

Crypto Ecosystem 2021

Some of the interesting categories and projects worth reading about. For higher-level introductions see the A16Z [Crypto Canon](#) and [Startup School](#). [Gemini](#) and [Kraken](#) also have great introductions to all the currencies and projects. I also wrote a doc on [Bitcoin](#).

It's useful to play around with these protocols. My suggestion is to download the [Metamask Chrome extension](#), buy some Ethereum on Coinbase, send it to your Metamask wallet, and then visit [Compound](#) for lending, [Uniswap](#) for trading, or [OpenSea](#) to buy some digital art (NFTs).

[Currencies](#)

[Stablecoins](#)

[Layer 1 Protocols](#)

[Layer 2 Protocols](#)

[Cross-chain Interoperability](#)

[Sidechains](#)

[Self-hosted Wallets](#)

[Hosted Wallets](#)

[Lending](#)

[Centralized Exchanges \(CEX\)](#)

[Decentralized Exchanges \(DEX\)](#)

[Other Financial Applications](#)

[Synthetic Assets](#)

[Oracles](#)

[Governance](#)

[Social Tokens](#)

[Decentralized Media](#)

[Decentralized Storage](#)

[Digital Art](#)

[Internet Infrastructure](#)

[Gaming](#)

[NFT Marketplaces](#)

[Insurance](#)

[Index Funds](#)

[Developer Tools](#)

[Other Projects](#)

Currencies

Digital alternatives to fiat currencies or store of values like gold and silver. While there are many medium-of-exchange tokens (tokens used to pay fees on an internal blockchain network), there are only a few promising store of value assets (Bitcoin, Ether, ZCash, etc). Stablecoins seem to have taken over the unit-of-account function, although Ether is widely used to price NFTs.

- Bitcoin - [Whitepaper](#) - Store of Value, Digital Gold. It's unlikely to achieve mass adoption as a medium of exchange, especially since transactions are taxable events, but it may be used as a settlement layer between banks, with transactions happening in layer 2 or centralized networks like VISA. You can see more of my Bitcoin thoughts [here](#).
- Ethereum - [Whitepaper](#) - Smart contracts
- ZCash - [Whitepaper](#) - Privacy coin, but [regulator friendly](#). It has the best privacy technology around, while also providing a way for regulators to request access to their citizens transactions, if needed.
- Dogecoin - [Web](#) - "Future currency of Mars" - Initially a joke, forked from Litecoin. It's become an internet legend, which makes it valuable despite not being actively developed. I expect it to stay around for a long time.

Stablecoins

Coins backed by stable assets like USD, EUR, or gold to reduce volatility. Stablecoins form the backbone of Decentralized Finance (DeFi) protocols. The most popular stablecoins rely on centralized organizations like Coinbase or BitFinex, who custody real US Dollars before "minting" and distributing a digital equivalent.

- Dai - <https://makerdao.com/en/> - Decentralized, multi-collateral backed stablecoin, pinned to USD. Uses a network of price oracles to provide the exchange rates for collateral pairs (ETH/USD, BTC/USD, etc). Users deposit collateral and receive a low-interest loan of Dai. From there, Dai trades on the open market, which means its value can fluctuate based on supply and demand. To keep the peg, Dai relies on arbitrageurs who buy/sell DAI on exchanges, redeem/load collateral and pocket the difference. Maker incentivizes these arbitrageurs by providing (or charging) a small interest rate. The system works because people trust they can always exchange 1 DAI, for the corresponding amount of collateral from the Maker smart contract.
- USDC - <https://www.centre.io/usdc> - Centralized stablecoin backed 1:1 with USD. Coinbase buys US Dollars and mints USDC based on customer demand. Users trust they can always redeem 1 USDC for 1 US Dollar.
- Tether - <https://tether.to/> - Centralized stablecoin backed 1:1 with USD. This is the largest stablecoin, but the institution BitFinex minting these coins has a shady history.

