralization / Trustlessness: Games are more secure, transparent, trustless, and traceable.
    - Ownership: Users truly own assets in the form of self-custodied NFTs, transforming in-game purchases from an expense to an asset.
    - Enhanced Functionality: Users may resell their assets to others. Composability may enable users to port assets between games or developers to build on top of existing games.
    - Greater Impact: Blockchain-based games can embrace user-generated content or DAO-based community governance, where users may be able to create worlds/in-game assets and craft storylines or refine the game's economic model.
    - Incentives: Token incentives can reward users for their contribution to the game, such as accomplishing tasks, producing popular content, or onboarding new users.
    - New Revenue Streams: Rather than mainly selling in-game items, developers can now oversee a dynamic virtual economy where they may take a cut of all commerce.
- Blockchain-based games first appeared in late 2017 with the launch of CryptoKitties. CryptoKitties enabled users to collect and breed digital cats based on a cattribute-determining, smart contract-based breeding algorithm and was so popular that it clogged Ethereum. The next hit blockchain-based game came in 2021 when Axie Infinity, a digital pet universe play-to-earn game allowed players to collect, breed, and battle NFT-based fantasy Axie characters to earn tokens through gameplay. At its peak, Axie had nearly three million daily active players, many of whom quit their day job and relied on the game for income. Other popular games include Ember Sword, Star Atlas, Splinterlands, The Sandbox, and Sorare.
- Gamers have generally been skeptical of blockchain-based games, viewing them as a money grab by developers, and GameFi has also been criticized as a veiled Ponzi scheme that relies on an ever-increasing player base and may fall just as quickly as it grew. In addition, blockchain games face a number of other challenges as well, such

as regulatory, security, scalability, UI/UX, and generally poorer gameplay/graphics. However, developers are now focusing primarily on the games themselves as well as the unique benefits blockchain technology brings, while eschewing out ponzinomics incentives. Additionally, given long development times, we are finally on the cusp of the first true AAA blockchain-based games, with games like Illuvium, Shrapnel, and Otherside as examples.

- There are several other players in the blockchain gaming ecosystem in addition to the games themselves, including development studios (egs. Sky Mavis, Blockade, Mythical, Dapper, Wax), marketplaces (Immutable, Rarible, OpenSea), blockchains/scaling solutions (Immutable, Ronin, Polygon, Flow, Wax, Hive, Safa, Oasys), infrastructure/tooling (Enjin, Ronin, Forte), and gaming guilds (Yield Guild Games, Avocado DAO, Merit Circle).

Borrow/Lend Protocols

- Borrow / Lend markets, such as Aave and Compound, are a cornerstone of DeFi and allow users to permissionlessly borrow or lend cryptoassets via smart contracts to gain leverage, take short market exposure, or earn extra yield. Smart contracts enable such services to be facilitated on a non-custodial basis without an intermediating party.
- Often referred to as peer-to-pool lending, lenders lend their cryptoassets to a liquidity pool from which borrowers can borrow from. Interest rates are commonly variable and determined algorithmically based on supply and demand (i.e., pool utilization). Higher demand for borrowing drives up interest rates and provides greater returns for lenders, and vice versa.
- Lenders typically get a receipt token corresponding to their lending deposit similar to the design of liquid staking tokens. The lending yield either accrues into the balance of one's receipt tokens (aTokens) or into the price of one's receipt tokens (cTokens). Given the peer-to-pool lending model, lenders can only call back a loan when there is spare capacity and they may be unable to redeem when a lending pool is at full utilization (i.e., all deposits are borrowed). However, since interest rates are typically variable and rise with utilization, one would expect some borrowers to return the loan under these circumstances, allowing lenders to reclaim their collateral from the pool. Additionally, since receipt tokens are provided in correspondence with a loan, the lender could sell their loan position on the secondary market via a decentralized exchange if liquidity was urgently needed.
- Borrowing typically requires overcollateralization to help reduce the risks of the protocol accruing bad debt. Borrowers face liquidation risks in the event that borrowed assets rise sharply in value or the posted collateral falls in value, and most protocols charge an additional fee if a position is liquidated so the health factor of one's loan should be monitored closely. Borrowing / lending assets are typically only supported on a permissioned basis as risks are commonly pooled, so supporting smaller/riskier assets introduces greater risk of the protocol accruing bad debt. As a result, typically only large tokens are supported, but protocols like Euler have taken an approach of isolated lending markets and allowing borrowing/lending markets to form permissionlessly.
- Borrow / lending markets have also introduced entirely new financial primitives that are non-existent in traditional markets, with perhaps the most prominent example being flash loans. Flash loans allow borrowers to borrow any available amount of assets without putting up any collateral so long that the liquidity is returned to the protocol in the same block (i.e., imagine ETH is more expensive on Uniswap than Sushiswap, you may want to borrow USDT to buy the ETH on Sushi and sell on Uni, clipping the spread before repaying the loan in the same block). If the loan isn't repaid in the same block the whole flash loan transaction fails (i.e., capital doesn't leave the lending pool).

