



A MESSARI REPORT

# Crypto Theses for 2021

*Key trends, people, companies, and projects  
to watch across crypto, Bitcoin, and Ethereum,  
with predictions for 2021*

SPONSORED BY

Bitstamp

BABEL  
FINANCE

UPDATED 12/17/2020



## I won't hold it against you if you skim this 134-page monstrosity and immediately think: too long; won't read.

That's how I feel about most books, long reports, and verbose blogs as well. But when it comes to year-end crypto analysis pieces, to paraphrase a great American classic: "There are many others like it, but this one is mine."

I've been a full-time analyst in the industry for more than seven years. (Back then, it was just called "bitcoin.") As an independent writer, then early stage investor, then research and data services entrepreneur, I know the struggle of staying on top of this industry's information flow. It's a tall order to ferret out noisy, unreliable data from your content diet, discover real insights, and map new developments to your priors.

Fortunately, I have the benefit of a 25-person team with some of the best analysts in the world ([join us!](#)); amazing software tools that make it easier to spot trends and organize data ([buy them!](#)); and scar tissue to help with pattern recognition (for better and for worse).

It's still a full-time job to keep up, but it's possible.

I write these year-end pieces (for the fourth year in a row, because I'm a masochist) to help myself, my team, and you start the new year with a clean mental model you can refer back to as the bull market picks up steam and things get wild in 2021.

I'm impatient when it comes to crappy content. Fifteen minutes wasted on a surface-level Medium post is fifteen minutes not spent digging in on the next breakout asset or critical trend. Or fifteen minutes falling behind a competitor. Or worse, fifteen minutes fueling up the brain with soy vs. meat\* that leads to a bad decision from which it takes many, many multiples of those fifteen minutes to recover.

Believe it or not, I wrote this beast to save you time and money. Crypto moves fast, but it's worth the investment. I hope you enjoy this, and can refer back to it as a reference in the year ahead.

Cheers,  
TBI

*P.S. Good ideas in this report are plagiarized. Bad takes are my own.*

*Also: You are an adult. (I think.) None of this is investment advice. To the extent we have conflicts of interest with respect to any of the assets or companies referenced in this report, we do our best to note them. You can see a full list of teams we work with on our registry initiative (a paid membership) [here](#), and a list of our team's investment holdings can be found [here](#).*

*\*Eat meat.*

# What's In This Beast

A discerning reader may notice I've changed the format of this year's report slightly from prior editions. As we're on the cusp of a new crypto bull run, I wanted to create a sensible narrative arc that cleanly introduces the industry to newcomers (leave no one behind!), while still sharing more inside baseball than a typical year-in-review post. This report serves as my lattice for the year ahead, and I hope it helps you map the market as well.

We start with crypto's top 10 trends (1) and people to watch (2). If you just want to read the intro and the report's punchlines, that's cool. If you'd like to complement that by keeping tabs on the ten folks highlighted in the second section, even better; you'll learn via osmosis throughout the year, and can come back to this report as needed.

Most of the remainder of the report is about other investable themes across the industry.

**(But again, not investment advice!)**

I start with a breakdown of my high-level investment framework (3), and what I think about real vs. relative valuation models for crypto. Then Bitcoin gets its own chapter (4) as the industry's most important asset, and Ethereum gets one (5) as the industry's most important platform. I cover the investment case for both assets, their technical roadmaps, and the opportunities and challenges these networks will face in the year ahead, while addressing their competitors towards the end of the sections. It doesn't make sense to think about Litecoin independently of Bitcoin or to think about a newly launched smart contract platform without Ethereum in mind.

Next, we go deeper by theme, starting with an overview of DeFi's top ten 0-to-1 innovations (6). If you're used to investing in equities only, or haven't made it past bitcoin as a crypto investment, it's impossible to weigh the merits of decentralized network assets without that primer. With the DeFi stage set, we work through four central themes in which centralized and decentralized services are competing for primacy: stablecoins (7), synthetic assets (8), credit markets (9), and infrastructure (10).

Finally, we wrap up with some of the more futuristic elements of the industry: Web3 applications like digital resource provisioning (file storage, video transcoding, IoT bandwidth), and various types of non-fungible tokens ("NFTs"). These assets may get ahead of themselves in 2021, but that doesn't change our conviction that they will be incredibly big by 2025 (11). We put policy in the final section (12) as both a warning flag on the rest of the report, and as a teaser of the idea I'm most infatuated with right now: how crypto technologies can help us disrupt nation-states themselves.

The '20s are going to be wild.

# Table of Contents

## 1. Top 10 Trends We're Following

*Narratives over fundamentals.*

- “Blue Chips”: Real vs. Relative Value
- Bitcoin: Brrr Money and Digital Gold (BTC)
- Ethereum: The Everything Marketplace
- DeFi: A Bankless Future
- Stablecoins: Eating the (Crypto) World
- Crypto Credit: Locking In Value
- Synthetics: All About Accessibility
- Infrastructure: Crypto Exchange Unbundling
- Web3 & NFTs: The Digital Resource Economy
- The Final Boss & The Network State

## 2. Top 10 People to Watch

*Same, same, but different.*

- Sam Bankman-Fried
- Michael Saylor
- Barry Silbert
- Balaji Srinivasan
- Brian Brooks
- Caitlin Long
- Andre Cronje
- Hayden Adams & Rob Leshner
- Anonymous
- Danny Ryan
- Honorable Mentions

## 3. Top 10 Investment Themes: Real vs. Relative Value

*Do you wanna be right, or do you wanna make money?*

- Stablecoins as Stimulants
- Passive Aggressive
- APE ME: Tracking Crypto Fund Manager Portfolios
- Directional Correctness (Build AND Go Long)
- Traditional VCs Behind the Eightball
- The Crypto IPO Calendar
- The Non-IPO Calendar: DCG
- Top M&A Targets
- Work to Earn: Fund, Vote, Build
- Assets We Like (HODL)

## 7. 4. Bitcoin: Brrr Money and Digital Gold (BTC)

*Memetic, programmable gold.*

- 7 Bitcoin Bull/Bear Elevator Pitch
- 8 The Case for Bitcoin: Your New Bitcoin Library
- 10 The Prism: Bitcoin Personas
- 11 Demand > Supply for Crypto Custody
- 11 Demand > Supply for Countries
- 12 Fungibility & Surveillance
- 13 Taproot & Schnorr
- 13 Lightning & Sidechains
- 14 Miner Diversification and Predictability
- 15 Litecoin, Bitcoin Forks, and Toxic Waste (XRP/XLM)
- 15 Zcash: Trojan Horses, Hypermodels, and True Privacy

## 16

## 5. Ethereum: The Parallel Financial System

*The asset and the upgrade.*

- 17 ETH is Not Money
- 18 ETH as a Defensive Asset
- 18 eth2: PoS, Sharding, and a Beacon (Chain)
- 19 Actually ETH 1.5: Rollups, PoS
- 19 Beacon ETH
- 20 ETH Farming Rewards
- 20 Minimum Viable Security Spend Settlement
- 20 Layer 1 Redundancies
- 21 Layer 1 Specialization
- 21 The Philosopher Kings

## 22 6. DeFi: Money Legos

*About participatory financial markets.*

- 23 Maker's Fully Collateralized, On-Chain Bank
- 24 Uniswap's Secure Exchange
- 25 The Liquidity Mining Spark
- 26 Dynamic Automated Market Makers
- 26 Smart Vaults
- 27 Unsecured Credit & Flash Loans
- 27 Crypto's Data Middleware: Oracles
- 29 Vampire Attacks: Legal Theft
- 29 Treasury Governors
- 29 DeFi Bug Bounties

# Table of Contents

## 7. Stablecoins: Eating the Crypto World

*A \$20 billion explosion.*

USDT: Crypto's Biggest Threat

USDC: The Multichain Stablecoin

PAX: The PayPal Stablecoin?

Dai

aDai or cDai or yDai

yUSD: Smart Dollars

Ampleforth & Yams

Libra

Celo, Terra, Reserve

CBDCs

## 8. Crypto Credit 2021: Leverage Is a Helluva Drug

*Never go short (with special guest CMS Holdings)*

Record CME Growth

Credit Wealth Effects

Lender Economics

Basis Trading: Cash-Collateralization In.  
Coin-Collateralization Out.

Arbitrage & Boring Ass Delta Neutral Trading

Grayscale Collateral Risks

BitMEX Rekt Funds

DeFi is the Tail Wagging the Dog

So Many Options

DeFi's Yield Curve

## 9. Synthetic Assets: All About Accessibility

*The race to marketability.*

The Grayscale Trade

Crypto ETF(s) Approval

Yearn Strategy

Play Safe and Wrap It Up

I Predict Prediction Markets

Synthetic Stocks

Exchange Securities Tokens

On-Chain Indices

DAOs: FOMO in & Ragequit

Bonding Curves and the IDOs of March

## 10. Infrastructure: Crypto Exchange Unbundling

*Powerful, but not invincible.*

73 Exchange Aggregation Theory: The Case for Bundling 102

74 Exchanges Unbundled: CEX vs AMM for Retail 105

75 Exchanges Unbundled: Prime Brokerage 106

75 Exchanges Unbundled: Qualified Custody 106

77 Exchanges Unbundled: Web3 Wallets as Sovereign Banks 107

78 Quants: A Company for Every Metric 107

80 Educators: News, Research, Marketing 108

81 Governance Tools 108

81 Blockchain Monitoring 109

82 Messari: A Bloomberg for Crypto 110

## 11. Web3 & NFTs: The Digital Resource Economy

*Purely virtual marketplaces.*

83 Filecoin, IPFS, and the Uncensorable Web 112

84 Other Decentralized Hardware Networks 113

85 Content Scoring: Reddit, Twitter, and New Entrants 114

Citizen Journalism & Convexity 115

86 NFT 101 115

86 There's Always Money in the (Digital) Banana Stand 117

87 Social Money & Community Tokens 118

87 VR Interior Design 121

88 VR Interior Desire (Sex, Fear, Greed) 122

88 Data Marketplaces & Gravity 123

## 12. The Final Boss: Exiting to the Network State

*Crypto policy and self-sovereignty.*

90 Money as Bookkeeping 125

92 Western Bias & Chinese Fear 126

93 A Western Temperature Check 127

95 The Enemy at the Gates: FATF 128

97 Swiss Banking in Your Pocket 129

97 Bitcoin Banking 130

98 Illegalizing Participation 130

98 It's Good to Be Well-EnDAO'd 131

99 The Network State 132

100 Conclusion 133



# Try the new Messari.io

- Custom watchlists
- Fast, comprehensive data
- Built for the pros

## Go Pro for 20% off

Access our industry leading  
research and Pro data tools

USE OFFER CODE **THESES2021**

[Start Your Free Trial](#)

The screenshot displays the Messari.io platform interface. At the top, there's a navigation bar with links for Watchlists, Chart, Screener, Feed, and Intel. A search bar on the right says "Search the Messari database". Below the navigation is a "WATCHLISTS" section where users can add assets to their watchlist. The current list includes Bitcoin, Ethereum, Polkadot, Cosmos, Uniswap, yearn.finance, Zcash, and Synthetix. The "CHART" section shows the price of Bitcoin at \$18,870.15. The "VOLUME" section lists the top assets by volume, including Tether, Bitcoin, Ethereum, XRP, Binance USD, Litecoin, Chainlink, yearn.finance, Cardano, Stellar, USD Coin, SushiSwap, Bitcoin Cash, EOS, BNB, and others. The "FUNDAMENTALS" section shows the current market cap for Bitcoin as \$350.77B. The bottom of the screen features a smartphone displaying the mobile version of the Messari app, which also shows a chart for Ethereum.

# 1.0

## Top 10 Trends We're Following

Crypto investing has always been about buying into compelling narratives vs. "fundamentals," and that's unlikely to change any time soon.

The good news is there has never been a better narrative environment for crypto than today's AND there might even be some compelling "**fundamentals**" to back up the noise. I'm mega-bullish on what lies ahead in 2021. Optimism is not out of consensus, but maybe the magnitude of my bullishness is: this next bull cycle will be "the big one," and I think we'll hit \$100k/BTC at least before the end of 2021, with crypto hitting \$3 trillion in cumulative network value in this cycle's top.

Here are the top ten narratives I believe will drive that rally. In fact, consider these evergreen trends for the entire decade.

---

### 1.1 “Blue Chips”: Real vs. Relative Value

The most maddening part of the 2017 ICO craze was how **infatuated** so many smart people became with the idea that dozens of crypto **currencies** could ultimately emerge as viable investments. It seemed like complete nonsense that so many tokens would earn lucrative monetary premiums, and we argued from day one that "money" was a winner-take-most market where even the also-rans would need to offer differentiating features to win market share in the long-tail. On the other hand, "utility" tokens would either find a way to capture network fees or **fade to irrelevance** as cash generating network assets took their place.

That thesis has held up, and it's become easier to think about assets on both a relative- and fundamentals-driven basis now that we're seeing actual usage. The lines are blurry, but we generally think about crypto in six categories: monies (mostly proof-of-work currencies like BTC), smart contract platform tokens (ETH and friends), crypto dollars (stablecoins), DeFi's "cooperative" tokens, pegged & synthetic assets, and Web3/NFT assets.

If you compare bitcoin to other proof-of-work currencies, its [market dominance](#) is ~90%. If you compare ETH to other platform tokens, its dominance is closer to 70%. There may be a large “ETH is Money” crowd, but I personally don’t think of pureplay currencies like BTC the same way I think about platform tokens like ETH (more on that truth bomb later). For stablecoins, market “dominance” may not inform VC bets, but it could help you monitor systemic risk to know Tether still represents 75% of the dollar-pegged market.

The assets within DeFi and Web3/NFTs and Synthetics have more bespoke value drivers.

This makes sense! Those asset valuations can be derived from the underlying fees their marketplaces generate or the “real” digital or financial assets they represent. And even though most crypto assets are correlated, we’ve begun to see clear performance separation over time between sectors and assets with real economic models.

Sector segregation isn’t just an exercise in relative valuation analysis; it helps us identify sector-specific KPIs. We may care about inflation rates and on-chain liquidity for currencies; staking yield and network fees for platform tokens; and adjusted / fee-driven yields on DeFi network tokens. We’re still figuring out what matters for the whole lot, and it might take a long time to agree on crypto’s novel capital asset pricing models. Still, for a change, it’s helpful to know [Uniswap](#)’s native token trades at 10x its annualized network fees, while its centralized exchange counterparts trade off of implied business earnings.

This is progress! And it informs much of the analysis in the rest of this report.

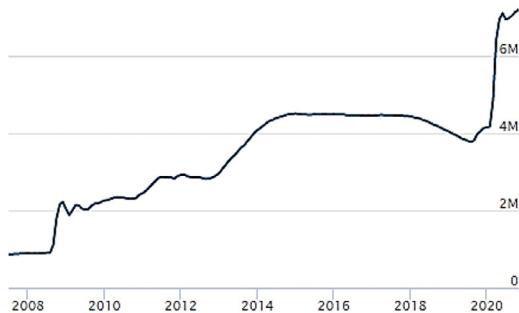
## 1.2 Bitcoin: Brrr Money and Digital Gold (BTC)

We’ll look back on 2020 as equal parts aberration and accelerant. Amidst the chaos of coronavirus (temporary) and the subsequent lockdowns (temporary), we had the real story for bitcoin: central banks [added trillions](#) of dollars to their balance sheets, monetized sovereign debt at record levels, and drove real yields negative for [record levels of debt](#) (permanent effect).

Currencies				
Mcap: \$410.88B	ROI: +167.34%	BTC dominance: 88.35%		
#	NAME	PRICE	MCAP	1Y
1	Bitcoin	\$19,582.43	\$363.02B	+169.38%
2	XRP	\$0.657	\$22.42B	+199.60%
3	Bitcoin Cash	\$313.11	\$6.00B	+46.81%
4	Litecoin	\$89.08	\$5.89B	+98.30%
5	Bitcoin SV	\$181.21	\$3.36B	+82.16%
6	Stellar	\$0.198	\$3.34B	+256.58%
7	Monero	\$129.68	\$2.30B	+139.91%
8	Dash	\$113.20	\$1.10B	+115.89%
9	Zcash	\$80.35	\$0.84B	+191.86%
10	Dogecoin	\$0.00356	\$0.45B	+61.14%

### Explosion of Central Bank Balance Sheet

Total Assets of the Federal Reserve: \$7.2 trillion



Source: Federal Reserve  
Note: As of November 24, 2020

### Negative Yielding Debt at ATH

Global Negative-Yielding Debt Market Value (US\$ trillion)



Source: Bloomberg, The Daily Shot  
Note: As of November 8, 2020

In short, Modern Monetary Theory (the belief that state capacity for deficit spending and debt monetization is essentially unlimited) was not only normalized, it became policy in 2020. The powers-that-be aren't even feigning spending restraint anymore, and a divided government in the U.S. might be the only governor on a spending golf cart that's careening downhill.

If Democrats [sweep the runoff elections](#) in Georgia this January, it will improve the prospects of an unchecked [fiscal stimulus package](#) and add more fuel to the speculative fire around bitcoin and other financial and hard assets. If Congress remains split, the money printer will continue to go brrr. Please [watch this video](#) to understand how this works.

What's different today from several years ago is bitcoin's prominence in the macro conversation, and its emergence as a smart money alternative to gold.

- Paul Tudor Jones called it "[the fastest horse](#)";
- Stanley Druckenmiller said "[the bitcoin bet will probably work better](#)" than gold;
- Chamath Palihapitiya thinks "[everyone should have 1% of their assets in bitcoin](#)";
- Bill Miller "[strongly recommended](#)" investors get exposure if they didn't yet own bitcoin;
- JPMorgan wrote that family offices "[may be looking at bitcoin as an alternative to gold](#)";
- Raoul Pal says "[Bitcoin is a supermassive black hole](#)"

It's not about capital inflows from any one of these particular investors. It's about the smoke.