Layer 1 Protocols

Protocols that run their own blockchain network. Ethereum is dominant and has huge network effects (developer tools, ERC-20 tokens), but high fees and slow transactions. Ethereum is here to stay, but newcomers can capture market share with differentiating features, especially as cross-chain infrastructure matures. The winners will depend on how fast Ethereum can scale via side chains or Layer-2 solutions. The most likely outcome will be a multi-blockchain world with many winners, especially as cross-chain interoperability solutions (Polkadot, Ren) improve.

- Ethereum - [Web](#), [Whitepaper](#) - Biggest smart contract platform with widest adoption and biggest developer community. In-progress migration to Proof-of-Stake consensus and [layer 2 scaling solutions](#) which hopes to increase throughput to 100k TPS.
- Solana - [Web](#), [Whitepaper](#) - Uses Proof-of-history consensus to scale transactions up to 65K TPS vs Ethereum's 15 TPS. Small, but growing developer ecosystem, backed by some big names, including FTX / Alameda Research.
- Zilliqa - [Web](#), [Overview](#), [Whitepaper](#) - A sharding-first approach which scales linearly with the number of nodes, increasing throughput and reducing costs. A subset of nodes process transactions in a shard and then bubble up the results to a central pool of validators who run PoW to confirm the blocks. It also provides computational sharding (Map-Reduce), for compute-intensive workloads. It's [smart contract language](#) isn't user-friendly, but they plan to implement a higher-level framework similar to Solidity. The team is based in Singapore, without any name-brand backers.
- Flow - [Web](#), [Whitepaper](#) - Created by Dapper Labs (CryptoKitties, NBA top-shot) to improve scalability (5k TPS) and useability ([friendly smart-contract language](#)) with built-in logging and smart-contract upgrading. The chain is new, but supported by one of the strongest teams in Crypto and backed by some reputable investors. The chain scales by separating consensus from compute, allocating work across different node types (Consensus, Verification, Execution, Collection), where each type is optimized for its particular job.
- Binance Chain - [Web](#), [Whitepaper](#) - Binance-developed blockchain for non-custodial trading and smart contract execution. It powers the Binance DEX which allows fast and cheap order-book style trading and swaps. The original Binance Chain is based on the Tendermint consensus algorithm used by Cosmos and focused on payments/trading use cases. The [Binance Smart Chain](#) provides EVM-compatible smart contract support, for fully-functional dapps like PancakeSwap. It sacrifices decentralization for speed, however, with only 21 validator nodes elected for consensus.

Layer 2 Protocols

Build on top of a layer 1 protocol to improve scalability, lower fees, or add other features. There are many approaches and each has pros/cons. We will likely see multiple successful solutions operating in parallel, with each layer 2 protocol optimizing for different types of transactions (e.g. asset transfer, data transfer, privacy, etc). For Ethereum, the community is rallying around rollups (optimistic rollup, zk-rollup) as the preferred scaling approach.

- [Lightning Network](#) - Scaling solution for Bitcoin payments. Users open private, off-chain payment channels with merchants/dapps where they can transact instantly with near-zero fees.
- [Ethereum Scaling](#) - A number of approaches to scaling ethereum are in development. We will see multiple different approaches deployed and adopted for different use cases (transactions, smart-contracts, privacy, etc). The winners will be the solutions adopted by the biggest applications (Uniswap, Compound, Aave, Balancer, Synthetix).
- Matic - [Web](#), [Whitepaper](#) - A [plasma-based](#) approach to scaling via sidechains. Similar to the Bitcoin Lightning network, it enables users to open state channels with merchants and dapps for rapid, zero-fee transactions. As of 2/2021 they now consider this existing sidechain an "out-of-favor Layer-2 solution" and are pivoting to an aggregator SDK.
- Loopring - [Web](#), [Exchange](#) - A ZK-rollup scaling solution, which uses relayers (nodes) to batch transactions which are verified with ZK-Snark proofs. It's the first Ethereum Layer 2 solution to launch a mainnet. It has an order-book exchange, uniswap swap/pool, and wallet. The user first deposits money from MetaMask (Layer 1) to Loopring (Layer 2), and then you can make instant swap/trades for extremely low fees (comparable to centralized exchanges). I swapped 400 DAI for \$0.36 on Loopring, while Uniswap cost me \$60 in fees (gas, liquidity).
- ZKSync - [Web](#), [Docs](#) - ZK-rollup solution, launched on MainNet. Allow writing mostly general smart contracts, but only using their custom smart-contract language, [Zinc](#). Buterin thinks ZK-rollops will win in the long-term, but Optimistic rollups may dominate short-term, since they're more compatible with Solidity/EVM. SushiSwap and Yearn Finance seem to be supportive of this protocol.
- Optimistic Ethereum - [Docs](#) - Highly anticipated optimistic rollup solution, but still no MainNet. Synthetix seems to be [adopting](#) this solution, citing how easy it is to migrate their existing smart contracts, without major changes.
- StarkWare - Backed by ZCash team. Another ZK-rollup team that uses ZK-STARK (I think) instead of ZK-SNARK.