Central Bank Digital Currencies (CBDCs)

- Central Bank Digital Currencies (CBDCs) are widely available digital forms of a country's fiat currency issued by a central bank. As CBDCs are a liability of the central bank itself, they have no credit or liquidity risk. Central banks aim for CBDCs to not harm monetary and financial stability, to coexist and complement other payment mechanisms and forms of money, and to support efficiency and innovation.
- There are two main types of CBDCs: Retail CBDCs are used by the public for day-to-day payments, while wholesale CBDCs are used as an instrument for settlement between financial institutions.
- CBDCs can improve payments and payments infrastructure, aid policy and enhance economic growth, facilitate global commerce and improve remittances, and support financial inclusion and fight inequality. Risks of CBDCs include potential impacts on financial system stability, monetary policy, the cost/availability of credit, and privacy.
- There are many design choices for CBDCs around interest, household limits, structure, payment authentication, functionality, access, and governance. For example, the architecture could be centralized or decentralized, transfers cold run through a central intermediary or be peer-to-peer, the system and payment access/authentication may be identity/account-based or token-based, the ledger could contain simple liability data or more sophisticated payment information, and ledger access can be relatively open or more restricted. Moreover, central banks must determine which responsibilities they will provide in addition to issuance, such as distribution, system administration, and device management.
- There are currently 11 CBDCs that have launched, 21 in pilot, 33 in development, and 46 in the research phase (data here).

Centralized Exchanges (CEXs)

- Centralized cryptocurrency exchanges are intermediary platforms connecting token buyers and sellers and enabling digital asset trading. Unlike in traditional finance, most CEXs have an expanded role, acting as the broker, exchange, and custodian.
- CEXs create user virtual balances upon receiving fiat/ token deposits, only transacting onchain upon withdrawal. This improves speed and reduces costs, but introduces large trust assumptions with the exchange custodying user deposits.
- CEXs use a central limit order book (CLOB), where crosses (ie. pairs) on the exchange have bids (the amount one is willing to pay for an asset) and asks (the amount one is willing to sell an asset for). The exchange matches bids and asks on a price-time priority, though market participants see order book depth, meaning they can see bids and asks beyond the best bid and ask.
- Orders may be maker orders, which make liquidity and add to the order book (ie. limit order), or taker orders, which are executed immediately at the best bid or offer (ie. market order) and reduce liquidity. Maker orders often have materially lower or even negative transaction fees in some cases while taker orders are typically much more expensive. Also, exchanges typically offer transaction fee discounts at higher volume tiers.
- Different CEXs offer trading in different crypto assets and products, such as spot, perpetual swaps, and options. Exchanges often offer their own token, which may grant holders trading fee discounts, access to launchpad listings, and can be used as gas on an exhange's associated blockchain.
- The largest exchanges include Binance, Upbit, OKX, and Coinbase for spot, Binance, OKX, and Bybit for perps, and Deribit for options. CEXs represent 85% of total spot volume (vs. DEXs) and 97% of derivatives volumes.

Decentralized Cloud (compute & storage)

- Decentralized cloud protocols utilize blockchain technology to offer storage and computing services:
    - Cloud Storage: provides space to store data, but off-site in cloud-based servers via the internet. Cloud storage is used for web hosting, file sharing, virtual desktop hosting, automatic data backups, etc, and enables users to protect data from disaster, secure sensitive data, supplement storage space, and reduce operational costs.
    - Cloud Computing: is any internet-based service that performs computational processes or runs applications. It is used for cloud-based communication platforms (eg. email), SaaS, remote data analytics, website content, and management systems (egs. CRM, CMS, ERP), and it facilitates easier collaboration, enables remote work, improves business agility, and consolidates important files and applications.
- Decentralized cloud companies deliver these services via a P2P network of service providers, who either put otherwise-idle infrastructure to work (eg. renting out unused storage space on your computer via Filecoin) or create and run the network from scratch after buying bespoke hardware in exchange for token rewards (eg. Flux miners buying and running Flux nodes in exchange for Flux rewards). Decentralized cloud providers compete against oligopolistic tech behemoths like Amazon AWS, Google Cloud Platform, and Microsoft Azure and offer lower prices, increased resilience, greater privacy, and censorship resistance. Examining decentralized storage and computing in more detail:
- Decentralized Storage: Decentralized storage solutions distribute and store data across multiple nodes or computers, eliminating the need for a central server and enabling data permanence and censorship resistance. They serve as a marketplace to allow anyone, from individuals to large cloud companies, to rent out unused hard drive space in exchange for a fee and seek to coordinate and ensure the process (which includes encryption, storage, retrieval, contract administration, storage audit, and more). Typically, users encrypt data, which is then split into smaller pieces called shards that are often duplicated for redundancy purposes and stored by nodes on the network. The nodes communicate with each other through the P2P protocol, receive token incentives that ensure availability and reliability of storage, and retrieve and share data when requested by users, all in a transparent and tamper-resistant manner.
    - Examples include Filecoin, Storj, Arweave, and Sia to name a few. Filecoin is built on top of IPFS, which stores files on a network of nodes using a content-addressed rather than a location-addressed system (this method assigns each data file a unique cryptographic hash that acts as a fingerprint for the file known as a CID), making it easier to share files without worrying about its location and ensuring that the files are tamper-proof. Filecoin sits on top of IPFS to provide a P2P marketplace for storage services, incentivizes storage

and retrieval providers, and ensures the process goes smoothly (miners post slashable collateral and submit proofs that they stored the data, known as proof-of-replication, and proof that they are continuing to store the data, known as proof-of-spacetime). Other storage solutions offer similar services but with some variation. For example, rather than relying on a single host for file delivery like IPFS does, Storj uses erasure coding and parallel file delivery for performance and availability. Arweave is another example that, unlike IPFS which is not permanent and requires a pinning service to make it so, enables a single one-time fee to be paid in exchange for storing a file forever.