The world's top institutional money managers have finally taken [public positions](#) that make it socially acceptable for their colleagues to jump into the fray and buy BTC, the gateway drug

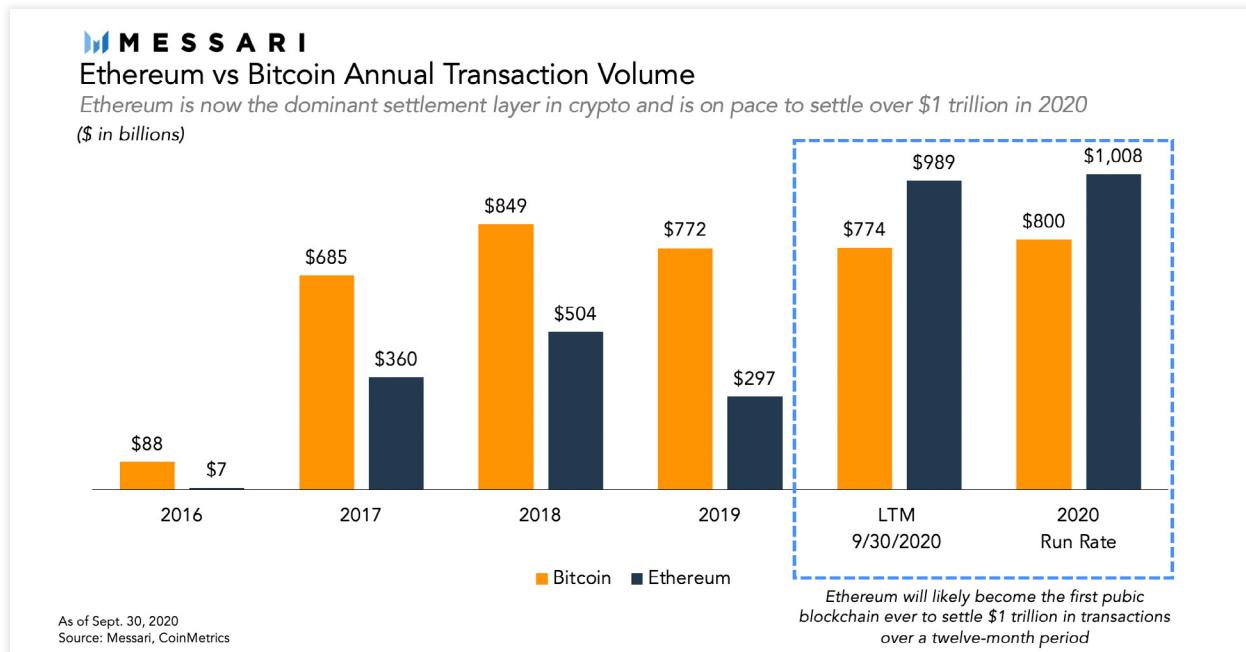
to the rest of crypto. By eliminating the career risk associated with crypto investing, they've opened the institutional allocator floodgates for 2021, just as Marc Andreessen (a16z) and Fred Wilson (USV) did for venture capital in 2013.

If you stop reading here, follow the leader, and allocate some of your portfolio to BTC, you'll probably have a prosperous new year.

### 1.3 Ethereum: The Everything Marketplace

It's hard to believe how many novel financial services and applications found product-market fit this year thanks to [Ethereum](#). Some cynics have dismissed the new projects as bubbles or toys (or both), but I'd venture to guess few of them have ever actually tested these products.

They're real, and they're spectacular.



There is so much to cover in the Ethereum (and broader smart contract) space that you'll find notes about Ethereum-based applications sprawled across almost every section in this report. Bitcoin may be primed for a big year due to its macro positioning, but it's Ethereum that has taken flight as crypto's most important platform...one that could power an entirely new financial system, and a more open, resilient internet.

Ethereum may have even taken a permanent lead this year versus Bitcoin in terms of [economic value](#) transferred on its rails.

It's hard to ignore five-year-old technologies that process more than \$1 trillion in real value transfers per year, a figure that has already eclipsed PayPal's. Ethereum has [challenges ahead](#), but its dynamism is undeniable, and it will continue to be the platform to watch in 2021.

## 1.4 DeFi: A Bankless Future

Say you want to create an entirely new financial system from scratch: payments, lending, insurance, asset issuance and exchange, the works.

The first thing that you're going to realize is that it takes a helluva lot of work to go from today's FDIC-insured financial system and etrade accounts to a crypto equivalent. Yet over the course of this year, crypto spawned the building blocks to do just that.

A parallel financial system first requires a synthetic dollar; the creation and management of that asset requires basic lending facilities and reference data infrastructure to maintain the asset's peg; scaling up and getting rates and spreads competitive with centralized solutions requires hefty incentives for capital providers; if you figure out how these markets can work, you'll have to contend with the lack of circuit breakers and chargebacks; you'll have to protect deposits from "bank runs" and hacks; you'll need savvy risk managers setting the protocol defaults, defenses to prevent application-draining attacks, and low cost insurance against technical errors.

Doesn't that sound fun?

Well, with Maker (crypto dollars), Uniswap (automated market making), Compound (liquidity mining), Balancer (dynamic liquidity pool rebalancing), YFI (smart asset management), Aave (flash loans), ChainLink (data oracles), SushiSwap (defensive countermeasures), CVP (proxy aggregation), and bZx (decentralized bug bounty protocol), we've got examples of the building blocks needed to power a fully decentralized and algorithmic financial system. (More on all of these later in the report.)

DeFi is justifiably hyped. The only thing I see slowing down the sector's momentum would be precedent-setting (and maybe logic-bending) **regulatory crackdowns** of top market projects.

I'm not betting on the regulators, though.

ADVERTISEMENT

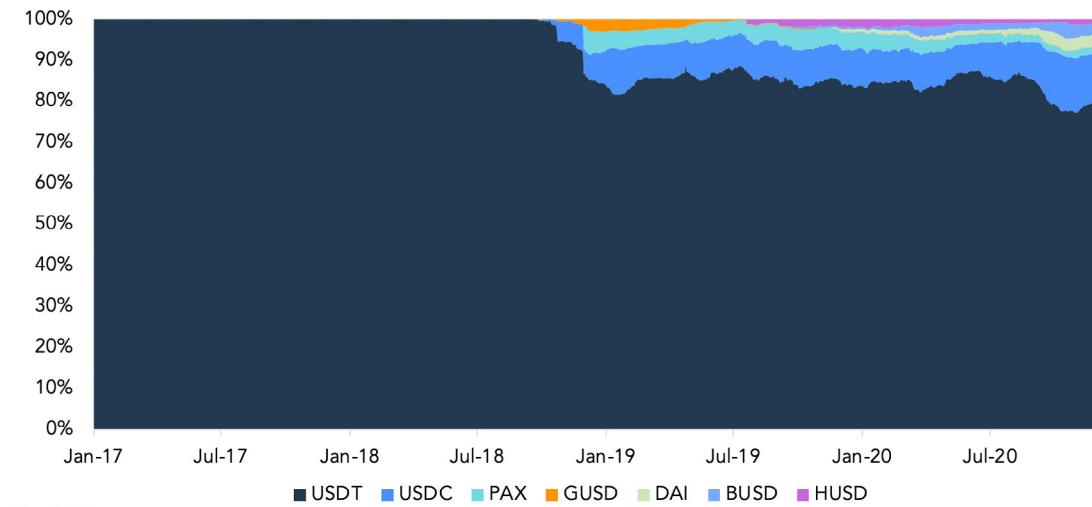
**Your Crypto Goals Are Our Goals** [JOIN 4 MILLION CUSTOMERS](#) **Bitstamp**

## 1.5 Stablecoins: Eating the (Crypto) World

Sometimes numbers speak for themselves. Stablecoins have absolutely exploded in size and usage this year. More than **\$20 billion** of supply facilitates hundreds of billions of dollars of transaction flow through "crypto dollars" today. The U.S. dollar is, ironically, still the reserve currency of crypto, a trend that shows no signs of abating as more crypto dollar applications come online, and countries introduce their own central-bank digital currency initiatives.

## Stablecoin Market Share by Market Capitalization

*Tether is still king even after a wave of competition came online in recent years*



As of Dec. 3, 2020

Source: CoinMetrics

Despite concern regarding potential seizures (not to mention the current reserve [status](#)) of [Tether](#), the leading stablecoin continues to grow and dominate its segment (and most international crypto exchange settlements). This year's explosion in DeFi likely doesn't happen without the proliferation of stablecoins, and with \$11 billion of USDT on Ethereum, Tether is second to just ETH itself in terms of economic value stored on the Ethereum blockchain.

Bitcoin will remain the most valuable digital currency, crypto or dollarized, indefinitely, but the same isn't necessarily true for Ethereum and its ilk. Crypto dollars on crypto platforms and Central Bank Digital Currencies (CBDCs) on state platforms will overtake platform tokens in circulating float in 2-3 years. What that means for smart contract platform security remains unclear for now.

## 1.6 Crypto Credit: Locking In Value

The biggest boon for crypto in the past year has been the explosion of crypto credit markets. Centralized, retail-facing services like BlockFi; institutional lenders like Genesis, BitGo, and Galaxy; and DeFi lending protocols like Compound, Aave, and Maker, all had banner years, and helped bring greater liquidity and stability (long-term!) to the hyper-volatile crypto markets. At the same time, they helped drive usage of new applications that require stable base currencies, tighter trading spreads, and fewer inter-platform price dislocations.

Most importantly, credit kept assets locked in the crypto economy, and away from the taxman.

In the past, if you had a major expenditure like a down payment for a new home or a student debt repayment, and you wanted to fund that payment with crypto gains, you'd take a massive capital gains tax hit and miss out on upside for the underlying portfolio. Today, things are different. It's reasonable (if not smart) to take on over-collateralized loans with healthy margins of safety to pay for one-time expenses like a new home.

The availability of on-chain collateralized credit in both **DeFi** and centralized services could seriously reduce selling pressure in the next uptrending market. That's true for both retail and institutional investors alike. A shock that sparks cascading liquidations is always a doomsday scenario, but that seems like more of a risk later in the cycle than early on. It's more likely the crypto credit market's maturation makes this the most liquid bull run yet.

## 1.7 Synthetics: All About Accessibility

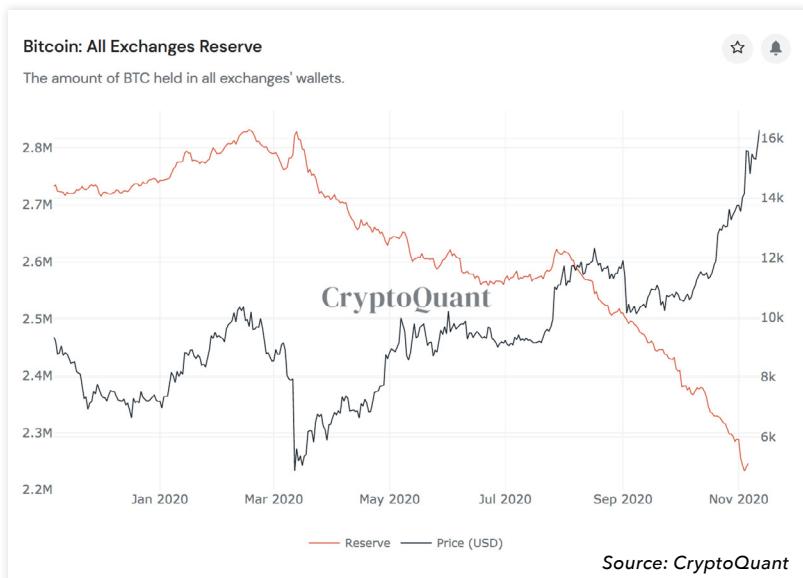
The Grayscale Trade. The Bitcoin ETF. A Wealthfront for DeFi. Wrapped Assets. Prediction Markets. Digital Stonks. Crypto Exchange "Securities." On-Chain Index Funds. DAOs. Programmable Financial Assets.

Every single financial asset that you can think of will one day be tied to crypto, and synthetics demonstrate how this transition could take place sooner than we appreciate. I don't want to spoil this section up front, but if you were in the "blockchain not bitcoin" camp, this is the purple pill section that will get boomer readers most excited.

## 1.8 Infrastructure: Crypto Exchange Unbundling

Exchanges are the 800-pound gorillas in crypto. They make all the money, they touch all the users, and they have their fingers in everything. Trading (duh). Custody. Lending. Staking. Research and Data. Governance. Venture. It almost makes you wonder how "decentralized" the crypto economy really is.

But users have more power than first meets the eye. There may be switching costs to moving funds out of the mighty exchanges, but it's still common. And it's much easier than switching banks! Look no further than the rapid (and publicly visible) flights of capital from **BitMEX**, **OKEx**, and **Binance**



in recent months due to regulatory fears. Money [leaked from exchange](#) vaults in 2020 to qualified custodians, fund managers, and mobile wallets, while trading volumes migrated (modestly) from centralized exchanges to prime brokers and DeFi markets.

It highlights how the real long-term value in crypto “exchange” could actually be at the data, custody, and prime broker level. Crypto has begun to (very slowly) unbundle the trading giants as their spreads and fees tighten. Trusted interfaces to the broader crypto economy will continue to matter even more than deep order books and 100x leverage casinos.

Just ask Poloniex and Bittrex.

Oh, and if the CCP can inadvertently cause [OKEx to pause withdrawals](#), and the DoJ can cause a [50% drop in customer deposits at BitMEX](#), and a Forbes article can spook Binance into [filing a flailing defamation lawsuit](#), is it so hard to doubt the inevitability of mega-exchanges as crypto’s entrenched bundlers?

We’ll keep an eye on exchange deposits as a percentage of the overall crypto market cap as a sign of their waxing or waning dominance.

Don’t get me wrong, I’m not betting against them. On the contrary, I’m expecting they get even more aggressive about inorganic expansion as their revenue mix rotates beyond trading fees.

## 1.9 Web3 & NFTs: The Digital Resource Economy

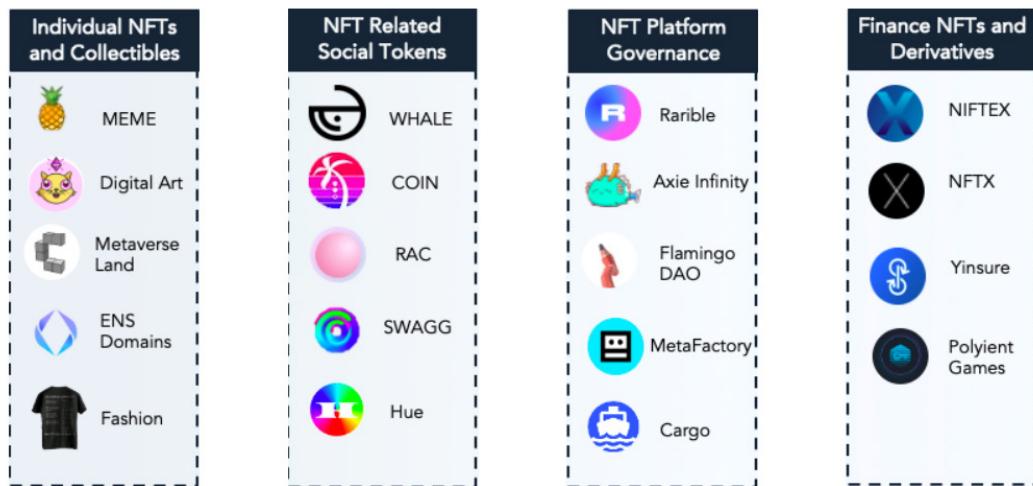
This fall, we finally got the long-awaited launch of decentralized storage network Filecoin, despite some last minute legal hiccups, and [some early token economics issues](#). Other storage solutions (Sia, Storj, Arweave) have also rallied since, as have decentralized networking tools like Orchid (VPNs), Livepeer (video transcoding), and Helium (IoT device networks). These decentralized hardware markets are arguably the most important infrastructure networks we need to ensure the web remains open in the years to come.

It’s about more than just money and DeFi. Web3 platforms open the door to a universe of new digitally native assets like gaming goods and digital art in the VR metaverse; new content and data licenses and uncensorable DNS; and even uncensorable bridges to legacy asset markets like real estate titling and insurance.

I [buy the thesis](#) that “almost every type of NFT built to date is likely to get traction eventually” and that Web3 platforms open the door to that natively digital future. Bitcoin and the smart contract platforms are predominantly rails for the decentralized financial system, but Web3 networks and NFTs are the real critical building blocks of a more open internet.

## NFT Sector Investment Categories

Tokens by NFT category



As of Sept 28, 2020 • Source: Messari

## 1.10. The Final Boss: Exiting to the Network State

The authorities have mercifully left us alone for years thanks to bitcoin's volatility.

Every peak and valley market cycle has been a head fake: bitcoin crashes to lull the powers-that-be into a false sense of security—a sense that this passing fad is finally actually dead and not worth the mindshare to regulate. Far from something to fear as a potential threat to their monetary monopolies!

Crypto at \$500 billion of market capitalization and **trillions** of dollars of annual transactions is harder to ignore. Fortunately, larger investors, lobbying entities, and even regulators (and now **senators!**) have begun to work the system from the inside in the U.S. I've taken to calling them the Bitcoin Insurgency. While they work their magic in D.C. (and Brussels and Tokyo and other power centers around the globe), some of us will start thinking about the ultimate exit: how to rebuild a crypto-inspired nation-state.

Insane, you say?

More insane than a \$500 billion emergent economy launched by a pseudonymous founder on Halloween 12 years ago?

Boo.

# 2.0

## Top 10 People to Watch

Last year's top 10 didn't disappoint.

CZ's Binance stayed on top of the exchange world (for now), and beefed up its marketing funnel with the [mammoth acquisition](#) of CoinMarketCap. Jack's one company censored #fakenews from the President, while his other company accelerated its bitcoin support, introducing bitcoin to record new users, sponsoring Core development, and even writing the [playbook](#) to help other companies add BTC to their balance sheets. Brian Klein had his hands full in the crypto legal realm, defending crypto evangelists from [alleged sanctions violations](#). Meltem's CoinShares joined the [three comma club](#) in crypto AUM. Brad Sherman remained an asshole, but one who may take a backseat to (slightly) less prickly colleagues in 2021. Libra's Diem's canary in the coal mine, Morgan Beller, [tapped out at Facebook](#), underscoring the project's slow progress in the face of significant regulatory headwinds. Rune's MakerDAO had a record year in many respects, but lagged its peers during DeFi's summer boom. Zooko got his funding (and halving) and major protocol upgrades; now he'll just have to ensure his life's work doesn't get outlawed. Justin Sun remained an unrivaled performance artist, and we learned he could star in both [comedies](#) and [dark dramas](#). And Peter McCormack is still [obsessed with me](#) (and bitcoin).

So who are the top players to watch this year?

Same, same, but different.





## 2.1 Sam Bankman-Fried

Sam Bankman-Fried is the kid in every page of the yearbook. This year, “SBF” launched new Solana-based decentralized exchange, Serum; [acquired](#) crypto portfolio tracker Blockfolio for \$150 million (the year’s second largest acquisition...behind CZ’s, of course); and invested in dozens of new DeFi projects via his trading firm Alameda Research. SBF and his team weren’t shy about backing some of DeFi’s more mercenary projects either, supporting Uniswap fork, [SushiSwap](#), and Compound fork, CREAM.

That’s to say nothing of SBF’s day job running the FTX crypto exchange.

There, volumes eclipsed \$250 billion (10x year-over-year), catapulting the exchange to the top ten by global volume. While FTX still trails established giants like Binance, Huobi, OKEx, and BitMEX, the gap is closing in part due to SBF’s willingness to push the envelope with levered instruments, prediction markets, and now [synthetic stock trading](#). And while his Asia-based competitors face challenges with the CCP or DoJ, SBF now has access to the White House: he was the [second-largest donor](#) to President-elect Biden’s campaign. Behind Michael Bloomberg.

## 2.2 Michael Saylor

The MicroStrategy CEO made waves this year not only for his public company’s bet-the-farm stake in swapping its cash treasury for bitcoin, but for his individual mega-purchases, and his unabashed embrace of crypto Twitter. Others may have been more thoughtful with their public investment thesis (looking at you, PTJ), and ultimately more impactful in helping other public CEOs make the case for similar allocations. But Saylor gets the nod here for going full degen cowboy and [evangelist](#), and because I’d expect this is merely the first nine-figure bet placed by a large corporate, not the last we’ll see this cycle. Since MicroStrategy yolo’d into BTC, their sleepy stock has added 2.5x in market cap for every dollar of BTC gains.