Cross-chain Interoperability

Layer 1 protocols designed to connect multiple blockchains together. As we move towards a multi-blockchain world, interoperability protocols will play a big role. The winners will be the ones who are most developer-friendly and best integrate with the Ethereum ecosystem.

- Polkadot - [Web](#), [Whitepaper](#) - An ecosystem of interconnected blockchains from the co-founder of Ethereum, and an SDK for creating your own blockchain in any language that compiles to WebAssembly. The architecture includes a main parent Relay Chain which handles consensus and a number of child networks (parachaine) which execute transactions. The parachains can pass arbitrary messages and trigger smart contracts on different networks in the same transaction. Notably, the smaller parachains benefit from the security of the main chain, so they don't have to bootstrap their own ecosystem of validators.

- Cosmos - [Web](#), [Whitepaper](#) - An ecosystem of interconnected blockchains from the [Tendermint](#) team. It provides an SDK for creating your own blockchain on top of the “Cosmos Hub”, which provides interoperability with other blockchains built on the Cosmos network. A lot of big name blockchain [projects](#) run on Cosmos. Cosmos requires each subchain to run its own network of validators, but in return each chain has greater control over transaction finality. Cosmos is good for projects with deep resources who want more control over their chain (e.g. Binance Smart Chain). Cosmos currently only supports cross-chain asset transfers (not x-chain smart contract execution, like Polkadot).
- Avalanche - [Web](#), [Whitepaper](#) - An ecosystem of interconnected blockchains. It uses a novel leaderless consensus algorithm based on the S3 concept of “gossip” where validators sample a subset of their peers to determine valid transactions. This enables greater scalability. It’s subnet-based architecture allows developers to attach custom, public or private blockchains with their own internal application logic, while still benefiting from global consensus. The Avalanche Default Chain is broken into 3 components: a payments chain, metadata chain, and smart contract chain, each optimized for a particular use case. Currently scales to 5000+ TPS, without layer 2 or sharding. It also supports an Ethereum subset called Athereum, which enables developers to use familiar Ethereum APIs and tools (MetaMask).
- Polygon - [Web](#), [Whitepaper](#) - An ecosystem of interconnected blockchains. A hybrid approach where developers can deploy sovereign networks (like Cosmos, bring your own validator), or piggyback on Ethereum’s security (like Polkadot).
- THORChain - [Web](#), [Whitepaper](#) - A non-custodial bridge network where users can swap assets between external chains (Bitcoin, Ethereum) without routing funds to a merchant address, like most sidechains do (WBTC, renBTC, etc). It does this by creating “vaults” on each external network, which are smart contracts programmed to store and return funds to users who want to swap. It uses a network of “witness” nodes who verify the user sent the funds to the Bitcoin vault, before releasing funds on the Ethereum network. For example, if a user wants to swap BTC for ETH. They send BTC to the THORChain Bitcoin vault address. The network of witnesses verify the user sent the funds and then trigger a smart contract on the Ethereum network to send an equivalent amount of funds to the user’s Ethereum address. THORChain uses a network of Oracles to determine exchange rates. The network is secured with PoS where nodes need to bond (stake) RUNE in order to participate in the validation process. It’s built using the [CosmosSDK](#), which makes it interoperable with any other applications built on the Cosmos network.