- Decentralized Compute: Decentralized compute protocols use geo-distributed compute resources to provide computation, data processing and data interaction services, which are often offered alongside data storage. Most offer CPU, RAM, and GPU (a newer offering), and enable computation on anything that can be put into a Docker container. In addition, many compute protocols offer enterprise grade service level agreements and may be compatible with existing centralized offerings like Amazon S3 for easy integration.
    - Examples include: Flux incentivizes miners to buy specialized node hardware that provides compute resources, and also offers decentralized storage (Flux Drive) and a decentralized wallet/identity solution (Zelcore). Akash is a Cosmos-based decentralized cloud marketplace connecting users and providers of compute and storage services, where individuals or corporate servers bid on jobs with their unused capacity to save users up to 90% versus AWS. And Internet Computer uses data centers and high-end node hardware to replace the legacy tech stack, serve web content directly to users, act as a public compute platform, and extend, decentralize, and enhance the web. Note that other protocols replicate smaller components of the current internet stack, such as Fleek, a decentralized edge network / CDN (like CloudFlare).
- Companies are increasingly moving to a hybrid cloud model with multiple providers, since traditional cloud costs have roughly doubled over the last two years and it doesn't handle novel tech like AI well. In addition, companies are also adding back on-premise servers to put computing tasks closer to the data source (known as edge computing) to reduce latency and save on bandwidth costs. Such hybrid infrastructure reduces dependence on and lock-in of the mega-tech providers and makes it easier for companies to adopt decentralized solutions.

Decentralized Exchanges (DEXs)

- A decentralized cryptocurrency exchange (DEX) is a decentralized application that functions as a peer-to-peer marketplace allowing cryptocurrency trades to occur directly between users. DEXs inherit the positive properties of crypto (decentralized, permissionless, trustless, censorship resistant, immutable, etc.), with two of the more notable characteristics being the removal of rent-extracting intermediaries and the enablement of self-custody.
- DEXs typically use a deterministic pricing algorithm called an automated market maker (AMM) instead of a central limit order book given speed and cost limitations of the underlying blockchains they're built on. AMMs utilize pools of tokens locked in smart contracts called liquidity pools and work by allowing anyone (called a liquidity provider or LP) to deposit tokens into a liquidity pool. The price of the tokens in the liquidity pool then follows a formula, such as the constant product market maker algorithm ($x*y = k$, where x and y are the amounts of the two tokens in the pool and k is a constant), resulting in the ratio of tokens in the pool dictating the price, slippage being determined by the size of the trade relative to the size of the pool, and the ability of liquidity to always be provided regardless of the trade size. Prices are then tethered to the global market price by arbitragers, who buy and sell tokens in the liquidity pool as it deviates from the global market price to push them back inline.
- Liquidity providers in a liquidity pool receive trading fees in proportion to the liquidity they provided to that pool. In addition, protocols often incentivize the provisioning of liquidity by giving liquidity providers protocol tokens, in what's called liquidity mining. Liquidity providers are exposed to impermanent loss, which is where one of the two assets provided to the pool moves materially differently than the other, causing the liquidity provider to have been better off by simply holding the two assets outright rather than providing the liquidity.
- DEXs represent about 15% of total spot trading volume and ~2-3% of total derivatives trading volume.
- Uniswap is the most well-known and used DEX, with its v2 implementation enabling permissionless pool creation (anyone can spin up a pool), v3 enabling concentrated liquidity (LPs can provide liquidity over a specific range to improve capital efficiency), and the coming v4 offering hooks (for improved pool customization). Outside of Uniswap, various protocols have iterated on the basic AMM model or introduced new models to offer improved performance for things like highly correlated tokens (Curve) many-asset liquidity pools (Balancer), and extended to derivatives such as with virtual AMMs for DeFi perpetuals protocols.

Decentralized Identity

- With over 1b people unable to prove their identity, the average internet user having 100 passwords, and identity fraud leading to tens of billions in annual losses, there are many issues with the current system of identity. Digital identity originally took the form of users creating individual accounts with each website (centralized model), and later saw users sign in via Google or Facebook (federated model, which sacrifices privacy for convenience/safety), and more recently to a new decentralized paradigm, known as self-sovereign identity (SSI) or decentralized identity, where users own and control their personally identifiable information (PII) and data without the need for centralized parties.
- Rather than have PII reside with and controlled by centralized authorities who may abuse this power, decentralized identity allows individuals to self-custody their own data. To do so, users create decentralized identifiers (DIDs) and are later awarded verifiable credentials (VCs) by issuers, where, using cryptography, users are able to prove ownership over the DID and assert claims that can be authenticated by verifiers.
- Decentralized identity leads to improved experiences (sign in with your wallet and bring your own data to websites), enables users to profit from their own data (receive payment for sharing data or viewing ads), enhances digital reputation (take out an undercollateralized loan), increases privacy (selectively disclosure information), and reduces risk (self-custody data). Use cases range from identity verification to compliance, access control, Sybil resistance, governance, employee management, medical records, supply chains, and more.
- There are several challenges decentralized identity systems face. First, the solution set is highly fractured across use cases and blockchains and there is little interoperability (there are over 90 DID method specifications across 80+ blockchains), and entities such as the World Wide Web Consortium (W3C) have a tall task in developing standards. Also, key management and UX remains difficult for most users. Additionally, it will take material time for user behavior to change and for decentralized identity to crack the strong network effects of the current digital identity construct. Issuers will have to become comfortable with new managing and issuing frameworks, and businesses and verifiers need to adopt verification technologies to facilitate acceptance of these credentials.
- There are many decentralized identity and credentialing protocols, with some built on generalized blockchains like Ethereum (POAP and ENS, which issue proof of attendance NFTs and name-to-address resolution, respectively) and others built as blockchains optimized for decentralized ID management (egs. Sovrin, Veres One, and Ontology). There are also protocols that offer credentialing-as-a-service, giving other dapps the ability to easily issue credentials, such as Galaxe and Gateway.