Saylor has become a must-follow on Twitter. He’s a meme machine. Bitcoin is “monetary energy,” “a monetary network,” a “monetary athlete,” even a dragon that will “eat the kingdom of gold.” But really, he’s all of us, trying to sound out bitcoin’s definition with new twists each and every day. My [favorite](#) so far? *“It is a bank in cyberspace, run by incorruptible software, offering a global, affordable, simple, & secure savings account to billions of people that don’t have the option or desire to run their own hedge fund.”* Nice.

## 2.3 Barry Silbert

There's a good chance Digital Currency Group passed Coinbase this year as the most valuable crypto enterprise in the U.S., even if it's much less likely to go public any time soon. (More later.)

DCG subsidiary Grayscale started its ascent up the S-curve, thanks to the de facto monopoly blessing the SEC bestowed on its side-door ETFs, vehicles with which other passive fund managers will find it impossible to compete, and which have now accumulated more than **\$10 billion in AUM**. At the same time, DCG prime broker Genesis, serves as an authorized participant for Grayscale products, and its lengthy history (and Bitlicense) gives the desk a reputational edge in the crowded OTC and lending markets, where it's seen **record quarterly growth** in spot, derivatives, and lending services every quarter this year.

CoinDesk gives DCG a marketing megaphone and events powerhouse for an unrivaled institutional marketing funnel; new subsidiaries, Foundry and Luno bring DCG capabilities in the staking and governance of major crypto networks, and better emerging markets penetration; and that's to say nothing of the company's \$1 billion+ liquid war chest of cash and crypto, or its 150-company seed investment **portfolio**. DCG is either crypto's Berkshire Hathaway or the eye of Sauron. Depends on your perspective.

## 2.4 Balaji Srinivasan

Balaji stepped away from his CTO role at Coinbase in 2019, but his impact this year was arguably more significant (within and outside of crypto) than it was in any year he spent full-time at a crypto company.

He started the year with a bang, launching crypto community and publication Nakamoto.com with a must-read post on Bitcoin as the **Flag of Technology**, and a killer 24-hour Telegram group conversation that quickly spiralled out of control because we can't have nice things. I was excited to see what Nakamoto had up its sleeve, then the real world got in the way, and Balaji shifted his attention to warning everyone about the coronavirus, where he was the **first mainstream voice** many of us in the U.S. heard sound the alarm on the coronavirus and the magnitude it might have across the globe. He also found time to regularly (**calmly, surgically**) eviscerate the media and woke culture warriors. His fingerprints seemed to be on Brian Armstrong's "**no politics**" policy at Coinbase, and Balaji's call for a rise in **citizen journalism** has resonated as media quality and consistency continued to decline in a frantic election year.

That's not why Balaji makes my list, though.

Instead, it's his new stealth project that I'm most excited about. Call it politics from first principles, a plan to build an actual, credible "Network State" in the cloud as an initial step towards bootstrapping a new country. This project scratches a **decade-long itch** for Balaji, who's been enthralled with the concept of "**exit**" for a while and believes we may actually finally have the tools and tailwinds to make new sovereign states (in a world fresh out of unclaimed territory and new dirt) a possibility.

## 2.5 Brian Brooks

Former Coinbase Chief Legal Officer Brian Brooks had a huge first year as **the new acting Comptroller** of the Currency at the OCC. (It also may be **his last**.) His interpretive letters over the summer could have positive ramifications for the industry for years to come if they manage to avoid new legislative reversals. Brooks **clarified** that regulated USD-pegged stablecoins could have their underlying deposits custodied by U.S. banks, and that banks could actually custody other forms of crypto themselves. Huge. And this fall, he went even further, proposing a rule that would forbid banks from discriminating against industries like adult entertainment and crypto. By asking banks to embrace “quantitative, risk-based standards” for supporting new clients he reset the default for gray market customers back to “not guilty.”

There are other key players to watch in D.C.’s “Bitcoin Insurgency.” Hester Peirce looks set to **remain at the SEC** for the foreseeable future, while Commissioner Jay Clayton is stepping down. The CFTC is set to lose one crypto proponent in Brian Quintenz, but **picked up another advocate** in new Chairman Heath Tarbert. Bitcoin-savvy Gary Gensler and Lael Brainard have inside tracks to key positions within the Biden administration, and are somewhat positive on crypto. And the Senate has its first public bitcoin holder in Wyoming’s Cynthia Lummis. Maybe two, if former Bakkt CEO Kelly Loeffler can retain her seat in Georgia’s runoff in January.

There’s something to be said for “**educating electeds**,” but the truth is that we’ve been starting behind the eightball **for years** without elected or appointed crypto proponents who have already been redpilled. My sense is that this next crypto cycle will include more informed (and invested) crypto allies than in the past. **Lummis may be particularly interesting** as her state has vested economic interests in crypto’s continued success via the various Wyoming blockchain initiatives. Speaking of which...

## 2.6 Caitlin Long

You don’t need a law degree to have a major policy impact on crypto, and you don’t need to be a big state to have a national policy impact. No one demonstrated that quite as much as Caitlin Long this past 18 months via her work in Wyoming. The former Morgan Stanley MD and serial crypto entrepreneur played the state regulatory arbitrage game to perfection, paving the way for a series of **crypto friendly pieces of legislation in Wyoming**, the country’s **first bitcoin-holding Senator**, and the approval of new deposit-taking, fully reserved crypto banks (“special purpose deposit institutions”) in Kraken Financial and **her new startup, Avanti**.

Long has been prescient in how she’s thought about U.S. crypto services with respect to Wall Street as well. I’ve been re-reading some of her earlier work on potential rehypothecation issues we could be in store for as the vampire squids enter the fray. Wall Street’s penchant for adding leverage to anything it touches could dampen prices and add risk to the underlying networks if left unchecked...eventually. “Will HODLers permit the leveraged-based financialization of cryptocurrencies?” is a **damn good question she asked** years ago. The answer will dictate whether Wall Street helps drive a mega-bull run, or kills the one it enters.

## 2.7 Andre Cronje

If Morgan Beller was last year's canary in the coal mine for mega-stablecoin project Libra, then Andre Cronje may be in the catbird seat in DeFi. He's relentless, and there's no one who better exemplifies the mania of this past summer than the OG who "tests in prod." That's not to say Andre plays fast and loose, and irresponsibly. On the contrary, his project Yearn.Finance may be the fastest growing financial network of all time, catapulting to a billion dollar network valuation (with real fees and value flows to support it!) in mere months, and showing no signs of slowing down with respect to new product releases, integrations, and even "[protocol M&A](#)."

I also have a soft spot for Andre because he regularly wants to quit the industry out of disgust.

**Feb:** "Building in DeFi sucks...It's expensive, the community is hostile, the users are entitled."

**August:** "Close to rage quitting again. So sick and tired of this space."

Yet we, I mean, he, can't quite quit crypto.

Instead, he continues to demonstrate just how far one developer can go in building valuable new applications in the iterative space of open finance, and he's operating on [another level](#) right now compared to his peer set. It's never been easier or more lucrative to contribute to open source crypto, but the products this year are a far cry from 2017 when the primary "innovations" were securities law violations that promised a fraction of what Andre has actually delivered.

## 2.8 Hayden Adams & Rob Leshner

Maker may have been the critical building block that laid the foundation for DeFi's credit markets, stablecoin markets, and ultimately, this year's DeFi bull run. But it was Uniswap's automated market maker, and Compound's "liquidity mining" schemes that took DeFi from 30 to 100 mph this year. Hayden Adams (Uniswap) and Rob Leshner (Compound) have been wayyy ahead of the curve with respect to security best practices, user-centered design, and stakeholder alignment. It's paid off bigly.

Uniswap, despite (because of?) a mammoth [giveaway](#) to its early supporters, did an equivalent amount of trading volume to Coinbase in September, and its token enjoys a valuation on par with Kraken's last private valuation, mere months after its token launch. Likewise, Compound's money markets protocol [accumulated billions in locked collateral](#), and its governance token reached unicorn status, too. (More on both projects later.) These two entrepreneurs look poised to lead the way in 2021 as well; they've thus far kept aggressive rivals at bay. They (and Andre) seem like the most likely DeFi leaders to answer the UNEASY question: "how can you build moats around open-source financial markets?"

## 2.9 Anonymous

Last year, it was Justin Sun's fork and tokenization bonanza that made me reach for my popcorn. This year, it's vampire attacks, food token forks, and rug pulls. If you're a normal human with

a respectable career and that sentence makes no sense, you're better than me. But anon/pseudonymous contributors have had a YEAR in DeFi, shilling new tokens for million dollar pay days ([Blue Kirby](#)), stealing valor (and liquidity) from the teams in the trenches ([Chef Nomi](#), [0xc4ad](#)) for even bigger pay days, and simply absconding with user funds when they're not even feeling creative (too many "Pool 2" liquidations to even link out to here).

If you want a taste for this summer's shenanigans, you can [read our account](#) of SushiSwap. Otherwise, you can save some time by merely appreciating that in 2020, pseudonyms became cool again. Even bitcoin luminaries like Erik Voorhees wish they could relaunch their projects fully anonymously.

Anon wasn't all negative either. DeFi Twitter has some excellent pseudo producers like "[DegenSpartan](#)" and "[CeterisParibus](#)." Square now employs lightning developer "[ZmnSCPxj](#)," and Paradigm poached top DeFi security research (and perpetual DeFi savior) "[samczsun](#)" to its A+ team. And let's not forget the industry's two biggest M&A winners to date, the founders of Poloniex and CoinMarketCap, who have remained largely unknown despite \$400 million pay days that, reinvested in crypto, could very well make them two of the world's most under-the-radar billionaires.

It's better to be rich and anonymous than poor and famous. I mean, just look at me.

## 2.10 Danny Ryan

Vitalik may be the face of Ethereum, but it's Ethereum Foundation researcher Danny Ryan who has become [the face of this year's mammoth eth2 upgrade](#). From coordinating research across technical teams, to [outlining updates for the community at large](#), to [fielding countless interviews](#), and finally submitting [the official EIP for the eth2 network upgrade](#), Ryan has been at the heart of arguably the most complex and critical network upgrade in crypto's history. There isn't much more to say than that, and it's worth keeping your eyes and ears open whenever he speaks about eth2's progress in 2021.

## Honorable Mentions

Pomp had a monster year with massive audience growth across his podcast network, YouTube channel, [Substack newsletter](#), and of course Twitter, but he gets honorable mention status once again to keep his ego in check. (Hi, Pomp!) The chats he had with [Chamath](#), Mark Cuban, and Raoul Pal are must-listens.... Everyone recruits "world-class talent" to their teams, but Paradigm's team truly is loaded. I called out Samczsun up top, but there was [a great profile in Forbes](#) on the whole enterprise.... CMS Holdings and Three Arrows Capital would rather make money than be right, and they captured the DeFi zeitgeist better than anyone else on Twitter.... Kraken's Jesse Powell [started a bank](#), which is interesting, and Jerome Powell saved the economy and ignited the bitcoin mega-bull macro narrative better than anyone else could have. [BRRR](#).

# 3.0

## Top 10 Investment Themes: Real vs. Relative Value

Is it me, or do the top 50 cryptoassets right now, seem... sensible?

At the height of the blow-off top in late 2017 and early 2018, everything was overvalued, and most assets didn't even seem to have a clear purpose. Today, half of the top ten proof-of-work based "crypto monies" may be write-offs, but bitcoin accounts for ~90% of their value with some interesting, privacy-focused complements competing for the scraps. There are eight stablecoins worth \$250 million or more to make up for the fact that the Lindy effect-protected "private money" networks like XRP and XLM persist in the top ten despite their inanity.

There are a dozen or so smart contract platforms vying for market share in today's top 50. Most generate network cash flows (in theory, at least) as investors secure transactions by staking deposits to their chains, and earning gas fees and seigniorage. Is there room for multiple winners here? Not even core Ethereum developers believe the eth2 base blockchain will settle 100% of transactions in the future, so you can understand why ETH's dominance in its sector is just 70%. Which other Layer 1 or Layer 2 network tokens stand to benefit from the explosion of crypto applications? Are they investable, too?

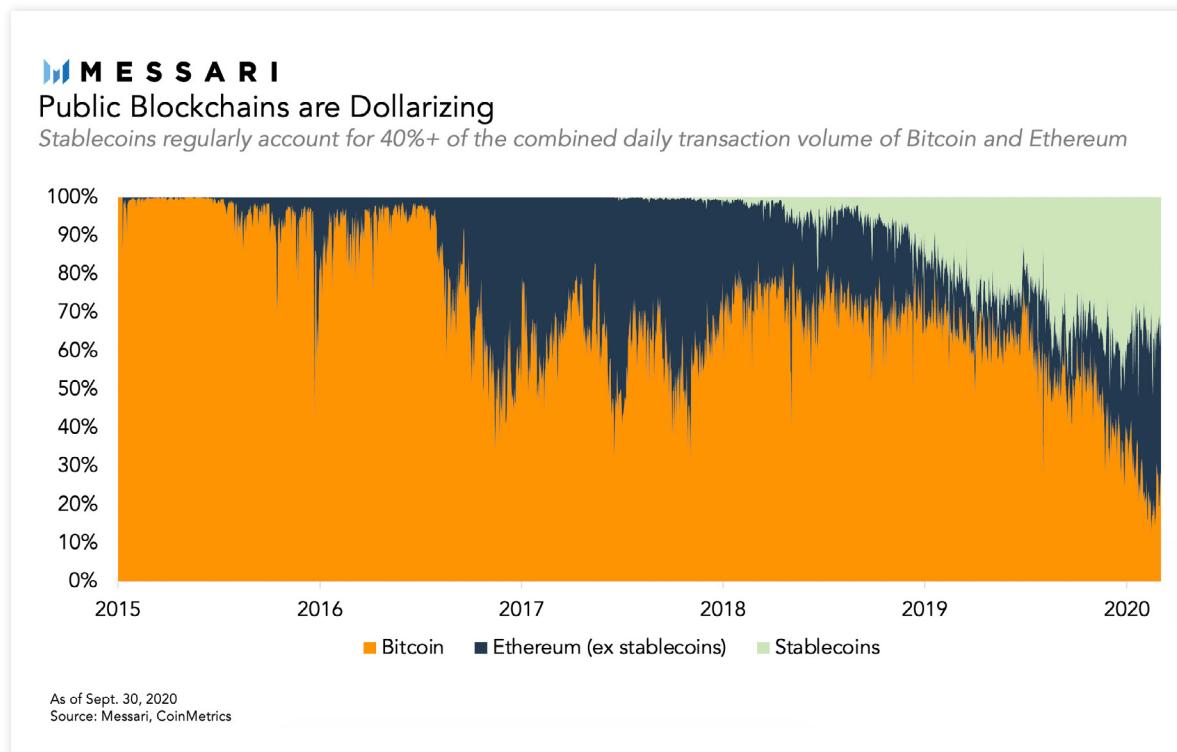
Even if you think you have the answer to these questions, can you outperform BTC and ETH net of gas, taxes, accounting fees, and the value of your time?

Perhaps. But most of your outperformance will likely come from insider status (the rich get richer); from your engineering prowess (you know the rules to the game better than others, and play lucrative, but extremely competitive on-chain sports); or from your big, high-conviction, out-of-consensus bets that an asset you like is fundamentally misunderstood by a lot of other smart people. That's hard by definition.

There's a lot of nuance to crypto investing, and the complexity increases daily. If you can swing it, the best way to place crypto bets is still probably through a crypto fund or funds. Whether that's a passive manager like Grayscale or an active investor like Paradigm doesn't matter. It merely depends on whether you believe the fund can beat the bitcoin benchmark, and whether you can access the fund manager. Both passive and active investors (except for those who blew up from reckless leveraged positions) had banner years, and show no signs of slowing down. It's hard to beat the blue chips, but it's even harder to beat the whales.

### 3.1 Stablecoins as Stimulants

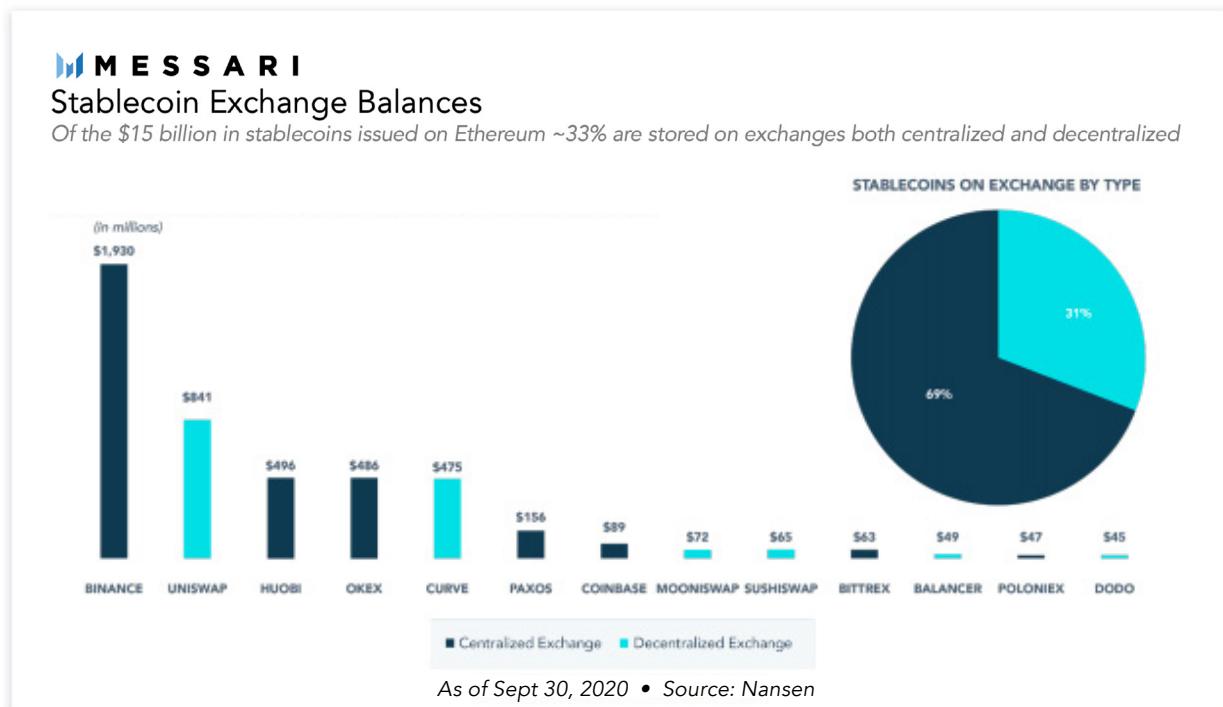
One of the most bullish aspects to this recent bull run is that it has resulted almost entirely from a winning macro narrative. BTC has thrived despite losing reserve status as an exchange quote currency since last cycle (stablecoins have taken its place); and ETH has survived despite losing its reserve status for ICOs and DeFi (again, thanks to stablecoins). It just so happens that both crypto commodities (BTC as digital gold and ETH as fuel for a new computing platform) hit major milestones that de-risked their investability from a store of value perspective.