See: [Cosmos vs Polkadot](#)

Sidechains

Using tokens from one blockchain (Bitcoin) on a completely separate blockchain (Ethereum). This usually involves a network of custodians who store the native tokens and mint/burn the pegged tokens for users.

- [Wrapped Bitcoin](#) - Use your Bitcoin on the Ethereum network. This unlocks a lot of liquidity sitting in the bitcoin network and makes it available for use as collateral in lending protocols.
- [Ren](#) - Protocol for creating wrapped tokens that works across blockchains. Integrations include renBTC and renZEC and future integrations with the Solana ecosystem, which offers scalability benefits.
- [Binance Bridge](#) - Binance Chain is an independent blockchain which cannot natively interact with other blockchains like Ethereum. In order to work around this, Binance developed a “bridge” service which swaps native tokens (ETH, BTC, ECR20) into pegged Binance coins (BEP2, BEP20), allowing users to trade native tokens on on the Binance DEX.

Self-hosted Wallets

Private keys are stored on your phone or desktop. Good for small amounts of money and for playing with the DeFi ecosystem.

- MetaMask - <https://metamask.io/> - Most popular Ether wallet. Gateway to DeFi. Only supports ethereum-compatible tokens.
- Coinbase Wallet - <https://wallet.coinbase.com/> - The offline wallet of Coinbase. Supports multiple blockchains (ETH, BTC), which is convenient.
- Trust Wallet - <https://trustwallet.com/> - Supports multiple blockchains (BTC, ETH, Binance). Native DEX integration (Uniswap, PancakeSwap, Binance DEX). Recently bought by Binance.

Hosted Wallets

Your private keys are held by an institution, good for large amounts of money.

- Coinbase - <https://www.coinbase.com/> - Top bank in the US

Lending

Borrow and lend money, earning interest and liquidity tokens.

- Compound - <https://compound.finance/> - Lend/borrow with over-collateralized loans
- Aave - [App](#), [Whitepaper](#) - Flash loans, borrow/return in a single transaction. The recently released an [undercollateralized](#) loan feature, where lenders can loan to a trusted party without full collateral.
- Curve - [App](#), [Whitepaper](#) - lending and borrowing stablecoins
- Notional Finance - [App](#), [Whitepaper](#) - Fixed-rate lending (others are variable-rate)

Centralized Exchanges (CEX)

Traditional order-book model to match buyers/sellers. Trades not recorded on the blockchain. Users do not control their private keys. But these exchanges are more efficient and lower fee.

- Coinbase Pro - <https://pro.coinbase.com/> - Biggest exchange in the US
- Binance - <https://www.binance.us/en/home> - World's largest exchange
- FTX - <https://ftx.com/en> - Derivatives and synthetic assets

Decentralized Exchanges (DEX)

Self-custody and trade tokens without a central intermediary like Coinbase. Cool because you can trade with anyone in the world, without signing up or giving personal info.

- Uniswap - [App](#), [Whitepaper](#) - Biggest DEX, 1:1 token swaps using liquidity pools
- Balancer - [App](#), [Whitepaper](#) - Swap baskets of assets like index funds
- 1Inch - [App](#), [Whitepaper](#) - Aggregates results across multiple DEX
- Serum - [App](#), [Whitepaper](#) - Traditional order-book style DEX built on the Solana blockchain which provides significantly lower fees. The experience is a bit clunky since it runs on a different blockchain, but they recently acquired [Ren](#) to help with cross-chain interoperability. It's developed by the Alameda / FTX exchange founders, who can provide deep liquidity and long-term support. The question is whether people care enough about staying decentralized to move from existing performant CEX, and how well they can provide access to ECR-20 tokens on Ethereum.
- [Binance DEX](#) - Decentralized, non-custodial exchange built by the Binance team. Most of the trading pairs are priced in BNB, which fluctuates frequently, but they have a growing amount of BUSD pairs. The process for getting funds onto the Binance Chain is non-trivial and requires buying BNB on a centralized exchange and then sending to the exchange or a compatible wallet, like Trust Wallet.

Other Financial Applications

Other interesting financial applications.