Decentralized Physical Infrastructure Networks (DePIN)

- Given the billions in investment required to set up and maintain large physical infrastructure and hardware networks, many areas of technology function as all-powerful oligopolies, immune from new competition. However, blockchain technology challenges this model by allowing projects to bootstrap and coordinate such networks via user-contributed infrastructure and token incentives. Such decentralized physical infrastructure networks or DePIN (also known as token-incentivized physical infrastructure networks TIPIN or Proof of Physical Work PoPW) incentivize users to contribute and operate devices on the network that may come together to rival incumbent networks in size.
- DePIN has several key differentiators. First, it enables networks to be bootstrapped via crowd-sourced hardware. Second, it results in the networks being owned and operated by its users rather than by large, rent-extracting corporations. Third, they democratize access to the network, as anyone can run a node or use its services. Lastly, they are decentralized and censorship resistant.
- In theory, DePIN enables a flywheel, where token rewards incentivize supply-side participants to deploy infrastructure. As the infrastructure network grows, developers create products and end users increase demand. As demand increases, fees generated from end users attract more hardware providers and the cycle starts anew. In practice, DePIN has done a fantastic job bootstrapping hardware networks, but they have not always been met with commensurate demand from users.
- DePIN networks are created from user-contributed hardware that may be new or existing-but-idle. The former involves users purchasing and operating nodes/hotspots in exchange for protocol tokens, while the latter involves users contributing already-existing, but idle resources, also in exchange for token payment. For example, Helium was the first to create a large, user-contributed new hardware network when it/third-party manufacturers sold plug-and-play Helium Hotspots to users to power IoT devices (Hotspots both mine HNT to build/secure the network and provide connectivity to nearby devices in exchange for HNT rewards). While Helium built the world's largest LoRaWAN network, demand did not materialize as anticipated, and Helium is now more focused on rolling out a 5G cellular network. Other protocols such as Filecoin and Arweave allow users to rent or purchase unused hard drive space on others' machines in exchange for FIL or AR tokens, putting excess storage space to use while also increasing data persistence and censorship resistance as files are stored on multiple machines.
- DePIN is being utilized across various infrastructure subsectors, including:
    - Storage Networks: Filecoin, Arweave, Sia, Storj
    - Databases: Ceramic, Tableland
    - CDN Networks: Fleek, Meson
    - VPN Networks: Boring, Deeper, Orchid
    - Compute Networks: Akash, Flux, Render, Livepeer, Gensyn

- 5G Networks: Helium, Pollen, XNET
- LoRAWan Networks: Helium, Chirp
- WiFi: WiCrypt, Wifi Dabba
- Sensor Networks: Hivemapper, DIMO, Planetwatch, WeatherXM
- Energy Networks: React, Arkreen

Liquid Staking Tokens (LSTs)

- Liquid staking is an innovation in the Proof-of-Stake (PoS) blockchain ecosystem (see Staking) that enables stakers to maintain liquidity while concurrently earning staking rewards. In exchange for depositing assets to be staked with a liquid staking provider, users receive liquid staking tokens (LSTs) that serve as a proof of deposit and provide a liquid, fungible, and reward-bearing claim on the staked assets that are otherwise illiquid. In addition to retaining liquidity, LSTs can be freely used for other DeFi purposes, such as for collateral to borrow funds or to provide liquidity in a DEX. Overall, LSTs improve capital efficiency and increase flexibility while still earning staking rewards in exchange for a small fee priced as a percentage of the rewards.
- Rewards typically accrue to the LST in one of two ways. First, rewards may accrue into the LST's price and thus the LST becomes more valuable than the underlying as rewards are earned. Or, rewards may accrue into the LST's token balance, increasing the supply of the LST (e.g., new LST tokens are minted in proportion to the value of the rewards accrued). While the latter model allows the price of the LST to track the underlying token 1:1, it may have negative tax implications in certain jurisdictions.
- Vectors of competition and variables to consider include:
    - Is the LST battle hardened? How long has the provider been live on mainnet.
    - How much stake does the provider control?
    - Who manages the stake? Is it one entity? Multiple entities? Can anyone become a manager of stake (permissionless node operator) or is it a whitelisted function?
    - How much liquidity does the LST have? Are there many uses for it other than buy/sell liquidity? Is there a broad suite of DeFi integrations?
    - What is the fee structure?
    - Are there any governance implications? Does the underlying PoS blockchain employ rigid stake-based governance or is it a more Ethereum-like soft governance? Does the LST provider have its own token with governance power like Lido's LDO?
    - How is the LST structured?
- Liquid staking has flourished on Ethereum specifically as the network does not allow stake to be delegated natively, so the overwhelming majority of ETH stakers are staking indirectly via staking service providers, and such providers tend to offer an LST. Conversely, ecosystems like Cosmos, Solana, Avalanche, and Polkadot all natively allow delegation, and thus delegators may simply delegate stake directly via the protocol without seeking out a third-party liquid staking provider.
- The most prominent LST is Lido's Staked ETH (stETH), which represents Ether staked through the Lido platform at a 1:1 ratio. There are many smaller competing LST providers on Ethereum too though. The liquid staking ecosystem is much smaller outside of Ethereum, but most other chains have at least one LST provider. For

example, Solana has Jito and Marinade, Cosmos has Stride, which supports liquid staking for all IBC-compatible chains, Avalanche has Benqi, and Polkadot has Acala.