With brief exceptions (March's Black Thursday liquidity crisis), BTC has remained an uncorrelated investment with a good sharpe ratio. Its recent halving slashed inflation below the Fed's target rate for the first time. Ethereum's inflation will be similarly slashed with

its eth2 migration, when value starts accruing to ETH holders: tens of millions of dollars in staking seigniorage and nearly as much burnt via transaction fees (gas). Other platforms may become worthy of institutional investor attention, but for now, it's still just a two horse race.

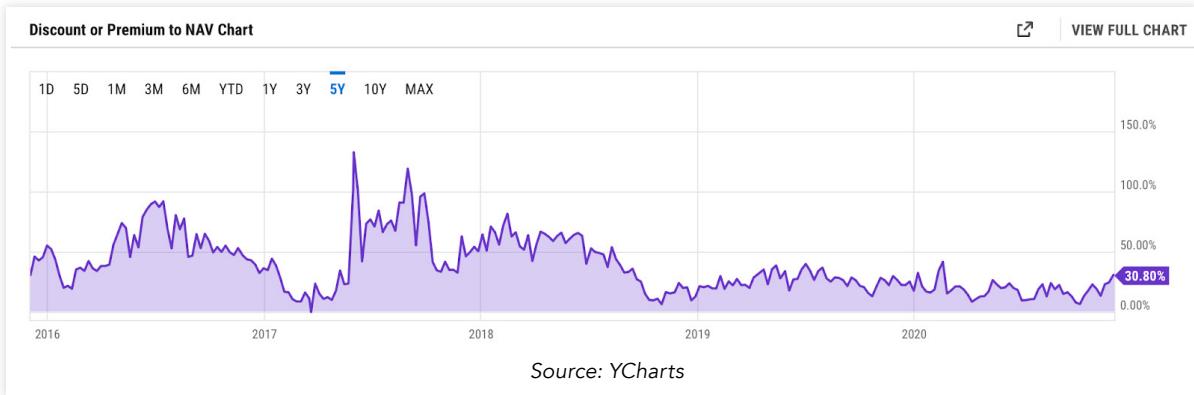
The rise of crypto dollars is, counterintuitively, just **one more potential catalyst** for the market this cycle. Stablecoins keep assets locked in the crypto ecosystem, as the flow of fiat tends to go one direction to take advantage of the persistently high interest rates and 10x improvements in crypto exchange settlement times. If the adverse scenarios played out (collateral deposits were seized or regulatory crackdowns killed stablecoin support), it would likely draw investors back to BTC and ETH as reserves.



## 3.2 Passive Aggressive

If you're an accredited investor, but you don't want to waste time diligencing crypto funds, or YOLOing into long-tail DeFi assets, your best bet may be to lever up into Grayscale trusts.

I'll walk through the mechanics later (**Section 9.1**), but if you're comfortable with a 6- to 12-month holding period, you can take risk in the underlying blue chip assets (BTC, ETH, LTC) and likely sell the shares later at a significant premium to spot. GBTC currently trades at a 30% **premium** to its net asset value, and hasn't traded at a discount to NAV in four years. ETHE trades at a whopping 60% premium, and has never traded at less than a 15% premium. LTCN trades at **multiples** of its underlying spot price. Even when premiums come down, they're unlikely to flip negative, so you can clip some coupons here while you get blue chip exposure.



### 3.3 APE ME: Tracking Crypto Fund Manager Portfolios

What's that? You're not accredited? One of the cool things about crypto is that it's possible to identify fund wallet addresses, track their flows, and follow on to their positions.

I'm sure firms will get better about privacy over time, but we've caught VC private placements in projects like Numerai, Arweave, and Synthetix wayyy before they were announced, simply by looking on-chain. We've [compiled liquid portfolio trackers](#) that match the disclosed positions of many top VC firms, so if you can't get an LP commitment into [a16z](#) or [USV](#); or a crypto hedge or venture funds like [Blockchain Capital](#), [Digital Currency Group](#), [Multicoin](#), [Pantera](#), [Polychain](#), [Placeholder](#) or [Paradigm](#), or an exchange fund like [Binance Labs](#), [Coinbase Ventures](#), and [Huobi](#), you can at least copy-paste their liquid portfolios!

#	ASSET	PRICE (USD)	CHANGE VS USD (24h)	REPORTED MARKETCAP	MARKETCAP DOMINANCE	REAL VOLUME (24h)	CHANGE (%)	CHANGE VS USD (30d)	CHANGE VS USD (90d)	CHANGE VS USD (YTD)	SECTOR	LIQUID SUPPLY
1	Bitcoin - BTC	\$19,371.96	+1.41%	\$359.53B	63.12%	\$2.99B	+12.72%	+38.12%	+85.80%	+168.59%	Currencies	18.56M
2	Ethereum - ETH	\$613.07	+2.92%	\$69.19B	12.15%	\$1.73B	+17.99%	+58.39%	+59.81%	+369.89%	Smart Contract Platforms	0.11B
3	Polkadot - DOT	\$5.46	-0.41%	\$4.84B	0.85%	\$65.57M	+13.68%	+35.86%	+7.56%	-98.33%	Smart Contract Platforms	1.01B
4	Tezos - XTZ	\$2.42	+1.23%	\$1.79B	0.31%	\$27.96M	+7.65%	+29.67%	-11.50%	+76.66%	Smart Contract Platforms	0.80B
5	Filecoin - FIL	\$30.57	+0.70%	\$1.36B	0.24%	\$26.10M	+2.10%	+5.94%	-29.88%	+399.45%	File Storage	--
6	Cosmos - ATOM	\$5.59	+1.99%	\$1.16B	0.2%	\$24.42M	+4.95%	+25.32%	+2.79%	+27.93%	Smart Contract Platforms	0.26B
7	yearn.finance - YFI	\$29,442.17	-4.66%	\$0.89B	0.16%	\$0.26B	+26.45%	+216.00%	+7.47%	+2594.76%	Asset Management	--
8	Maker - MKR	\$594.40	+5.82%	\$0.60B	0.1%	\$5.87M	+13.16%	+14.41%	+1.70%	+36.39%	Lending	1.00M
9	Compound - COMP	\$135.15	+23.19%	\$0.56B	0.1%	\$41.80M	+26.53%	+54.66%	-27.51%	-46.04%	Lending	4.39M
10	Zilliqa - ZIL	\$0.0329	+3.11%	\$0.35B	0.06%	\$25.15M	+27.67%	+89.86%	+99.25%	+629.70%	Smart Contract Platforms	14.15B
11	Ox - RXZ	\$0.431	-0.11%	\$0.32B	0.06%	\$6.80M	+6.01%	+32.93%	-15.61%	+136.75%	Decentralized Exchanges	0.98B
12	Celo - CELO	\$1.84	+1.06%	\$0.23B	0.04%	\$1.08M	+5.02%	+14.58%	-53.46%	+24.40%	Smart Contract Platforms	0.12B
13	Orchid - OXT	\$0.296	-0.12%	\$0.11B	0.02%	\$6.41M	+12.12%	+49.46%	-17.24%	-7.67%	Data Management	0.92B
14	Avalanche - AVAX	\$3.79	-0.33%	\$92.94M	0.02%	\$2.27M	+7.07%	+13.91%	-9.84%	-9.84%	Smart Contract Platforms	--
15	Nervos Network - CKB	\$0.00414	+3.67%	\$89.43M	0.02%	\$0.18M	+8.08%	+35.58%	-25.50%	-40.36%	Smart Contract Platforms	22.36B

Total: 15 assets

Not that I recommend doing that blindly. Many of these investors back projects pre-launch at 90% discounts to where they first trade, so their returns may be significantly higher than post exchange-traded asset performance suggests. I'd bet on top fund managers outperforming

BTC and ETH next year, even if we end up with a 5-10x “blue chip” rally. That’s a **big** reversal from my earlier days as a crypto fund skeptic, but that also means part of their alpha is your bag holding. (So be careful copy-pasting their positions for yourselves.)

### 3.4 Directional Correctness (Build AND Go Long)

One of the very worst pieces of advice I received when I started working in crypto full-time was that I shouldn’t collect a paycheck from a crypto company AND be heavily invested in the market’s underlying assets. Too much concentration, and no safety net. Luckily, I ignored that advice, and I assume (hope) other entrepreneurs will as well.

The reason is simple: the internet has generated trillions of dollars of wealth for entrepreneurs and innovators. Most of that value has been captured by startups that grow up to become big public companies (either through IPOs or acquisitions from the FAMGA). But rewards are highly concentrated, and thousands of other entrepreneurs, who also saw the value of the web and failed, did not properly participate in the upside. To become a successful tech entrepreneur or investor, you had to be right about both the market and the specific companies you backed. In crypto, on the other hand, you only need to be **right about the markets**.

The rest is all leveraged upside.

The democratization of rewards is what helps curious observers quit their jobs and build. It’s what helps failures move on to their next projects more seamlessly. And it’s what keeps the whole crypto tribe united and marching towards its larger end goals. You can sit on the sidelines, and make successful passive bets on some of the generation’s highest potential assets and markets, but it’s simply much more fun to join the fray.

### 3.5 Traditional VCs Behind the Eightball

The death of venture capital is generally exaggerated, but I doubt “traditional” VCs will tap much upside in the next cycle unless they’ve already been active (e.g., USV, a16z). For one thing, there is a serious wealth effect that ensures plenty of early crypto contributors can become seed capital contributors at the earliest stages of various community projects. Many of the most prestigious funds (Paradigm, Placeholder, Polychain, etc.) have industry reputations that meet or exceed those of legacy firms.

Crypto upstarts need hands-on stakeholders, and they usually aim to start with big syndicates of backers rather than sell 20% of their network to single lead investors. The “IPO at onset” mindset has been normalized for these sort of projects, which makes Series B+ firms somewhat anachronistic. Many traditional investors may find it easier to back crypto funds rather than invest directly themselves. The window is closing for them to capitalize on this particular cycle.

Few VCs understand this.

### 3.6 The Crypto IPO Calendar

In terms of crypto mega-IPO candidates in the U.S., there are four to keep an eye on, but perhaps the most interesting is also the least likely to actually file.

**Coinbase** shares have priced on secondary markets for \$7-12 billion. That makes sense given the giant's **most recent \$8 billion** raise during the last frothy market cycle, and the numerous competitive threats they've had to stare down since 2017. Coinbase has four advantages going into a potential listing: 1) It's a household name, and Coinbase has dominated due to its reputation for fraud prevention, secure custody, and good design; 2) The company's fee model has remained remarkably resilient, preserving the 1% transaction fee model in its core wallet onramp while splitting out its lower fee Pro exchange was a stroke of genius, and I'm not sure lower cost options like Square and PayPal will have much of a dent in Coinbase's retail dominance based on CB's brand; 3) Coinbase has become a major player in the custody game, and will generate significant revenue from that side of the business as staking becomes a novel and meaningful component of crypto ownership; and 4) The company is a regulatory darling. BitMEX, Huobi, OKEx, and Binance have all had their issues this year. Not Coinbase.

**Kraken** is an interesting one. Their acquisition and integration of U.K. derivatives platform Crypto Facilities may have been one of the most **lucrative M&A actions** in the industry to date. The company just launched a bank in Wyoming. They have a successful emerging data platform called CryptoWatch. And the exchange remains a top five spot trading venue globally. Their last valuation of \$4 billion seems like a conservative mark for a company with a legacy, strong global presence, and compelling inorganic growth story.

**BlockFi** has been openly **flirting with a public offering** since earlier this year, and they've grown (**and raised money**) at a breakneck pace. They are the current retail leader in crypto lending today, but it's not clear to me a) whether they've got a sustainable competitive advantage, or if Coinbase et al. will be able to eat their lunch if they enter lending; b) if the business's unit economics are a four-alarm fire since net interest margin in crypto lending has shrunk rapidly; and c) how effective their risk management policies are. It only takes one bad quarter to bankrupt this type of business **as Cred recently demonstrated**.

### 3.7 The Non-IPO Calendar: DCG

Frankly, I'm skeptical DCG will ever go public, so we may never find out how much the business is actually worth. Barry doesn't strike me as a public company CEO (why be Warren Buffett when you can be Charles Koch), and the company will never need additional cash. A presentation from 2018 showed the company had **\$500 million of assets** and no debt through June of that year. Bitcoin's price has tripled since then, while DCG operating subs have grown revenue ~5x. The combined businesses will do north of \$150 million of EBITDA this year, and their growth is accelerating due to Grayscale's monopoly over the crypto "ETF"

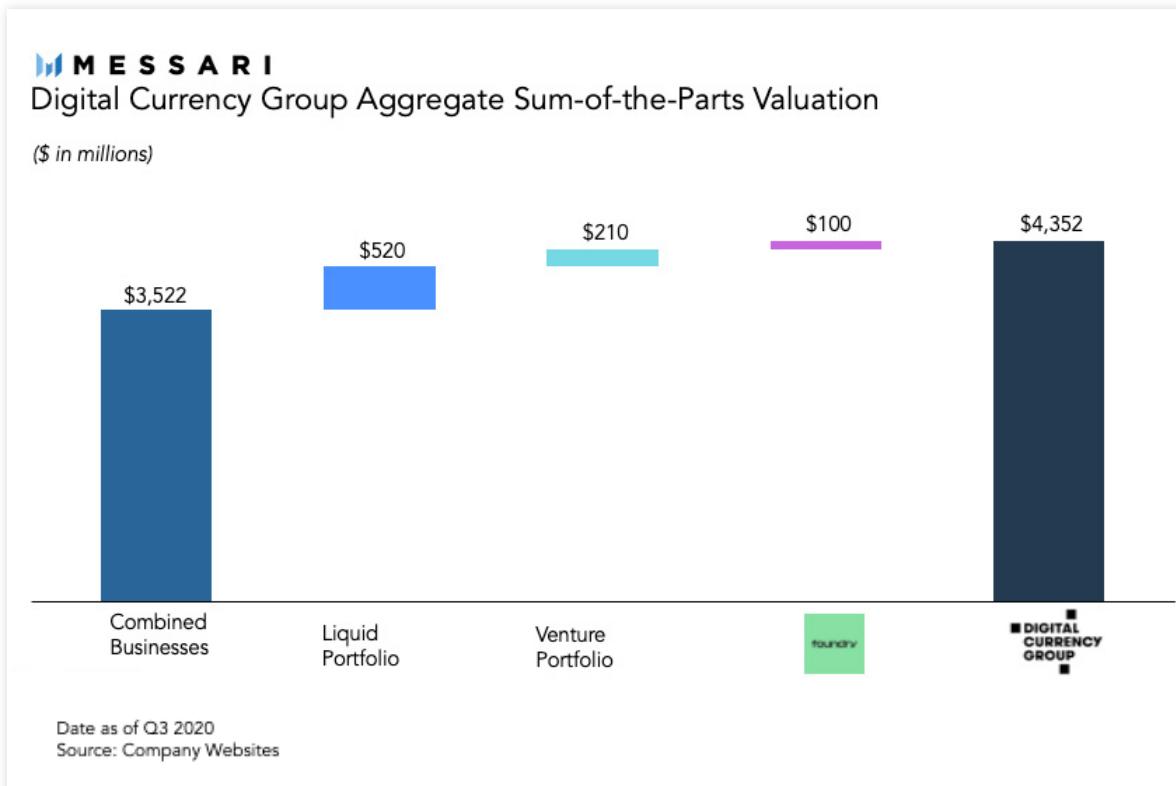
market. What's more, those numbers are essentially annuities, as Grayscale is structured in a way that AUM literally cannot check out. Their fees will only get threatened by competitors once new products are approved and/or they run into some inexplicable regulatory issues.

Really? How about liquidity for early investors?

Actually, they've got a logical solution for that.

Under DCG's predecessor, SecondMarket, private company tender offers were an integral part of the business. That same private market specialization was what helped Barry and Co. identify the crafty path to marketability for Grayscale's trusts. And DCG actually **did** complete several private share tenders in late 2017 as part of a corporate restructuring. I wouldn't be surprised if they gear up for more of them in 2021. The company bought back shares at a \$650 million valuation in December 2017, even though its liquid balance sheet assets alone were likely higher than that at the time (thanks to that fortuitously timed BTC blowoff top). I'd put money on Barry doing a gradual management buyout (maybe even in conjunction with his fellow billionaire board member Glenn Hutchins) before going public when he never needs to.

Don't expect to buy DCG shares next year. Jack thinks they're a **\$4 billion company**. I think they're closer to \$15 billion in this froth. Doesn't matter, though. DCG could have its first billion dollar EBITDA print next year if we see \$100k BTC, and live happily ever private.



### 3.8 Top M&A Targets

DCG may be an outlier in terms of earnings power, but it's certainly not the only company that's flush with cash right now. Bull markets create wealth effects, and the major exchanges and seigniorage-producing crypto projects alike will likely have plenty to spend in the next cycle. At the same time, Wall Street might find an appetite for infrastructure acquisitions, creating three different sets of buyers with multi-billion dollar budgets for strategic investments. If BTC hits the magical \$1 trillion market cap mark in 2021, I don't see how many of the banks can play catch up **without** committing to serious inorganic growth via M&A. And they'll need some exposure to growth in a negative interest rate environment.

My top picks for targets?

Prime Brokerage (BitGo). Custody (Anchorage). Data (CoinGecko, Etherscan).

### 3.9 Work-to-Earn: Fund, Vote, Build

At the end of the day, somebody needs to do the work. Fortunately, there's never been a better time to jump into the fray (part-time or full-time) and start contributing. That typically means you can bring one of three things to the table: code, capital, or content.

Mindshare has historically gone to incentivizing developers to actually build these protocols. This year, non-VC contributors finally got their due as well thanks to liquidity mining. But most projects are also starting to open their wallets to content producers, consultants, marketers, and even watchdogs and voting proxies in order to sponsor educational resources, streamline stakeholder communications in a noisy market, and make sure people actually review proposals and vote on system parameters.

### 3.10 Assets We Like (HODL)

Don't tell me what you think, show me your portfolio.

A stuffy legacy research analyst might not like that our team holds risk in some of the assets we cover. But we have intentionally avoided cumbersome trading restrictions on our analysts (with obvious exceptions) because we believe it's counterproductive. How well do you really understand crypto, if you aren't rolling up your sleeves and participating in these protocols?

**TBI Likes:** BTC, ETH, ZEC, YFI, FIL, LTC (via Grayscale, NOT spot), LUNA, SIA, ANT, NXM, REN, and a smattering of rounding errors.

**Ryan Likes:** ETH, RUNE, YFI, HNT, CVP, ANT, LUNA, CREAM, RPL. TL;DR long DeFi, long ETH 2.0, long governance innovation.

**Wilson Likes:** ETH, BTC, HNT, UNI, Blue coins, Cross chain liquidity (RUNE) and liquid staking

(RPL) networks, and DOT/KSM (initial parachain offerings give 2017 Ethereum ICO vibes and KSM could tag along for the ride).

**Aidan Likes:** BTC, ETH, renZEC, CVP, HEGIC, CHI (long gas tokens cannibalizing the ETH block space market), YAX, and AXS (CryptoKitties meets Tamagotchi: what's not to love?).