- Perpetual Protocol - [Docs](#) - Another type of fancy derivative product called "Perpetual Contracts" e.g. margined futures with no expiration.
- Opyn - <https://opyn.co/> - Trade options on Ethereum

Synthetic Assets

Proxy assets for real-world assets like real estate, commodities or stocks or digital assets on other chains.

- Mirror - [App](#), [Whitepaper](#) - Brings traditional, off-chain assets like stocks and bonds to the blockchain. Uses Oracles to obtain off-chain prices.
- Synthetix - [App](#), [Whitepaper](#) - Derivatives and synthetic assets

Yield Farming

Recursively lending money and then relending the borrowed money to maximize fees. I would also include “smart” asset management here.

- Yearn.finance - [App](#), [Whitepaper](#) - Users deposit money in “vaults” which are designed by strategists to maximize returns via yield farming. Yearn is expanding into other categories, including lending and insurance.
- Alpha Finance - [App](#), [Whitepaper](#) - Leveraged lending and yield farming.

Oracles

Bridge real-world data and blockchain. In order for prediction markets to work, or synthetic assets like futures on silver, blockchains need a way to access real-world data.

- Chainlink - [Web](#), [Whitepaper](#) - Allows smart contracts to read/write off-chain data from external data feeds and APIs. Responses from oracle nodes and data sources are aggregated to improve reliability. Oracles must stake \$LINK to participate and accrue a reputation score based on their past performance.

Governance

Protocols for managing decentralized communities. On-chain voting and decision-making.

- Algorand - [App](#) - Protocol for building self-governing communities

Social Tokens

Tokens to support creators and grow communities. This would remove middlemen (Spotify, Twitch, Amazon) and let fans support creators directly. Creators could switch between platforms without losing their monetization capabilities.

- Rally - [App](#) - Platform for issuing creator coins. Initially targeting gamers and streamers. Backing from major investors.
- Roll - [App](#) - Platform for issuing creator coins. One of the interesting coins is WHALE, which represents a vault of NFTs currently valued at 30M. Users can buy into the vault, which is similar to an index fund.

- SourceCred - <https://sourcecred.io/docs/> - Framework for incorporating social cred and rewards into existing Telegram and Discord communities. Users accumulate cred for posts with lots of upvotes, etc.
- Friends With Benefits - <https://fwb.help/> - A private discord community with its own social token to reward active contributors.

Decentralized Media

Decentralized content platforms connecting creators directly to fans without middlemen. Can also help with “last-mile” availability in remote locations without centralized CDNs.

- Audius - [App](#), [Whitepaper](#) - Spotify for music streaming. They’re building the infra, but plan to partner with user-facing applications.
- Theta - [App](#), [Whitepaper](#) - Video streaming network. They’re building the infra, but plan to partner with user-facing applications like YouTube, Vimeo, Netflix. They have their own blockchain to allow for more scalability and micropayments.

Decentralized Storage

Decentralized file stores like S3 or Google Drive.

- IPFS - [Docs](#) - Interplanetary file system, supported by [Brave](#). IPFS users persist the data they want on their own IPFS nodes. E.g. Host-your-own data.
- FileCoin - [Docs](#) - IPFS does not include a built-in mechanism to incentivize the storage of data for other people. Filecoin is like S3, where nodes can rent storage space. Filecoin can be seen as a cold storage layer, perfect to safely store large batches of data long-term. Applications could use IPFS directly for hot storage and caching.
- Arweave - [Docs](#) - File store focused on censorship resistant permaweb. Tackles the problem of how to incentivize miners to persist data forever without “renting” space like S3 or FileCoin.

Digital Art

A type of [NFT](#) (Non-fungible token) which holds artwork that can be collected and sold to other collectors. Ethereum has a [standard way](#) to define these NFTs, which makes it easy for creators to build and list their own NFTs on marketplaces.

- HashMasks - [App](#) - Beautiful designs and a unique mechanic where you can change the name of the work after holding the token for ½ year. Each work has attributes that are ranked by rareness. The most rare attributes command the highest prices.
- CryptoPunk - [App](#) - The first major crypto art collection, which gives it historical significance and value. Only 10k ever created.