- While liquid staking introduces increased utility and flexibility for stakers, it also introduces new risks and considerations. The value of LSTs can diverge from the underlying assets to an extent as the underlying assets are not immediately redeemable (e.g., the time to unstake varies drastically and can range from days to months or even years in some cases). Additionally, the smart contracts involved in liquid staking add layers of technical risk, including potential vulnerabilities or bugs. Liquid staking may also introduce risks that were not accounted for when the original protocol was designed (e.g., if all stake was delegated to unbonded node operators, new attack vectors may present themselves).

Memecoins

- Memecoins are cryptoassets that originated from internet memes or have a humorous or whimsical character. Such coins gain popularity and value primarily through community and social media hype, influencer endorsements, and viral internet trends, rather than fundamental value or technological innovation. More specifically, memecoins may derive value from evoking certain emotional and psychological contexts, such as the ability to be part of a community or the belief that others will pay more for the token in the future. Such hedonic value is hard to quality, particularly given its behavioral nature.
- The success of memecoins is largely driven by their communities and cultural appeal. These communities often engage in coordinated efforts to promote the coin, creating a sense of belonging and fun. In addition, memecoins are also often created in real time in response to real world events. Lastly, memecoins tend to also frequently have a unit bias, using incredibly low prices at fractions of a cent and very large supplies posing some psychological advantages for some.
- Dogecoin (DOGE) is one of the earliest, most valuable, and most well known memecoins. DOGE was created in 2013 as a joke based on the "Doge" meme featuring a Shiba Inu dog. Dogecoin was a simple Bitcoin heir (a fork of a Bitcoin fork) and was simply meant to be a joke but not innovative. Other examples include: Shiba Inu, Pepe, Bonk, SafeMoon, Dogelon Mars, and many others.
- Memecoins are known for their extreme volatility and speculative nature. Their value can skyrocket or plummet based on social media trends, celebrity tweets, or community-driven hype, making them high-risk investment choices. Indeed, DOGE routinely increases sharply in response to comments from Elon Musk, such as when Elon temporarily replaced Twitter's blue bird logo with the DOGE meme, causing the DOGE token to skyrocket in price. Such short-term games are frequently hype-driven and unsustainable though, and prices often revert rapidly.
- Without any fundamental growth or development reason as to why a memecoin's value should persist, investing in memecoins is often very player versus player in nature. It's often a game of being early and dumping on others rather than a game of growing the pie, though new memecoins are sometimes created with sustained cultural importance and value.

Payments

- The legacy financial system is built on antiquated technology, leading to high costs, long wait times, and in some cases, discriminatory practices, poor user experience, and suboptimal security. For example, ACH and remittance payments can take up to five days to transfer, credit card networks charge merchants 2-3% resulting in higher consumer prices, and a complex clearing and settlement system delays the settlement of stock trades for days after execution, all resulting in suboptimal convenience, cost, risk, and capital efficiency. Even fintech, with innovation largely confined to the front-end, still operates on these traditional, antiquated rails on the back-end.
- Blockchain technology, by contrast, innovates on the back-end to reimagine the rails themselves. Already, blockchain-based payments can occur 24/7/365 at near-zero costs and with near-instant settlement. Businesses can accept digital asset-based payments with only a public key and without the need for specialized hardware or payments to issuers, merchant acquirers, and card networks. And the blockchain itself can serve as a real-time, verifiable, immutable public ledger resulting from open code executed as written to materially increase transparency and reduce disputes. In the future, financial inclusion will increase with permissionless protocols requiring only an internet-connected device to participate, user experiences will improve with key pairs serving as identification, account numbers, and passwords, and security can strengthen with private information self-custodied by the user rather than spread across innumerable institutions, companies, and websites.
- In addition to the payment of money, blockchain technology enables the exchange of many other forms of value and introduces new capabilities not possible with the existing financial rails. Tokenization, for example, will eventually bring the exchange and record of account benefits to nearly all other assets in addition to money, such as with blockchain-based digital forms of traditional securities known as tokenized securities. And these speed and cost advantages introduce new capabilities and constructs, such as enabling previously-impractical micropayments to charge fractions of a penny per song streamed to better reward creators or per web page viewed to reduce DDoS attacks. Programmability will enable new capabilities, such as subsidy payments only spendable on specific categories, composability will make accepted token formats ubiquitous and usable across the digital realm, and fractionalization will improve accessibility and liquidity. These examples, with significant improvements in speed, cost, inclusion, and transparency, only scratch the surface of what's possible.
- Despite vast benefits, several challenges remain for crypto payments. First and foremost, strong network effects exist within the legacy system (merchants accept credit cards because buyers have them and buyers have them because merchants accept them). Similarly, consumer behavior takes decades to change, as exemplified by cash to card conversion (ie. shoppers using a credit card rather than cash) being a multi-decade phenomenon. In addition, regulations are not clear,

acceptance/integrations are currently limited, UI/UX needs improvement, and challenges around fraud/security and chargebacks/disputes need to be solved.