**Mason Likes:** ETH, BTC, UNI, YFI (Long Andre), ANT (post-ANJ merge), cash-generating governance-tokens, AXS (see Aidan), community-owned marketplaces and networks (e.g., RARI, AUDIO), application-specific chains (HNT), Tokens (NFTs and ERC20s) with exclusive partnerships (NBA Top Shot, SoRare, CHZ).

**Jack Likes:** HNT, BTC, ETH, YFI, ALPHA, HEGIC, PERP—decentralized derivatives are DEXs in 2019, hyped but no substantial usage (yet). Expecting them to make noise in 2021.

**Eric Likes:** BTC, ETH, ZEC, YFI, MLN, RUNE, CVP (anything that aggregates liquidity, yield, governance, etc.) make it easy for people to participate.

ADVERTISEMENT



We have your best INTERESTS in mind



■ **Leading Lender  
in Asia**

\$900 million outstanding loans  
(BTC/ETH/Stablecoins only)

■ **Asset Management  
Expert**

100,000+ BTC subscriptions

■ **Top Prime Finance  
Provider**

50+ institutional clients

■ **Prudent Financial  
Innovator**

100,000+ BTC monthly derivative  
trading volume

# 4.0

## Bitcoin (and Crypto Monies)

Remember the original crypto “alts” like Peercoin and Primecoin? Maybe you came later during the ICO boom and heard a bunch of chatter about “payment tokens” such as Dentacoin, a currency specially crafted for dentists. (Brilliant!)

When most people talk about cryptocurrency, they use it as a catch-all term, but when I do, I’m just talking about BTC, LTC, XMR, DASH, and ZEC. Money tokens spawned the birth of the entire crypto movement, and it’s hard to imagine a bigger prize than the pool of capital that will accrue to the winning crypto monies.

Before I move on, a discerning reader will notice some absences here:

- Ripple, Stellar, and Bitcoin forks are excluded here. They are in my “barf bag” at the end of this section. (Enjoy the schadenfreude.)
  - Stablecoins are excluded. Crypto dollars are discussed later, but to me, they are more similar to digitized fiat currency than digitally native money, and they aren’t investments.
  - ETH is excluded. It’s a platform token covered extensively in the next section.
- 

### 4.1 Bitcoin Bull/Bear Elevator Pitch

**BTC Bull Case:** [Bitcoin](#) is an unseizable form of private money that’s proven very hard to kill. It’s outperformed every major asset class over every relevant time period in its history, and it’s got perfect macro tailwinds and momentum. It’s getting “safe” to purchase from a legal and reputational standpoint as a professional money manager, and its supply will inflate less than the Fed’s target rate no matter what happens next year. When you look at BTC vs. gold, and its growth vs. global M1, M2, and central-bank balance sheets, it’s a compelling investment.

RATIOS			
		24hr change	
Gold:BTC (marketcap)	38.75x	-1.73	-4.27%
M2:BTC (marketcap)	64.51x	-2.14	-3.21%
BTC:Oil (price)	373.27x	+1.46	+0.39%
Gold:Oil (price)	44.19x	-1.72	-3.76%
US GOVERNMENT STATS			
		30-day change	
Federal Reserve Balance Sheet	\$7.16T ↘	+\$82.83B	+1.17%
M1 Money Supply	\$5.58T ↘	+\$62.40B	+1.13%
M2 Money Supply	\$18.84T ↘	+\$139B	+0.74%

**Bitcoin & Traditional Assets ROI (vs USD)**

	Bitcoin	Gold	S&P 500
1 year:	+79%	+28%	+16%
2 year:	+148%	+54%	+30%
3 year:	+144%	+46%	+38%
4 year:	+2,101%	+50%	+65%
5 year:	+4,918%	+71%	+72%

Source: [CaseBitcoin](#)

**BTC Bear Case:** The “final boss” to beat is the state. For years, countries have regulated bitcoin as a peer-to-peer payment network. Authorities have focused on regulating network edges (exchanges) and monitoring flows (payments). For the U.S., bitcoin presents a tool to undermine international sanctions, and 80% of mining capacity now sits behind enemy lines in China, Russia, and Iran. Will a Biden administration like BTC? TBD.

## 4.2 The Case for Bitcoin: Your New Bitcoin Library

Is “crypto” still just “bitcoin” to you?

My co-founder Dan McArdle launched an excellent resource to help you make the [Case for Bitcoin](#) to your colleagues, friends, and strangers on the subway. CaseBitcoin features key macro metrics, bitcoin network charts, and a curated library of 101 info and must-read position papers/posts by other bitcoin luminaries that help put crypto in a proper global context. This is the must-read resource for anyone who likes dishing out red-pills.

## 4.3 The Prism: Bitcoin Personas

One of the best quotes of the year came from Castle Island Ventures's Nic Carter, who wrote in "[Bitcoin at 12](#):

*"Something unowned, with no one to speak for it, will appear multitudinous in the minds of its users. [Bitcoin] is a glittering prism, refracting the opinions of observers, spitting out radically different visions of itself based on their perspectives."*

Wow. Beautiful. After reading that I feel pretty vulgar comparing bitcoin to wild animals, but I'm not as smart as Nic, so fuck it.

- **The Honey Badger:** You can't subdue bitcoin with threats. Several of the most important exchanges were threatened with serious legal actions this year (BitMEX, Huobi, OKEx), yet BTC didn't flinch. It simply [does not give a shit](#) about custodial exchanges anymore.
- **The Platypus:** As I wrote last year ([h/t Spencer](#)), the platypus isn't a good duck, or otter, or beaver, or reptile. It's a platypus! For bitcoin, its weaknesses are protective armor. BTC is volatile, so it's bad at being money or a credible store of value. Great! It hides in plain sight.
- **The Cockroach:** A line I liked from this [recent conversation](#) with Su Zhu: "Today, BTC is 40% more Lindy, and in terms of years normal people have seen BTC is 10x more Lindy." Lindy = won't die; rides out winters. Every BTC holder must experience a capitulation, bear market emptiness, and a lengthy skin-hardening trough before they can appreciate the cockroach.
- **The Fastest Horse:** The best thing written this year on the institutional investor front came from Paul Tudor Jones. It's a [cogent portfolio allocation thesis](#) vs. an outright speculative bet, and I think it will go down as the best catalyzing thesis on BTC this cycle. (Like [Pfeffer's in 2017](#).)
- **The Bull:** It bothers me that bitcoiners can be derided as chicken little doomsayers; I certainly don't relate to that. Balaji wrote that bitcoin was the "flag" that encoded tech's values: "internationalist, capitalist, decentralized, hyper-deflationary, networked, encrypted, digital, volatile, ambitious, and quietly revolutionary." **That's** the bullish view of the future of money.

Why waste time on all these animal analogies? It's about persona creation. Bitcoin clicks slightly differently for everyone. The honey badger appeals to the cowboy, the platypus to the rigid skeptic, the cockroach to the gold bug, the fastest horse to the rational investor, and the bull to the technologist who wants to bet on the future. Know your audience.

## 4.4 Demand > Supply for Crypto Custody

Call them bitcoin's "big three." Grayscale now holds \$10 billion in assets under management in its flagship Bitcoin Investment Trust, and nearly 3% of the BTC outstanding. Square turned Bitcoin balance sheet accumulation into a serious topic of conversation at board rooms around the globe when it **put 1% of its treasury** into digital gold (and wrote the playbook for other corporates to follow suit) and when it announced quarterly records in bitcoin sales with each passing earnings call. Then there's PayPal, **which offers a preview of what's to come** as crypto support becomes ubiquitous across financial services.

You might think, "How many financial venues do we really need bitcoin to be made available on?" and "Isn't this a little redundant?" I was guilty of that line of thinking at first. But then I looked at the numbers:

- **PayPal:** 346 million users; 26 million merchants; 20th largest "bank" by deposits; \$658 billion in total payment volume.
- **Square:** 30 million users, 2 million merchants, and \$106 billion in payment volume.

It's an order of magnitude change in new potential converts.

Much of the bitcoin that's getting sucked up right now may never touch the market again. These are long-term positions getting built and plowed into cold storage for long-term use by investors and corporates with 5-10 year investment horizons. **And the ratio keeps getting further out of balance.** New bitcoin purchases from PayPal, Square, and Grayscale already exceed newly mined BTC rewards, which means all of the bitcoin is essentially spoken for. In fact, we'll be able to **track them** over time, as more of the mega-acquirers disclose their balance sheet changes from here on out. No virgin coins for the likes of Fidelity, Goldman, JPMorgan, DBS, et al. They'll have to buy our bags instead.

I believe, on Wall Street, the phrase is "It's a beautiful thing."

Perhaps the only note of caution I'd sound regarding corporate hyper-adoption of bitcoin is this: beware and be watchful of Wall Street attempts to fractionalize and rehypothecate BTC. Uncollateralized synthetic bitcoin could dampen demand and create unclear risks to the underlying network's health at some point.

But we're a long way from that being a real concern, and by the time it is, we'll have ample warning and will have already won: BTC will be \$100k+.

## 4.5 Demand > Supply for Countries

Hundreds of millions of people struggling with capital controls, high inflation, or poor financial infrastructure can usually still count on bitcoin as a store of value. BTC is now #15 vs. other global currencies if you compare it to [global M1](#). Its exchange rate hit fresh all-time highs [earlier this year](#) against Turkish Lira (#35), Brazilian Real (#38), Argentine Pesos (#50), and Iranian Rial (#56). And in November, it added new highs vs. the Indian Rupee (#14), Russian Ruble (#26), and South African Rand (#37). As of this writing, it's flirting with and has probably already exceeded previous all-time highs against shitcoins like USD, EUR, GBP, JPY, and CNY.

In a world of unrestrained spending and central-bank debt monetization (QE), many smaller fiat currencies could begin to wobble in 2021 and 2022. Some of the more creative central banks may follow the corporate playbooks out of desperation and turn to BTC as a lifeline. (Iran may have done this already, for better or worse, but we really want central bank buys that we can feel good about promoting.) If you're a central bank, you don't have to outrun the bear (market); you simply have to outrun the countries with whom you trade. Printing worthless reserves to buy or mine BTC seems like a gamble worth making when the alternative is certain loss.

We'll see a MicroStrategy-esque move into BTC by at least one small central bank in 2021.

## 4.6 Fungibility & Surveillance

Bitcoin has made it out of mom's basement and onto the world stage. That's the good news.

The flipside is that a significant percentage of bitcoin now sits within known centralized institutions around the globe. Between custodians like Anchorage, BitGo, and Fidelity, exchanges like Coinbase, Binance, and Huobi, and asset managers like Grayscale and CoinShares, you can begin to triangulate on how much BTC is held by centralized, regulatable third parties. That's a risk, and the more BTC that accumulates at these power centers, the higher the likelihood the currency eventually loses fungibility as institutions are forced to monitor for "coin taint" and abide by the expansive FATF "travel rule" (more on this in [Section 12](#)).

As Compound's General Counsel [Jake Chervinsky explained](#), we've been in a honeymoon phase so far: big enough to be relevant, but not so big as to threaten the status quo. In 2019, we were fortunate that Facebook and the Libra team took the regulatory arrows for us. Next year, there will be no such bogeyman to distract global authorities.

If Bitcoin's core developers push privacy enhancements that are too good, we could end up with another (much more damaging) hard fork: one that preserves the ability for chain analysis companies to conduct their forensic investigations (and for regulated financials to surveil their customer transactions), and an anarchist-driven fork that mixes coins natively. Reigning in travel rule-inspired surveillance overreach will be the industry's greatest regulatory challenge to date. The battle to preserve self-custody and private transactions must be won at all costs.

## 4.7 Taproot & Schnorr

Hey, what's on the bitcoin technical roadmap, anyway?

I feel a bit guilty saying this, but I haven't thought about the bitcoin roadmap once this year until I got to this section of the report, the very last one I'm writing.

I suppose that's sort of the point with bitcoin: you don't have to worry about missing changes, because it's a system more or less on autopilot. That's how the general narrative goes, anyway, but the truth isn't quite so simple, and I'd hate to shortchange the developers who've been propping up the protocol (entire industry?) for years, often for very little compensation, by ignoring their contributions and upgrades.

There's actually a bit to be excited about in 2021, starting with "Taproot." The proposed soft fork aggregates three primary BIPs ([340](#), [341](#), [342](#), [nerds](#)) to improve privacy on bitcoin through something called Schnorr signatures. Schnorr is fun to say, and also provides greater privacy (and efficiency) for broadcast transactions by batching signatures so multi-sig and single-sig transactions are indistinguishable. The big use case here is aggregating signatures for transactions that flow through mixers like CoinJoin, so Schnorr makes it marginally harder, but not impossible, for blockchain forensics companies to do their jobs. Also included in the proposed soft fork is "Tapscript" an upgrade to bitcoin's programming language that introduces new protocol operators and allows devs to use more complex scripts on bitcoin.

We'll almost certainly see Taproot soft-forked in early 2021 as 82% of miners are now [signaling support](#) for the upgrade, and are now just deliberating on an "activation method" and date.

On the mining / security front, most of the updates were geared towards further decentralizing transaction processing: miners switched over to Stratum V2, a protocol that helps reduce network latency and remands transaction support decisions (which transactions can go into a block) to hardware owners [vs. pool operators](#); Bitcoin Core v0.21.0 (expected to be released this month), includes support for Tor V3 addresses that help the network's Tor nodes "gossip" with each other; and Dandelion++ will basically spoof where transactions originate by default so that adversaries have a tougher time identifying the actual source of a transaction.

Like I said, it's the inner workings of the rocketship. Don't ask questions, just grab your seat.

## 4.8 Lightning & Sidechains

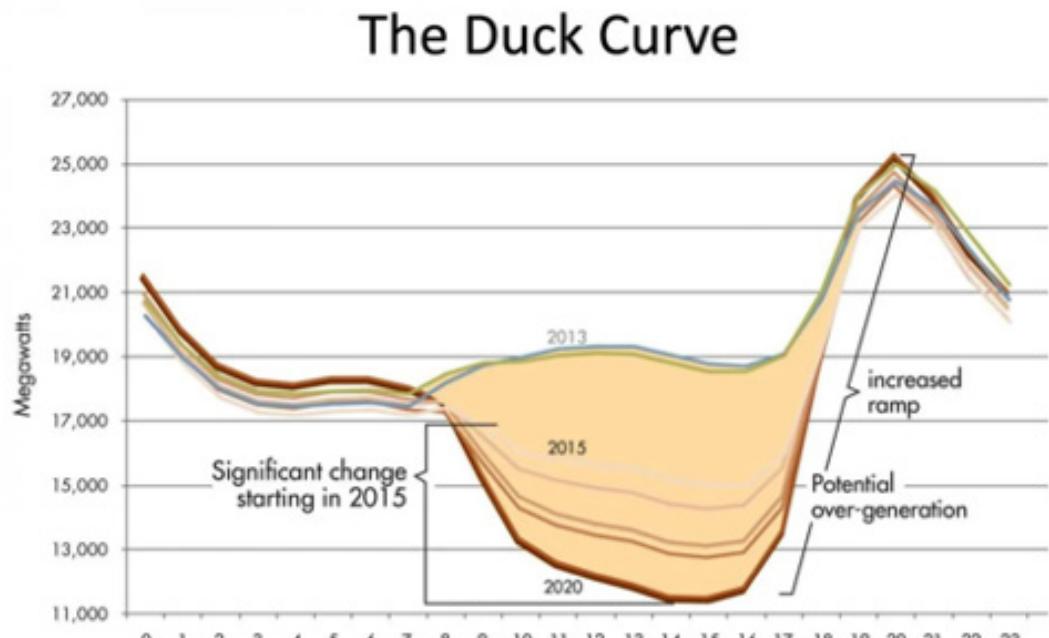
Has Lightning and Sidechains development stalled? Well, it's early, and my earlier predictions about 2019 and then 2020 being a breakout year for Lightning appear wrong, but fuck it, let's triple down. There have been some meaningful [UX improvements](#) (liquidity and privacy) in Lightning, but honestly, it increasingly looks like Lightning has been lapped and then some by Ethereum stablecoin payment applications. Wake me up when I can do something with it.

As for sidechains, it looks like they will be interesting primarily for wrapped bitcoin transactions, Blockstream's proprietary Liquid network, and Confidential Transactions, which mercifully look like they have no shot of making it into the primary bitcoin blockchain due to the regulatory issues I mentioned above. That might be a net positive for all involved, as CTs on sidechains ensures the full bitcoin supply can still be continuously audited over time (which is a major limitation for Zcash—more on ZEC in [Section 4.11](#)).

## 4.9 Miner Diversification and Predictability

Liberal governments worldwide may yet succumb to the narrative that bitcoin is just one big, wasteful, polar bear-slaughtering digital smokestack, whose energy consumption patterns will inevitably destroy the planet. In fairness, it's hard to argue that proof-of-work mining **today** is not an electricity hog. It is. Still, we also have to allow for the possibility that proof-of-work mining **could potentially reduce** total carbon emissions one day.

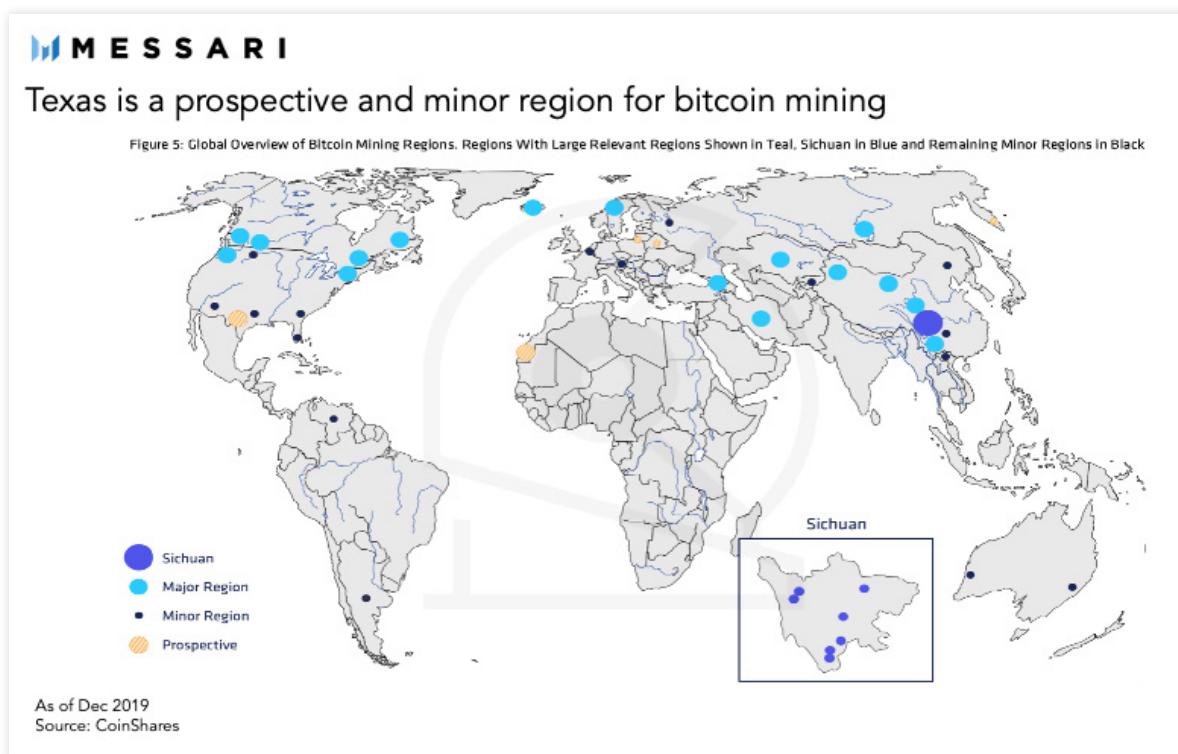
To understand why, you first need to understand the "[Duck Curve](#)" and the role of modern energy grid demand-response systems. Take Texas's grid for example. The state's deregulated markets have led to a surge in power generation, particularly in renewables, where Texas is now one of the largest producers of wind and solar energy in the world. But the variance in intra-day energy production and energy consumption patterns often leads to wasted energy or even negative energy prices when the grid is strained to capacity. Excess energy needs to get funneled off of overloaded power grids to **some** external source. What if bitcoin mines could eventually serve as clean energy grid load balancers?