- CryptoKitties - [App](#) - Digital cats you can collect and trade.
- NFTX - [App](#), [Whitepaper](#) - Index funds for portfolios of digital art. A curator first purchases a bunch of individual NFTs and locks them in a Balancer pool, so they can be traded like a fungible token. A certain number of shares are created and sold to investors.
- NBA topshots - [Web](#) - Buy highlights from NBA games. Use them in an upcoming game.

Internet Infrastructure

Decentralized versions of basic internet infrastructure and tools.

- Orchid - [Web](#), [Whitepaper](#) - Decentralized VPN. Current providers are centralized and sometimes sketchy. This is a safer approach, but may struggle with scalability.
- Civic (Identity.com) - [Web](#), [Whitepaper](#) - Identity verification and selective sharing of PII with vendors. A way to prove who you are. Can be used for undercollateralized loans.
- Helium - [App](#), [Whitepaper](#) - WiFi network for IoT devices using LPWAN (Low Power Wide Area Network). They have a [mining device](#) you can buy for your apartment.

Gaming

Games and virtual worlds who use the blockchain to keep track of digital assets. Players enhance their gameplay experience by purchasing digital goods and can trade them with other players on external marketplaces (OpenSea).

- Axis Infinity - [Web](#) - Collect and battle cute digital creatures for fun and profit.
- PoolTogether - [Web](#) - No-loss party games where players pool funds together and winners are paid-out using the interest earned by all the money in the pool
- Decentraland - [Web](#) - 3D virtual world where players can collect and trade digital goods and land with other players
- Gala Games - [Web](#) - Game studio building [Mirandus](#), an upcoming MMORPG built on the blockchain owned by the players. Selling land in game as NFTs. One of their [deeds was recently purchased for \\$800k](#).
- The Sandbox - [Web](#) - 3D Game and game creation platform on the blockchain. Play and govern games and create and trade land and 3d game models using their SAND token.

NFT Marketplaces

The EBay or Etsy for digital collectibles and artwork. There are many types of [NFTs](#), but digital collectibles are currently the most popular use case.

- Rarible - <https://app.rarible.com/> - Search, filter, browse both auctions and buy now listings. They have their own token so users can invest and benefit from the website's growth.
- OpenSea - <https://opensea.io/> - Search, filter, browse both auctions and buy now listings. Images, animations, land in virtual worlds

Insurance

Blockchain-based insurance protocols, which protect funds in the event of smart-contract hacks or bugs which result in lost customer funds. In the future, they can scale to real-world assets.

- Nexus Mutual - [App](#), [Whitepaper](#) - Smart-contract insurance for hacks and protocol bugs. Users pool money into reserves which earn interest, but are depleted in the event of claims. Requires users to buy insurance for specific smart contracts and time periods.
- Armor.fi - [App](#), [Whitepaper](#) - An insurance broker built on Nexus Mutual, which provides real-time, pay-per-second coverage across a range of protocols, without users having to open up individual contracts for each protocol. Their smart insurance will track your funds across protocols and bill you accordingly.

Index Funds

ETFs and index funds which track baskets of assets like Vanguard.

- Index Coop - [App](#) - Community-managed index funds built on the [Set Protocol](#). They currently manage the largest crypto ETF, the [DefiPulse](#) index. [Roadmap](#). [Vision](#). [Tokenomics](#).
- PieDao - [App](#) - Index-funds for baskets of digital currencies, build on Balancer.

Developer Tools

Libraries, frameworks, and infrastructure for building Ethereum applications.

- Solidity - [Docs](#) - Most popular Ethereum smart contract language.
- Vyper - [Docs](#) - A Python-based Ethereum smart contract language which is simpler, but more restrictive to increase security. Pairs with [Brownie](#) for testing.
- Truffle - [Docs](#) - Framework for testing and deploying smart contracts. JavaScript and NPM-based. Supports multiple blockchains. Pairs with [Ganache](#) for deploying a local blockchain.
- Infura.io - [Docs](#) - A relay service, which submits your transaction to the Ethereum nodes. Helps with optimizing gas fees and retrying stuck transactions.

Other Projects