- Examples of digital asset payment systems include: Bitcoin was initially intended to be a peer-to-peer electronic cash system, but has since morphed into a store of value given technical limitations and a fixed supply. Ethereum supports not only its own cryptocurrency ETH but also enables the creation of tokens and development of various payment solutions through its smart contracting abilities. Ripple offers a payment protocol designed to facilitate fast, low-cost international money transfers, offering its services to banks and financial institutions to facilitate cross-border payments of XRP. Stellar is similar to Ripple, though it focuses on providing financial services to individuals with limited access to traditional banking. And Dash focuses on privacy, speed, and UI/UX with its PrivateSend and InstantSend payments features. And stablecoins remain the main payments mechanism today, such as USDT payments on the Tron blockchain.

Scaling / Layer 2s (L2s)

- Ethereum is the most popular smart contract layer 1 blockchain, but given its choice to optimize for decentralization and security, it is slower relative to competing L1s, often experiencing network congestion, low throughput, and high transaction costs during times of high activity. To remedy this, a number of scaling solutions aim to process transactions off of mainnet while also relying to varying degrees on the security of Ethereum mainnet itself.
- The major types of scaling solutions are:
    - Sidechains: an independent blockchain attached to the main chain by a two-way bridge. Sidechains enable EVM-compatible smart contracts for scaling and testing purposes. They may not be as decentralized as Ethereum, and as they have their own consensus mechanism, do not inherit Ethereum security guarantees so are therefore not technically a layer two.
    - State Channels: a process where users transact directly with one another outside of Ethereum an unlimited number of times prior to batching and submitting transactions back to the main chain. State channels enable high throughput and low costs, but require payment channel funds to be locked into multisigs and don't support general purpose smart contracts.
    - Plasmas: Plasmas use smart contracts and Merkle trees to enable the creation of separate blockchains called child chains that are copies of the mainnet and derive their security via fraud proofs that are used to arbitrate disputes on the main chain. However, plasmas cannot scale general purpose smart contracts.
    - Rollups: Rollups execute transactions on a separate chain before batching, compressing, and posting data back to mainnet. Transaction execution occurs off the main chain, but data posted back to the main chain enables anyone to recreate state and verify the validity of the transactions, thus enabling high throughput and low costs while also inheriting many of the security properties of the main chain.
- Rollups are the most popular type of scaling solution and come in two varieties:
    - Optimistic Rollups (ORs): ORs assume transactions processed on the L2 and posted back to mainnet are valid unless the transaction is challenged, at which point a fraud proof will be generated and if proven invalid, the correct state will be recovered and the transaction submitter will see their staked bond slashed. ORs are further along than ZKRs and have a first mover advantage, but have long withdrawal times given the need for a challenge period and require a good actor watching the chain. Examples include Arbitrum and Optimism.
    - Zero Knowledge Rollups (ZKRs): ZKRs bundle transactions and execute them off-chain, and generate cryptographic proofs known as validity proofs that are posted back to mainnet along with batched state changes known as state difs. ZKRs enable fast withdrawals and have fewer trust assumptions, but only

recently saw ZKRs launch on mainnet. Examples include: zkSync, Scroll, Polygon zkEVM, and Starknet.

- Rollups gather many transactions together, execute them off-chain, bundle compressed transaction data or state differentials into a single transaction, and send the data back to Ethereum. Rollups utilize sequencers to collect, order, and send batched transactions back to mainnet. Ethereum rollup sequencers are currently all centralized and simply use FIFO transaction ordering, but there are efforts underway to utilize shared sequencers (multiple rollups using the same sequencer to enable atomic, cross-chain composability) and decentralized sequencers (to improve trustlessness, though challenges exist). Centralized sequencers lead to risks around censorship resistance (a government could force the rollup to censor) and liveness (if the sequencer goes down, the L2 cannot fully operate, though some have safety mechanisms where users can force funds back to the L1). Rollups earn money from the sequencers, with revenues coming from L2 transaction costs and in the future, the ability to order transactions and extract MEV. Rollup expenses are mainly the cost of posting data back to mainnet, which in Ethereum will fall after it implements EIP-4844 in its Dencun upgrade in early 2024.
- Challenges remain for general purpose rollups (egs. Optimism Mainnet and Arbitrum One) as apps compete for L2 blockspace, cross-chain fragmentation and bridging risks between rollups increases, and dev overhead to deploy a dapp on multiple chains increases. One popular solution is to create a composable rollup ecosystem with shared infrastructure, enabling ecosystem chains to get customizable execution environments, streamlined cross-chain communication, and increased revenue opportunities. Note that this is part of the trend for roll-apps, where each dapp is its own rollup, often built as an L3 sitting on top of an L2, and therefore doesn't need to worry about blockspace scarcity caused by other applications. Examples of rollup ecosystems, which often are accompanied by developer toolkits, include: Optimism SuperChain, Arbitrum Orbit, zkSync HyperChain, and Starknet L3s.
- Example L2s / rollups include:
    - Arbitrum: Arbitrum is an optimistic rollup offering Arbitrum Rollup (general purpose OR; current is Arbitrum One), Arbitrum AnyTrust (OR with off-chain data for ultra-cheap costs, current is Arbitrum Nova), Arbitrum Orbit (interconnected universe of customizable chains that settle to One or Nova), and Arbitrum Stylus (enables smart contracts to be written in Rust) all powered by Arbitrum's technical stack called Nitro.
    - Optimism: OP mainnet is an EVM-equivalent Layer 2 optimistic rollup. It offers the OP Stack, the standardized, shared, and open-source development stack that powers Optimism, and The Superchain, a network of chains that share bridging, decentralized governance, upgrades, and communication protocols that's currently in development. Importantly, Coinbase built its layer 2 Base using the OP Stack.