Certainty regarding bitcoin's role as a climate change accelerant ignores the potential that we could get better at storing clean energy, balancing grid load (intra-day and intra-season), and generally figuring things out. It's a bet against human ingenuity (and history), and it ignores that bitcoin mining, in the West especially, is increasingly clean.

Energy concerns won't be the only ones policymakers have with bitcoin mining. It's not great for national security to have the majority of bitcoin's hash power (not to mention the monopoly on ASIC chip manufacturing) sitting behind the Great Firewall. But Western mining outfits at least bring some much needed transparency to that shadowy part of the market these days. U.S. operators like Layer1, DCG's Foundry, and Galaxy Digital Mining can provide a clearer picture of mining supply chains than we've arguably ever had before.

For now, all we know is that **MicroBT and Bitmain are SOLD OUT** of their rigs through next April, even though Western companies are still trying to buy them.



Mining is still ruthlessly competitive, but there are reasons to be optimistic that it could get more dispersed over time.

For starters, the liquidity of bitcoin derivatives markets and the commonality of local energy contract negotiations make it easier than ever to manage the unit economics of the mining business if you have sufficient scale and a strong supply chain. Second, the giants that may enter the space, such as Fidelity or DCG or other major Western institutions might be ok with mining as a (small) loss leader now that their downsides can be more clearly hedged, and these operations become (at worst) a small tax that helps show they take geopolitical risk seriously.

## 4.10 Litecoin, Bitcoin Forks, and Toxic Waste (XRP/XLM)

I can't fucking believe I still have to write about these piles of shit.

But at least this year, there's a silver lining. Look, Bitcoin forks BCH, BSV, BTG, et al. are useless. Bitcoin Cash can't stop infighting and forking, and it's become a soap opera (or underage telenovela) starring crypto's formerly important people<sup>tm</sup>. BCH had its shot in 2017, but bumped into its ceiling, and now means nothing. You lose. Good day, sirs.

XRP and XLM pumped in mid-November, because they're old coins that traders are front-running based on the reflexive belief those assets have "staying power," and low nominal prices will entice newbs stupid enough to buy them. Synthetix founder Kain Warwick [captured my feelings nicely](#) when he compared making money on an XRP trade to "liquefying orphans as fuel for street lamps or something." Sure, you can do it, but maybe hold yourself to a slightly higher standard, bro.

You can say I'm bitter because I missed out on the trade, but then you'd have to believe I'm lying about trading things I don't believe in (it's a slippery slope to monetizing a reputation through pump and dumps), or that my comprehensive takedown of networks like XRP in 2018 ([shot](#) and [chaser](#)) were flawed.

They weren't. These are toxic assets propped up by regulatory capture, and they go against everything that got me into crypto.

That brings us to Litecoin, which is essentially bitcoin's production testnet. Litecoin adopted and tested SegWit, lightning, and sidechains before they were activated on bitcoin, so LTC at the very least serves as a sort of bounty pool for hackers to stress test BTC upgrades. Attack the litecoin network and steal funds there if you can. LTC is somehow still unironically referred to as "digital silver," but unlike the other assets listed above, its tight coupling with BTC does make it at least somewhat interesting. And... holy hell, it's the MVP of the Grayscale trade. (I know I keep teasing the mechanics, go to [Section 9.1](#) to skip to the details.)

There may not be a better risk/reward profile in the entire crypto market right now than the Grayscale Litecoin Trust trade. As of this writing, LTCN trades at about 6x the underlying holdings once its shares become unrestricted. Sure, you take principal risk on LTC during the 12 month lockup, which you may not love, and sure, it's likely the Grayscale premium comes wayyyyy down as other investors slam this trade in the months ahead, but ETHE is a good proxy for how long and at what magnitude these premiums can last (hint: a while). If LTCN eventually follows GBTC and ETHE as SEC reporting companies, even better: the holding period for the trade would drop to six months.

Nice risk/reward play here, and one in which I'm considering a position myself. The downside? When you play this trade, you are really fucking over the retail buyer on the other side of the 12 month lockup. My loathing for the SEC and its ineptitude in getting a bitcoin-ETF approved

puts this over the edge, though. Time to liquefy some orphans with the SEC as an accomplice.

Bitcoin Cash and Ethereum Classic present similar opportunities at Grayscale, but you take much more principal risk with them given their history of forks and 51% attacks. XRP and XLM trusts might become publicly tradeable at some point as well, but that's not a foregone conclusion; Grayscale has only listed proof-of-work coins publicly so far.

That leaves one other Grayscale trust, and it's an asset I like....

#### 4.11 Zcash: Trojan Horses, Hypermodels, and True Privacy

As discussed earlier, [Bitcoin](#) isn't truly private, which creates some risks and scalability challenges regarding its fungibility. There are several privacy-focused cryptocurrencies that complement BTC in this regard, and push the envelope where bitcoin (practically) cannot. [Monero](#), [Dash](#), and some smaller currencies like [Horizen](#) and [Decred](#) are worth mentioning, but ZEC is the "trojan horse" I like for its opt-in privacy model, and for the pragmatism of its core builders and promoters. And I want to be [a good hypermodel](#), so I shill it, too.

[Zcash](#) was launched in late 2016 by some of the world's best cryptographers with the goal of creating the "https" of crypto money ("cybercoins" as the founder, Zooko, calls them). The protocol's key innovation was the introduction of "zero-knowledge proof" cryptography into its native payments network, which provides stronger privacy guarantees than typical blockchain transactions. The team also pioneered the concept of *storing* assets in "shielded" pools vs. merely anonymizing transactions. More than 90% of the Zcash blockchain's transactions run through viewable, pseudonymous wallet addresses, but the remainder are stored in the network's completely anonymous "shielded pool." This sounds mundane, but it's a big deal.

Crypto fund Multicoin (though a vocal critic of privacy coins) has a [great primer on privacy coins](#), which I recommend. They come to a different conclusion about the merits of these assets, but what you'll notice from this graphic is that Zcash is cleverly designed and incrementalist. Zcash brings privacy tech to market gradually, but once assets are anonymized, they are basically impossible to crack in the shielded pool.

	BTC	ETH	ZEC (Transparent)	BTC + CoinJoin	ETH + Mixers	ETH + Aztec	XMR	ZEC (Sapling)
Sender	Red	Red	Yellow	Yellow	Yellow	Yellow	Yellow	Green
Receiver	Red	Red	Yellow	Yellow	Yellow	Yellow	Yellow	Green
Amount	Red	Red	Yellow	Yellow	Yellow	Yellow	Yellow	Green
IP Address	Red	Red	Yellow (+ Dandelion)	Yellow (+ Kovri)	Yellow (+ Kovri)	Yellow (+ Kovri)	Yellow (+ Dandelion)	Green

Legend:

- Public (Red)
- Obscured (Yellow)
- Private (Green)

Table 1: Privacy spectrum for cryptocurrency transactions.

Source: [Multicoin Capital](#)

That anonymity balance, and the seamless bridge between “z-addresses” (anonymous) and “t-addresses” (pseudonymous like BTC and ETH) is no small feat. Korean and Japanese regulators have made it difficult for their regional exchanges to support any assets that facilitate anonymous transactions. U.S. regulators provided similar (not-so-subtle) guidance that “anonymity-enhancing currencies” may be impossible for regulated exchanges to support given their lack of traceability.

But when it comes to truly encrypted cash, ZEC set the dividing line clearly to help attract some early advocates and enterprise supporters.

Some Western businesses may [delist privacy-focused currencies](#) like Zcash to limit their regulatory risks. Others may support all privacy coins and fight restrictions in court. Coinbase and Gemini (typically regarded as best-in-class from a compliance perspective) are the ones I watch most closely, though. They've historically shied away from Monero (which offers default privacy through a private, but imperfect solution called “ring signatures” that allows transactions to “hide in a crowd”), but they've supported Zcash because of the protocol's default transparent (pseudonymous) addresses and opt-in privacy. It helps that Zcash's affiliated entities have been assertive with education and advocacy, backing groups like Coin Center and the Blockchain Association, and collaborating with institutions like [JPMorgan](#). But Zcash still generally stands to benefit from hiding in BTC's shadow and slowly building its shielded pool over time if it possibly can.

ZEC has a resilient community of investors (it takes a strong stomach to have held ZEC despite the relentless selling pressure it's faced from high initial inflation), and its November halving (its first) was material. It also provided ongoing funding to core developers to keep the upgrades coming. And more bridges are being built to other smart contract protocols (Ren, Keep, and Wrapped.com) that could make it easier to leverage ZEC while still storing funds in a default private pool. Other protocols may incorporate zero-knowledge transactions, but they won't necessarily solve the private wealth storage default that Zcash gets right. I'm bullish on anonymous cash, so I'm bullish on ZEC. It's my second largest crypto investment.

Note: [Some of my colleagues are skeptical](#) that ZEC is interesting as an investment.

# Your Crypto Investing Goals Are Our Goals

Bitstamp is the longest-running global cryptocurrency exchange.  
Since 2011, we've earned the trust of over four million customers and leading financial institutions.



## Security Comes First

Advanced storage and insurance coverage for your crypto assets



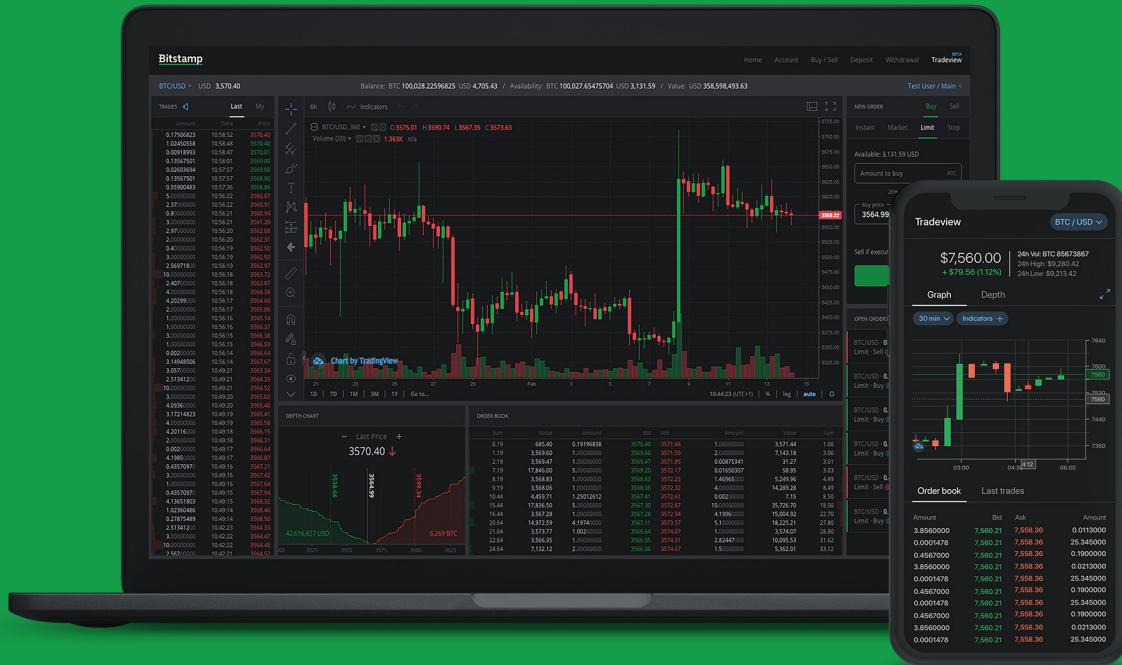
## Intuitive Tools, Powerful Tech

Buy and trade crypto on web, mobile or APIs, powered by cutting edge tech from Nasdaq



## Support with a Human Touch

24/7 global customer service and personal managers for high-volume traders



VISIT [BITSTAMP.NET](https://bitstamp.net) OR DOWNLOAD THE BITSTAMP APP TO GET STARTED



# Bitstamp

Trading since 2011

# 5.0

## Ethereum

Ethereum's acolytes believe they can build the transaction settlement layer for *all* of the world's markets. Money and financial applications. Secure, decentralized computing. Digital goods and gaming economies. Intellectual property and personal data. Everything.

To be honest, they've earned that swagger. Ethereum, for all its early limitations, has worked, and it's spawned thousands of high-potential applications in just five short years.

Ethereum is the most important smart contract platform today because it was the first to foster a large community of passionate, well-incentivized contributors. Unlike the early internet, even Ethereum's "failures" have failed up, as early tinkerers have ridden the wave of ETH from less than \$1 to ~\$600 today. Ethereum is on pace to process more than \$1 trillion worth of transactions this year, including the vast majority of volume in the burgeoning (and increasingly complex) DeFi and "crypto dollar" sectors. It's been so successful that eth1 is now at max capacity, and must scale by orders of magnitude, quickly, to maintain its market share vs. newcomers, and keep its vibrant ecosystem cost-competitive.

I believe it will succeed. First things first, though, a point of clarification....

---

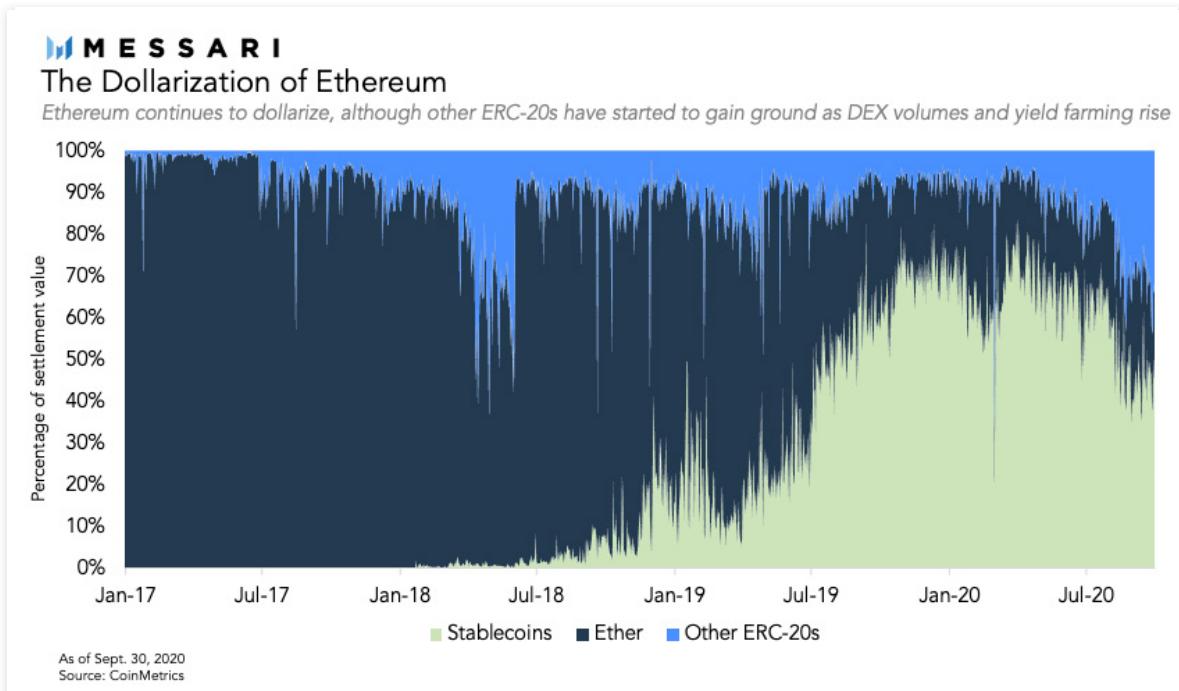
### 5.1 ETH is Not Money

That's ok! It will likely prove to be a terrific investment, anyway. A commodity that secures transactions on the world's most valuable computing platform (gas for throttling, staking for processing), and that can be ubiquitously leveraged as collateral within a burgeoning new financial system, is plenty valuable. I love ETH, and I own a bunch.

But here are ten reasons ETH is not money, why it will never eclipse BTC, and why its 2017 flirtation of a “flipping” was a one-time anomaly:

**1. History:** In 2017, there was a brief period when Ethereum looked like it might \*potentially\* be more secure than Bitcoin. ETH had survived the previous summer's **ETC hard fork** and **Shanghai attacks**, while BTC was embroiled in an ugly battle for the soul of the project. Bitcoin's “scaling” debate wasn't about transaction throughput, so much as whether the project would be “peer-to-peer electronic cash,” or higher-stakes store of value settlements. The community chose the latter path. The minority chain, Bitcoin Cash, rallied to 0.45 BCH:BTC at first, but then receded and never tested those levels again. When the BCH threat subsided, BTC added a new layer to its anti-fragile armor, and ETH may never again test its market cap high of ~50% of BTC. With the eth2 migration, BTC will be **95% dominant** in the proof-of-work monies category, while ETH must compete with dozens of viable platforms to retain its 65% dominance. Substitutes hurt monetary premiums; BTC has few substitutes, ETH may have many.

**2. Reserve Rotation:** As discussed earlier, demand for ETH during the last cycle was fueled in large part by its reserve currency status for ICOs. Once the market corrected and dollar-denominated Simple Agreement for Future Tokens (SAFTs) agreements replaced mega on-chain ICOs, the reservation demand for ETH leveled off. That demand was only partly replicated in this year's DeFi boom as ERC-20 crypto dollars largely replaced the need to hold ETH, which is an important (40% of total locked value), but not critical, collateral asset for DeFi applications today.