- Polygon: Polygon offers a suite of scaling solution options, with its most popular being Polygon PoS, a sidechain that relies on its own validator network for security but that Polygon is looking to upgrade to a zkEVM validium (similar to a ZKR but with data made available off-chain). Polygon also has Polygon zkEVM and its Polygon Chain Development Kit, and is convertingits MATIC token to an ecosystem-wide POL token.
- Mantle: Mantle is an optimum, which is similar to an OR, but uses off-chain data availability. Mantle uses MantleDA and its data availability committee for its data availability.
- Linea: Built by ConsenSys, Linea is a type 2 zkEVM, meaning its fully compatible with Ethereum dapps.
- Starkware: StarkWare develops StarkEx, a standalone permissioned Validity Rollup, and StarkNet, a permissionless decentralized ZKR. Starknet utilizes STARKs rather than the more common SNARKs for its zero-knowledge rollups, which offer enhanced security but have larger proof sizes that take longer to verify. Starknet uses the Cairo smart contract language, though does have a compiler that can transform Solidity code to Cairo code.

Stablecoins

- Stablecoins are digital currencies whose value is tied to that of another asset, most often US dollars, and are designed to reduce the volatility inherent in cryptocurrencies. Stablecoins are predominantly used to facilitate simple and efficient cryptocurrency trading (fiat to crypto conversion is clunky, thus ~75% of crypto trading volume involves at least one stablecoin), though are increasingly used within decentralized applications and for payments, remittances, and settlement. Stablecoins offer many benefits including speed, cost, transparency, inclusion, and programmability and are considered one of the "killer apps" of crypto.
- There are three general types of stablecoins, delineated by their collateral:
    - Fiat-collateralized, where a centralized party is responsible for minting and burning the stablecoin, generally backing it with cash or fixed income instruments. Fiat-collateralized stablecoins have the strongest track record of price stability, are simple, and will be the first to have a robust regulatory regime, but they introduce centralization into an otherwise decentralized environment and thus require additional trust assumptions. Fiat-collateralized stablecoins make up ~90% of stablecoin market cap, and USDT and USDC are the most popular examples.
    - Crypto-collateralized, where a smart contract relies on monetary policy, arbitrage and overcollateralization to maintain its peg. Crypto-collateralized stablecoins eliminate many of the centralization drawbacks of fiat-collateralized stablecoins, but require over-collateralization, making them capital inefficient. Maker's DAI stablecoin is the most prominent example.
    - Algorithmic, where a stability mechanism maintains the peg despite the absence of collateral and are more theoretical in nature. Algorithmic stablecoins offer capital efficiency and decentralization, though have thus far failed to offer price stability, with failed examples including Empty Set Dollar, Basis Cash, Iron Finance, and TerraUST.
- Stablecoin companies make money via transaction fees or by earning interest on the reserves backing the stablecoin. There has been increased focus on reserve transparency, with many fiat-collateralized issuers releasing monthly attestation reports, particularly as questions around Tether's USDT backing have been present throughout crypto history. Lastly, note that stablecoin regulation varies by jurisdiction, with robust regulatory regimes in some (eg. the EU's MiCA), still developing/unclear (eg. US), or outright banned (eg. China).

Blockchains

Bitcoin

- The Bitcoin network is a decentralized database/distributed ledger comprised of a network of computers called nodes running the Bitcoin Core software. All nodes follow pre-set, codified rules to agree on valid transactions and keep the same local copy of the database, which simply records who paid what to whom and when.
- Special nodes called miners work to be the first to solve a mining puzzle in order to propose a block and receive bitcoin in the form of a block reward. By selecting the winning miner according to prespecified, codified rules and requiring miners to expend energy and computational resources to solve the puzzle, the network of unknown parties is able to agree on which valid transactions to add to the decentralized ledger without a central leader and despite the potential presence of bad actors.
- Payments on the Bitcoin network are denominated in bitcoin, a digital asset by the same name and of which is limited in supply to 21 million, made possible by the halving of block rewards approximately every four years.
- Such a construct - an open network of unrelated nodes following code-based rules to agree on and locally record valid transactions without a central leader - results in key properties of decentralization, trustlessness, censorship resistance, immutability, permissionlessness, pseudonymousity, and scarcity.
- Bitcoin was originally designed as a “peer-to-peer electronic cash system”, but is now commonly viewed as a store of value / non-sovereign digital reserve currency given technical limitations and a fixed supply.