- 3. Institutional Mirage:** “Smart money” demand for ETH is overstated. Most of the apparent bidding is happening thanks to the Grayscale trade with more than 80% of ETHE (Grayscale’s Ethereum Trust) currently restricted. That means all the institutional AUM growth has been from funds hammering the creation / rule 144 sale arb trade (with leverage) to **collect the 60% ETHE premium to spot**. Don’t get me wrong, that’s not nothing! But a synthetic trade is not a 5-10 year investment. As a macro hedge, ETH doesn’t come up in conversation. As an uncorrelated asset, ETH is relegated to the bench due to its correlation with BTC.
- 4. Narrative Complexity:** Memes work, and nothing kills a good meme like complexity. Bitcoin has simple narratives that septuagenarian money managers and politicians can sound out. I was even able to turn my 85-year-old grandfather into a BTC holder back in 2014 once I explained it to him because he’s better than your grandfather. On the other hand, I have never even attempted to explain Ethereum to him. It’s not that most people are too dumb or lazy to learn new things (though that’s true); ETH the asset is just tough to grasp because the narrative keeps changing. The “triple point” pitch is cute, but self-defeating because it makes you foie gras people with three concurrent radical investment theses at once.
- 5. Wrapped Assets:** As total value locked in DeFi and on Ethereum continues to swell, so will interest in wrapping synthetic Bitcoin (and other assets) and leveraging them on Ethereum. The same catalysts that should, in theory, drive ETH higher as collateral demand increases, will drive wrapped BTC higher as well. So ETH doesn’t gain ground.
- 6. Strong Hands:** Bitcoin holders have always been Spartans to Ethereum’s Athenians. They eat meat, they’re mean, and they’re specialists at war. The Ethereum community has more diversity and social awareness, I think, which is great for a platform. But that’s bad for weaponry like state-independent money. It’s not like BTC holders are getting weaker, either. The new money inflows are coming from 5-10 year holders. On the other hand, It’s unclear whether eth1 or eth2 will be the blockchain of record next year.
- 7. Sub-token Leakage:** With the eth2 roadmap moving to “eth1.5 with rollups” (more on wtf that is below), every transaction that moves to “layer 2” rollups essentially moves to new blockchains that could include new tokens. If you want those sub-chains secured, you might add transaction fees and security rewards there, too, which would erode value from the core eth2 blockchain.
- 8. Alt-token Leakage:** I cannot overstate how risky it seems that eth1.5+roll-ups look a helluva lot like *mainnet* competitors that don’t have the whole “existentially risky migration” thing to worry about. To a layperson (and maybe many technologists) Polkadot and Cosmos hub-and-spoke models look very similar to eth2. There are numerous ways these competitors might siphon value (again, more below).

**9. DeFi-token Leakage:** Financial applications are fatter and protocol tokens are thinner (less value accretive) than are commonly argued. That's because capital pools tend to centralize, but transaction *rails* tend to least-cost route around rent-seekers. It seems possible, if not probable that DeFi applications with lots of liquidity and locked value will capture more fees (proportionately) over time than base layer protocols whose fees are treated more like system imperfections than critical security model inputs.

**10. Cumulative Demonetization:** If Bitcoin is a prism that attracts different narrative seekers into the same base asset, ETH is the opposite: too many narratives, each of which can be better expressed by a more specialized protocol and token. Demonetisation has arguably been a gradual process already in motion with the explosion of stablecoins, but I think there's more to leak. The clincher is that you don't even need to agree with the threats above, just that the perceived threats exist to eventually hurt ETH's monetary premium.

There's one reason I might be wrong: bitcoin fails. Maybe it's attacked by sovereigns who choke off liquidity providers, criminalize self-custody, hijack mining capacity in order to 51% attack the network (or delay transactions) to oblivion; or the inflation subsidy expires and destroys bitcoin's security model; or something else. It doesn't really matter, though, if BTC is overtaken by ETH, we can pack our toys and go home because ETH will not have the memetic resilience or robust sovereign-grade security model to compete as crypto's primary value store.

(Note that Watkins and Wilson just wrote a [BIBLE on Ethereum 2.0](#), and they disagree with this section pretty much point for point. We'll have the analysts write a rebuttal piece to absolutely destroy their least favorite takes of mine from this document.)

## 5.2 ETH as a Defensive Asset

Now that I've sort of crapped on it already, here is the gist of the "[triple point asset](#)" thesis: ETH is valuable because it's a commodity (necessary for transaction usage), a capital asset (for network staking), and a form of money (reserve).

The faith in Ethereum's monetary premium comes from people who argue Ethereum users will find it convenient to hold at least some ETH for gas at all times, particularly following the [introduction of EIP 1559](#), which formalizes the ETH reserve requirement by forcing users to pay gas fees with ETH vs. any arbitrary ERC-20 asset, including stablecoins.

Under that new model, ETH will be burned rather than remitted to transaction validators, so triple pointers believe deflationary checks could make ETH even more scarce than BTC. I'm not convinced. To me, this is no different from filling up your car's gas tank periodically vs. every time you go out for milk and eggs. Of course you'll hold ETH for gas if you use Ethereum regularly. But a Uniswap user or DeFi borrower doesn't want or need ETH to use the platform. I don't siphon ounces of diesel from my fuel tank when I go to pay for a drive-thru order, either.

I'll admit maybe I just don't like the triple point analogy because it sounds offense-oriented. A triple threat position in basketball means you're in position to shoot, pass, or dribble.

I hear "triple point," and it sounds like ETH is great for scoring (winning the money use case), passing (collateralizing to speculate on other winning trades), and dribbling to create space (paying commodity gas fees to claim block capacity). Pick a lane, man. There are better speculative "shots" to take in the crypto money competition, and you can "pass" stablecoins to DeFi to earn yield with less principal risk. In the triple point analogy, that leaves "dribbling," which is a race to the bottom in terms of value capture; anyone can dribble around looking for the lowest cost rails to process a transaction. Woof for ETH.

Maybe better to think of ETH as a defensive specialist instead. It helps participants clear the boards (mempool) and settle transactions securely; steal from dishonest actors (slash security deposits), and block adversarial shots (prevent blockchain bloat and reject bad transactions). ETH as the world's top defensive cryptoasset is still important and very valuable.

It's ok to be Dennis Rodman to Bitcoin's Michael Jordan. There's a lot of money to be made in defending a network with ETH's transaction volume, through both fees and staking seigniorage under eth2. (If you can't tell, I just finished *The Last Dance*, and loved it.)

### 5.3. eth2: PoS, Sharding, and a Beacon (Chain)

Again, our senior analysts just wrote a [phenomenal primer](#) that digs into the nitty gritty of "eth2." I won't attempt to rewrite their overview of the new system, its design choices and underlying research, and its prospects, but I will provide a short summary here for my fellow short attention-spanned ladies and gents, along with a summary of what to expect in 2021 from the broader smart contract sector.

**Context:** eth2 is a fundamental change in how Ethereum operates and secures its ledger, and it will mark the first time a major operational blockchain has attempted to rebuild itself from scratch under a new consensus mechanism. eth2 is essentially a brand new blockchain. Ethereum developers are attempting to migrate the eth1 "state" to the eth2 chain with minimal disruption to the tens of thousands of applications that have already built atop Ethereum. It may take several years to complete the full multi-phase migration, but if successful, Ethereum could scale its transaction throughput by more than 1,000x, while strengthening its "store of value" bona fides by bringing long-term network inflation down to 1-2%. Many in the community think of eth2 as the most important design change the Ethereum protocol will ever undertake.

**The Solution:** eth2 introduces two fundamental changes to the Ethereum protocol. First, it switches its consensus algorithm from miner-driven proof-of-work (like bitcoin) to validator-driven proof-of-stake (like most of its "layer 1" smart contract platform competitors). Second,

it splits its blockchain into 64 different “shards” that can be processed simultaneously and independently. Proof-of-stake is straightforward-sounding, if complex underneath. Anyone with 32 ETH (~\$18,000 at the time of writing) can commit assets to the network as a security deposit, and validate new network transactions at minimal cost. Honest validators earn network rewards (new issuance), and would-be attackers get penalized harshly for dishonest transactions (lose their security deposits). Sharding, on the other hand, scales Ethereum by partitioning contract computation and storage across 64 sub-groups of linked nodes, plus the “central nervous system” of eth2, the beacon chain, which manages the registry of validators and stores reference snapshots to the various shard states.

**The Transition:** To minimize disruptions to tens of thousands of current Ethereum-based applications, the community has chosen a phased rollout of eth2. The two blockchains will operate in parallel during the transition, until the full eth1 blockchain merges into one of eth2’s 64 shards. “Phase 0” introduces the **beacon chain** and the eth2 validator set, but will have limited functionality (launched December 1). Phase 1 will introduce eth2’s 64 **shard chains** for enhanced data storage (launch Q4’21). Phase 1.5 will transition eth1’s current state to a shard of the eth2 network, fully swapping Ethereum’s consensus layer to **proof-of-stake** (launch 2022). And Phase 2 will unlock smart contract execution capabilities within shards, partition network state across shards, and introduce a new developer-friendly framework, EWASM (launch 2023).

If you thought, “wtf did he just say?” I promise I won’t do that again.

All you need to know is that years of research have gone into this proposed transition, and it’s looking promising. It’s exciting to see something as big as eth2 finally get launched, and from a theoretical standpoint, it feels like a less risky upgrade now that numerous other proof-of-stake and sharded blockchains have already come to market.

Still, Ethereum has never followed a straight (or timely) roadmap, and we’ve never seen a migration of this complexity or potential collateral economic damage in bad scenarios. Serenity could be a huge achievement, and I don’t like people who root against eth2 or SpaceX launches. We should all be rooting for it.

## 5.4 Actually ETH 1.5: Rollups, PoS

lol jk eth2 will probably never fully launch.

Vitalik and friends have already rallied around a **“Layer 2”-centered scaling solution** called “rollups” that will alleviate Ethereum’s congestion in the near- to medium-term, and likely lead to the scrapping of the most complex “Phase 2” network upgrades.

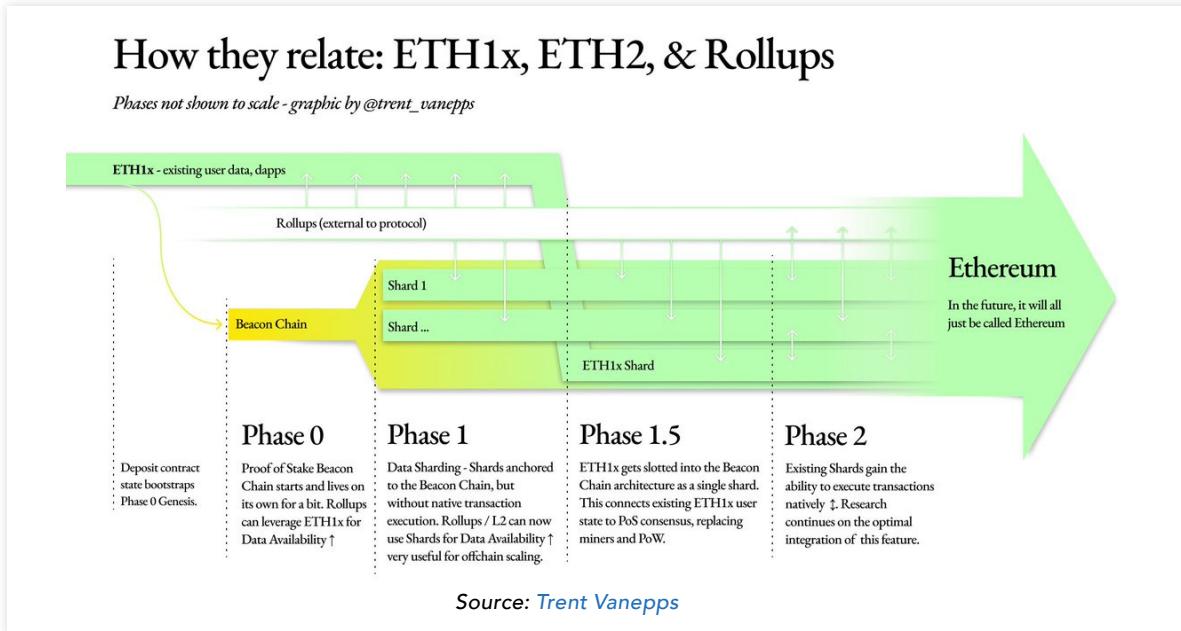
Rollups are essentially independent blockchains that process transactions independently of the Ethereum blockchain, but settle snapshots of their state to the main chain. They’re

structurally similar to bitcoin's sidechains. Success and prioritization of rollups would lead to a pragmatic shift in the Ethereum roadmap as eth1.5+rollups would amount to a >10,000x improvement in network processing capacity, while killing headaches that could arise from attempting to split contract **execution** across shards. (I'm told that's a challenging thing to do.) eth1.5+rollups would allow everyone to settle high value and bundled transactions directly to the eth1 beacon chain, while partitioning data storage across other eth2 shards.

In plain english, if a) the Beacon Chain launches, b) rollups get widely adopted across Ethereum's infrastructure, and c) Phase 1's introduction of shard chains goes smoothly (a lot of "ifs"), we'd see the full **effective** migration to eth2 by the end of 2022.

With history as a guide, I'm taking the over on that deadline.

It does seem teams from Optimism, ZKSync, and Starkware are ready to go live with rollup chains already, though. And other scaling solutions like OmiseGo's Plasma could help alleviate system strain in parallel. And Vitalik seems excited that the Phase 2 roadmap shift would allow core developers to spend more time focused on other technical challenges like eth2 inter-shard transaction latency, PoS security enhancements, and private transactions.



## 5.5 Beacon ETH

I might be bearish on the speed at which eth1.5 rolls out, but I never doubted the beacon chain would activate on December 1, if for no other reason than the Ethereum establishment (ConsenSys, DARMA Capital, Bison Trails, etc.) simply wouldn't allow for an **embarrassing launch delay due to a lack of quorum**. I'm surprised **the prediction markets were betting against** Uncle Joe and the eth2 activation, as the larger ETH players themselves had the capital to seed the beacon chain launch, and were actively recruiting fellow depositors by introducing collateralized loans against their stakes.

I do wonder, though, whether the decision to disable transfers of Beacon ETH (BETH) ends up incentivizing exchanges to stake on customers' behalf and then securitize BETH for trading and borrowing. That seems likely, as there's no reason to commit ETH to the beacon chain early, and tolerate indefinite illiquidity when [a synthetic BETH token could be used to generate yield](#) on both the beacon chain's staking and elsewhere in DeFi. Some have argued [BETH would actually replace ETH](#) during the transition (it would be a liquid, yield-bearing synthetic vs. boring old spot ETH), but if the goal is proving that Ethereum's new proof-of-stake model is the future, I'm not sure exchange deposit concentration and rehypothecation of staked ETH will be a good thing from a PR standpoint, or in fact.

It's worth noting beacon chain staking is a subpar deal for accredited ETH whales, too. As of this writing, the yield on staked ETH in the beacon chain is down to 15%, and will drop to the single digits with just 2.5% of the network staking. That's with illiquidity and eth2 technical risks. From an investment standpoint, it's more enticing to "stake" ETH to Grayscale's Ethereum Trust, where ETHE trades at a 60% premium to the underlying. This may be a crowded trade, with dozens of funds hitting Grayscale this year (often with leverage) to create new shares amidst hopes of flipping them after the lock-up. But even post those position liquidations, it's hard to see a scenario where that ETHE premium drops below 10% like BETH.

ADVERTISEMENT

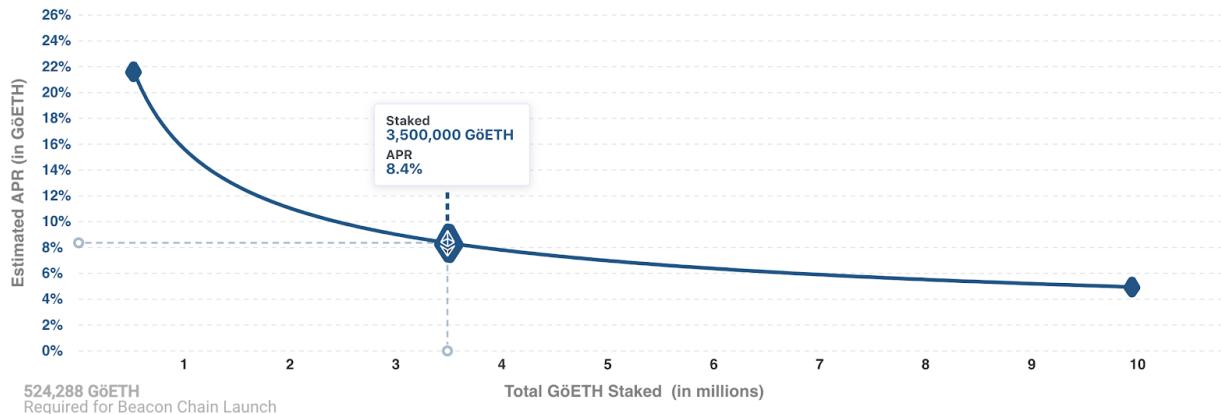


We have your best INTERESTS in mind

## 5.6 ETH Farming Rewards

The de-risking that will take place with eth2 in the coming months is important. If the beacon chain launches without a hitch, and ETH stake begins to accumulate quickly to the new chain, Ethereum's new security model can get slowly tested and reinforced. If the staking percentage remains low or concentrates among whales, it could be a double whammy: low signaled confidence in a timely Phase 1 launch, and concern around rewarding whales as the network's new rentiers.

Let's look at the positive, though: broad-based staking support would have major positive effects like dropping the ETH inflation rate below its more centralized, higher-inflation competitors, and proving something even bitcoin can't replicate any time soon: that Ethereum's "Minimum Necessary Issuance" policy secures the network, and prevents it from becoming overly reliant on variable transaction fees. A successful Phase 1.5 migration would also lead to the [third effective downward revision of issuance rates](#) in Ethereum's monetary policy, making it difficult for critics to argue the system could easily become inflationary in the future based on the whimsy of its core developers.



Source: [Eth2 Launch Pad](#)

ETH validating	Max annual issuance	Max annual network issuance %	Max annual return rate (for validators)
1,000,000	181,019	0.17%	18.10%
3,000,000	313,534	0.30%	10.45%
10,000,000	572,433	0.54%	5.72%
30,000,000	991,483	0.94%	3.30%
100,000,000	1,810,193	1.71%	1.81%
134,217,728	2,097,152	1.56%	1.56%

Source: [EthHub](#)

## 5.7 Minimum Viable Security Spend

We still don't know what the "right" security spend is to reliably process transactions on blockchain networks. On one hand, it seems intuitive that ETH should remain at least as valuable as the sum of the assets stored on its network. The market capitalization of ERC-20s *has* eclipsed ETH market cap in the past, but never for very long. This feels like a buy signal even if it's an unnecessary long-term dynamic. (A platform's assets *should* be much more valuable in aggregate if that platform is any good.) The better question: Is there an implied minimum value of ETH to secure transaction flow?



## Ethereum vs Bitcoin Daily Transaction Volume

Due to the rise of stablecoins on Ethereum and Defi's blowout summer, Ethereum now transacts two times more value than Bitcoin daily



As of Sept 30, 2020 • Note: Ethereum includes stablecoins, but not other ERC-20s to prevent double counting from DEX volumes.  
Bitcoin includes USDT issued on Omni • Source: Messari, CoinMetrics

We can confidently say you'd be unlikely to secure a trillion dollar transaction network with \$100 of annual security spend. This year, ETH fees plus miner rewards will be closer to \$2 billion or ~0.2% of total network transaction flow—depending on your methodology for counting on-chain transactions... (it gets complicated). By comparison, Bitcoin's security spend is actually slightly *higher* than ETH's at 0.4% of on-chain transaction flow.