Ethereum

- Blockchains historically had limited transaction types and were home to a single, siloed application like Bitcoin or Namecoin, forcing developers wishing to create new applications to build their own entirely new, purpose-built blockchain. However, Vitalik Buterin conceived Ethereum in 2013 as a Turing complete virtual machine, able to process general-purpose code and arbitrary computation without needing to modify the underlying blockchain itself. To do so, nodes on Ethereum not only keep track of payments like Bitcoin does, but also process code known as smart contracts and reach agreement on network state. Vitalik likens this to the introduction of the iPhone, which acts as a platform for any third-party developer to create an app. Moreover, common standards and open-source code enable applications to interact and build on each other, creating a composable programming environment. And similar to Bitcoin, Ethereum is decentralized, trustless, censorship resistant, immutable, permissionless, open source, and pseudonymous.
- Ethereum previously utilized a proof-of-work consensus mechanism similar to Bitcoin, but in September 2022 switched to proof-of-stake in an effort known as The Merge. Since Ethereum is a decentralized protocol running on thousands of machines globally, it could not simply stop the network to make the upgrade, but instead had to do it “mid-flight.” As a result, The Merge is considered one of the greatest feats in the history of blockchain engineering. Miners have been replaced by validators who stake (ie. lock) ETH into a smart contract and propose or validate blocks in exchange for rewards roughly proportional to their market share of the total network stake. Validators who perform their duties poorly or act maliciously will lose out on staking rewards or even see their stake slashed.
- Users pay “gas” to interact with the network, such as for deploying a smart contract or sending tokens, and to incentivize proof-of-stake validators to process transactions and secure the network. In return, validators receive both protocol emissions and transaction fees. Gas, which is priced in gwei (one billionth of one ETH), is a multidimensional resource and the price per unit of gas is dynamic, fluctuating based on supply and demand. Gas includes both a base fee, which scales up and down based on network demand, and an optional tip, which goes to the validator. As base fees are burned, Ethereum can have negative net issuance (more burned than created) during times of high activity, leading to the deflation meme of ultrasound money.
- Ethereum historically chose to focus on decentralization and security at the expense of speed. Ethereum’s roadmap, which includes six phases such as The Merge and The Surge, aims to improve on these characteristics, with the notable approach of offloading computation to layer two scaling solutions (ie. the rollup-centric roadmap). Notable roadmap highlights include single-slot finality that will materially reduce the amount of time for transactions to be considered final, danksharding that will materially reduce data availability costs (ie. proving that data was made available to recreate

state), and proposer-builder separation, which will separate the role of block builder and block proposer to mitigate and redistribute some of the negative externalities of MEV.

- Ethereum has a rich ecosystem of decentralized applications (dapps) spanning DeFi, NFTs, DAOs, and more. While other blockchains have optimized for other characteristics such as speed, activity continues to congregate on Ethereum, particularly during bear markets, given strong network effects.

GSR Resources

Topics & Concepts

Bridges	
Cryptography	Cryptography Decrypted
Custody	Institutional Digital Asset Custody
DAOs	Community Governance with Decentralized Autonomous Organizations
Decentralized Finance	DeFi Summer 2.0: Don't Call it a Comeback Innovations in Decentralized Finance with DeFi 2.0
Derivatives	Crypto Derivatives: An Ecosystem Primer Reading the Crypto Derivatives Tea Leaves
Market Making	Pondering the Future of Market Making Curve Wars & The Battle For DeFi Liquidity
Market Structure	Crypto Derivatives: An Ecosystem Primer
Maximal Extractable Value	The Battle of the Bots and Maximal Extractable Value
Mining	Bitcoin Mining Part 1: Overview of a Transaction Bitcoin Mining Part 2: The Inputs Bitcoin Mining Part 3: The Bitcoin Mining Business Model Bitcoin Mining Part 4: Environmental Considerations and Regulation The Future of Bitcoin Mining Finance
Modularity	
Non-Fungible Tokens	Punks & Dunks: NFT Volumes Soar Dude, Where's my NFT? Sports and the Blockchain
Staking	Securing the Blockchain with Staking A Guide to Ethereum Staking Enabling Staked ETH Withdrawals: Shapella
Tokenization / RWAs	
Tokenomics	Accelerating Protocol Objectives with Tokenomics

Zero Knowledge Proofs	
Subsectors	
Blockchain Gaming	Axie Infinity Goes Parabolic
Borrow/ Lend Protocols	
Central Bank Digital Currencies	At the Peak of Central Bank Digital Currencies
Centralized Exchanges	Pondering the Future of Market Making
Decentralized Cloud	
Decentralized Exchanges	Pondering the Future of Market Making
Decentralized Identity	The Next Wave of Crypto Adoption with Blockchain Domains
DePIN	
Liquid Staking Tokens	The Great Staking Debate: Lido Dominance and Ethereum
Memecoins	
Payments	
Scaling / L2s	On the Road to Mass Adoption with Ethereum Scaling
Stablecoins	Stablecoins in the Crosshairs Solving the Stablecoin Trilemma with Algorithmic Stablecoins Dissecting the Terra/UST Bank Run
Blockchains	
Bitcoin	How Bitcoin Works Bitcoin for Institutions Believe: Our Crypto Thesis What's on Tap for Taproot? What a Futures-Based ETF May Mean for Bitcoin The Long and Arduous Road Towards a US Spot Bitcoin ETF Sizing the Massive Spot Bitcoin ETF Opportunity
Ethereum	Ethereum's Updated Roadmap: A Guide to The Merge and Beyond Ethereum Ecosystem Is Getting Busier, Not Quieter, Amid Layer 2 Shift EIP-1559 Let it Burn

About GSR

GSR has over a decade of extensive experience in the crypto market, serving as a trusted liquidity provider and active, multi-stage investor. Our suite of services includes OTC Trading, Derivatives, and Market Making. GSR is actively involved in every major sector of the digital asset ecosystem, working with token issuers, institutional investors, miners, and leading trading venues.

Find out more at www.gsr.io.

Follow GSR for more content: Twitter | Telegram | LinkedIn

Required Disclosures