I'd imagine Ethereum could process 10x as much stablecoin volume as ETH-ETH volume in the future, and the network wouldn't be any less secure so long as ETH's implied security spend still captured network throughput fees. That's a bull case for ETH that no one seems to mention: could crypto dollar flows be a tail that wags the ETH? A skeptic might say "no." As interoperability between smart contract platforms improves and applications are built to least cost route across protocols, there will be pressure on the fees any given platform can charge.

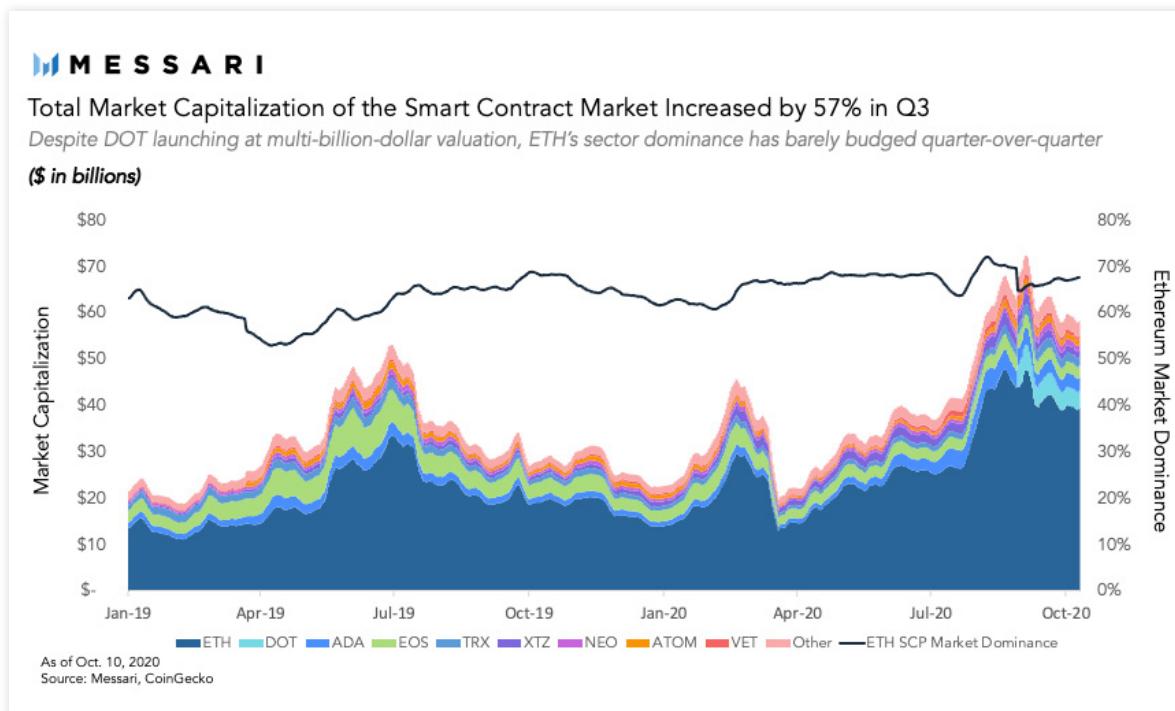
Maybe. I don't know, you probably want some basis points of security spend on real dollar flows.

## 5.8 Layer 1 Redundancies

Ethereum has such a tremendous infrastructure advantage vs. other Layer 1 projects today that it's hard to fathom competitors siphoning away material market share. But a 3-5 year head start doesn't strike me as insurmountable given that the eth1 to eth1.5+rollups migration isn't too dissimilar from bridging eth1 to an entirely new protocol like Cosmos, PolkaDot, Algorand, Cardano, etc. If you're forced to incur switching costs as an app developer or infrastructure provider, wouldn't you take the opportunity to broaden your protocol support, anyway?

For many, the answer will be "maybe," and layer 1's will likely leverage their massive treasuries and community funds to subsidize infrastructure work to turn those maybes to yesses. The opening for competitors to beg, borrow, and steal Ethereum users is now, in the early phases of the eth2 network upgrade, while gas costs on eth1 are outrageously high for certain apps.

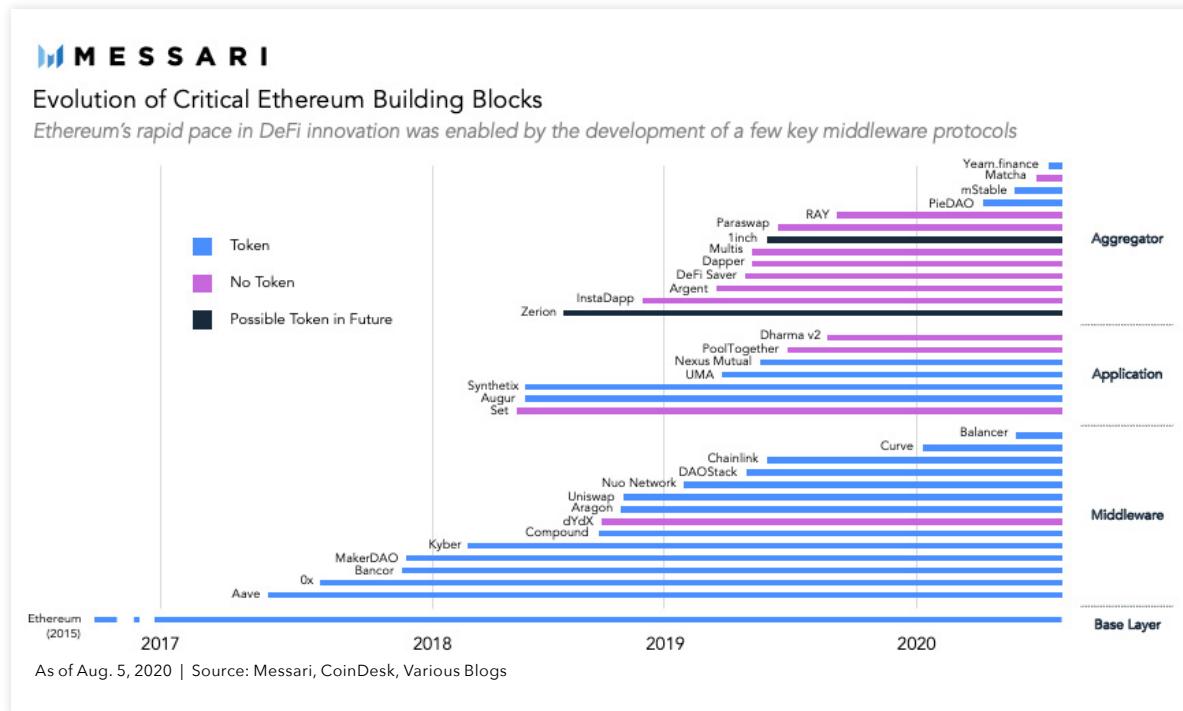
I hate to break your hearts, but given Ethereum's current dominance of the smart contract realm, and this report's length already, we'll stick with analysis of the smart contract platform market leader and gloss over platform by platform scoring.



For a look at how we think the other top 25 Layer 1 protocols like [Cosmos](#), [Cardano](#), and [Avalanche](#) will stack up, and how they've been growing their ecosystems, you can [subscribe to our Pro research](#). (Similar posts on PolkaDot, Algorand, and others are coming soon, as well.)

## 5.9 Layer 1 Specialization

I made the comment in May 2019 that ETH would likely end up being the DeFi chain (nailed it), as I was sure most DeFi applications would elect to build on Ethereum where all of the security spend was accumulating, and the money legos were getting battle-tested.



Liquidity begets liquidity in financial markets, and the yield framing / liquidity mining supercycle this summer (more on that next) provided Ethereum with even more fuel for its financial markets where high gas fees didn't necessarily dissuade users from sticking around and speculating.

That begs the question, "where will all of the non-DeFi applications live?" Will gambling stay on EOS and Tron? Will Flow prove to be an NFT lover's paradise? Will Hive or Steem build a mass market social application? Too early to tell, and for this report, the numbers are frankly too small to matter just yet. Again, [our Pro research](#) will help scratch that alpha itch for you if you're looking at the super early stage.

## 5.10 The Philosopher Kings

This was a meaty section, so I'll wrap up with a simple one: Vitalik remains Ethereum's core competitive advantage because I believe people want to follow him and believe in him, and because he built something that made a lot of people filthy rich.

I believe in the power of (non-denominational) immaculate conceptions in crypto and in philosopher-kings who make people wealthy. Bitcoin's birth and Satoshi's origin story was not replicable, but Ethereum's token sale, Yearn's "valueless token" launch, and Uniswap's retroactive airdrop may be the closest we've seen to bitcoin's immaculate launch in terms of their impact on attracting early religious community members. None of the other layer 1 founders can compete with Vitalik's celebrity persona or the original Ethereum launch.



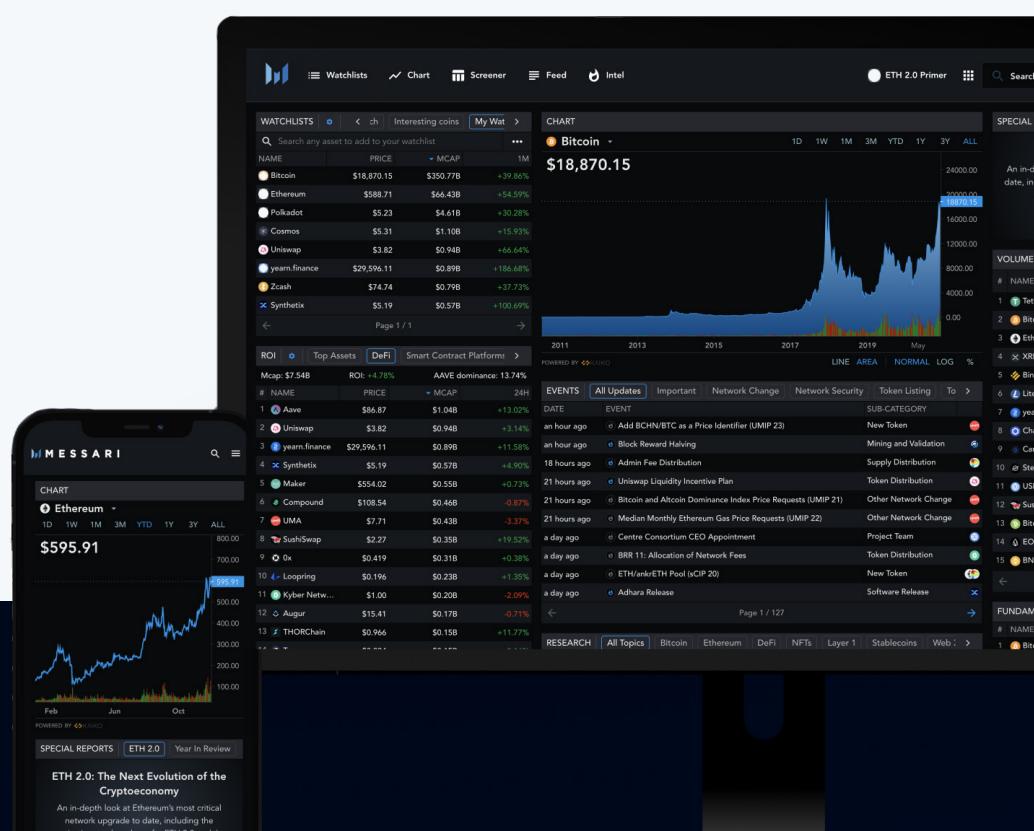
**Go Pro for 20% off**

Access our industry leading research and Pro data tools

*Offer code cannot be combined with other offers*

**USE OFFER CODE THESES2021**

**Start Your Free Trial**



# 6.0

## DeFi: Money Legos

In 2017, everything competed to be the winning “cryptocurrency.” In 2020, everyone has been clamoring to have their tokens classified as a “DeFi.”

Because words matter, our analysts developed a more rigorous definition for what we consider DeFi. Those protocols and their assets must satisfy the following requirements:

- Financial use: explicitly geared towards financial applications such as lending, exchange, derivative / synthetic asset issuance, asset management, etc.
- Permissionless: open-source; anyone can use or build on top of the projects without asking permission from a third party
- Pseudonymous: no need for people to reveal their identities to use the protocols
- Non-custodial: not reliant on third-party facilitators
- Decentralized governance: decisions and administrative privileges are not held by a single entity or a credible path exists towards removing them

It's helpful to provide counter-examples (what's not DeFi) before walking through the money lego evolution below. [Chainlink](#), a popular decentralized oracle is an important piece of data infrastructure, but it's more like middleware than financial plumbing. Similarly, smart contract platforms provide the rails that power DeFi, but aren't primarily focused on financial applications. Financial assets that serve primarily as “shadow securities” (e.g., crypto exchange tokens) aren't considered either. It's not a perfect categorization system, and Binance's [BNB](#) actually highlights the gray areas well given BNB can be used to secure the Binance Smart Chain, realize trading fee discounts on Binance, and reflect the exchange's revenue burns.

Under the stricter definition above, though, there were a lot of lego blocks added to the crypto toybox this year. We'll walk through each one of these primitives in plain English, then layer on some predictions for the year ahead. Mostly, we're here to help you make sense of this chart:

## Total Value Locked (USD) in DeFi

[TVL\(USD\)](#)

|

ETH

|

BTC

All | [1 Year](#)

|

90 Day

|

30 Day



DeFi is hardly a flash in the crypto pan. Its rebound this past month following a 75% correction, was ferocious in terms of both speed and liquidity (volumes). Still, the fledgling sector trades in aggregate at just a \$7 billion market cap, about equivalent to bitcoin also-ran BCH. My money is on DeFi rerating and continuing to rocket higher in the year ahead.

### 6.1 Maker's Fully Collateralized, On-Chain Bank

The first thing you need to build a parallel financial system is a stable digital currency whose purchasing power won't rise or fall 10% in a single day.

No one wants to spend currency they believe will be worth 10% more tomorrow, and no one wants to accept currency they think could be worth 10% less tomorrow. Same with credit. You don't want to borrow an asset that will be 10% more expensive to pay back because your effective interest rate skyrockets, and you don't want to lend an asset that might depreciate in value because your implied yield can go negative. With BTC and ETH, all transactions are inherently speculative because both parties agree to take principal risk with the underlying unit of account. Early centralized stablecoins, like Tether, were a temporary improvement, but came with the risk that the underlying bank deposits could be seized by the authorities.

We needed something entirely native to crypto protocols themselves. Enter [Dai](#).

A crypto-collateralized “peer-to-contract” lending platform called **Maker** launched in late 2017 to finally fix crypto’s volatility issue. With Maker, users could lock ETH in smart contract-enforced collateralized debt positions (now called “vaults”), and borrow newly created USD-pegged units called Dai against their holdings. The project created incentives for long-term ETH bulls to lever their long positions on-chain with Dai as the by-product.

So if you were an ETH whale with \$1 million worth of long exposure at the market top in January 2018 (right after MKR launched), and you wanted to cash in some chits to buy a new house, you could have done so without absorbing the huge capital gain that would have arisen from an outright sale of ETH: borrow \$500k against the \$1 million ETH position, pay interest into the Maker protocol, but no tax to the state. As long as your CDP maintained a 150% collateralization ratio, you were good.

The issue, of course, was that ETH tanked 90%+ from peak to trough in 2018. So people quickly saw the downside of leverage. That \$1 million long ETH CDP would have been liquidated (plus a fee) once the value of the collateral dropped to \$625k.

This was the sort of thing that led many skeptics (myself included) to believe Maker was fundamentally flawed, and would collapse during a drawdown. But miraculously, the system didn’t die in 2018. Nor did it die during the COVID panic-induced flash crash of March, when its liquidation protocol and emergency auction system mostly worked. **Mostly.**

Maker still has its critics (I’ll expand on the biggest critique in the next section on stablecoins), but now I think of the project as the industry’s most resilient and robust crypto-collateralized bank, and more importantly, the proof point that shows it may be possible for other on-chain stablecoin projects to create crypto dollars that help us avoid legacy banks entirely.

I like crypto protocols that refuse to die, and Maker fits that bill. Dai’s market cap rocketed 15x in 2020, largely thanks to DeFi. It will at least double again by the end of 2021 to \$2 billion, while other synthetic stablecoins join the competitive fray.

## 6.2 Uniswap’s Secure Exchange

Central limit order books (“CLOBs”), the backbone of modern crypto exchanges, aggregate bids and asks (limit orders) from market makers at various price points for various asset pairs. They generally work pretty well with centralized exchanges, but the CLOB model breaks down when it gets brought on-chain. The reasons are simple: every bid and ask, and every adjustment to those bids and asks, costs gas to store on-chain, and every order can theoretically get front-run since orders are prioritized by gas fees vs. timestamps. Some projects are working on layer 2 solutions to these issues with on-chain order books, but right now, just know it’s expensive to manage an order book on-chain.

**Uniswap** is a decentralized exchange that leverages an “automated market maker.” The concept was first proposed by Vitalik in late 2016, and pioneered by Bancor in mid-2017, but Uniswap brought it mainstream. AMMs solve the problem of maintaining a CLOB, by locking trading pair assets in “liquidity pools” rather than posting more ephemeral limit orders to a book. There are multiple flavors of AMMs today, but they all use something called a “constant function market maker” to price assets and ensure any order for any listed pair gets filled.

I’ll recommend a [series of \\*excellent\\* videos](#) that break this and other DeFi concepts down visually, but for now, just know the ETH-DAI pair on Uniswap holds equal amounts of ETH and DAI at a \$600:\$1 ratio. If there is a \$12,000 liquidity pool to trade against, that means that 10 ETH and 6,000 DAI are locked in the AMM.

The knock on AMMs used to be that they were only good for small orders. If you tried to execute a \$1,000 trade for ETH in a market with just \$12,000 in liquidity, you’d move the ETH price considerably, regardless of the centralized exchange-traded prices. Even with slippage, though, AMMs were a “zero to one” innovation that made it compelling to circumvent large exchanges. Not only for security reasons (self-custody), but for convenience and accessibility, too. AMMs don’t have as much compliance overhead for each market they support, and anyone can start a market for a new asset on Ethereum instantly—something that may make it impossible for centralized exchanges to beat them in terms of both availability and liquidity. AMMs are especially fast and convenient for listing on-chain synthetics, which we’ll discuss later.

I think about AMMs vs. CLOB exchanges the same way I think about BTC vs. global currencies. Bitcoin is a bad currency in relation to the U.S. dollar, but a very good currency compared to the Argentine Peso or Venezuelan Bolivar or Sudanese Pound. As bitcoin strengthens and other currencies inflate, it rises up the currency leaderboard. Likewise, Uniswap is a “bad exchange” compared to Binance and Coinbase (though even that is now somewhat arguable), but a very good exchange for long-tail assets and when compared to centralized exchanges outside of the top 50 by trading volumes. Soon, that will be the top 10 by volumes.

In the future, most liquidity for most markets will flow through decentralized exchanges, and AMMs will be a critical part of that story. Even better, AMMs ensure that retail investors will always have the opportunity to front-run institutions and VCs in crypto’s value creation game. Uniswap is likely to persist as a top 10 exchange. They only needed a spark to get going....

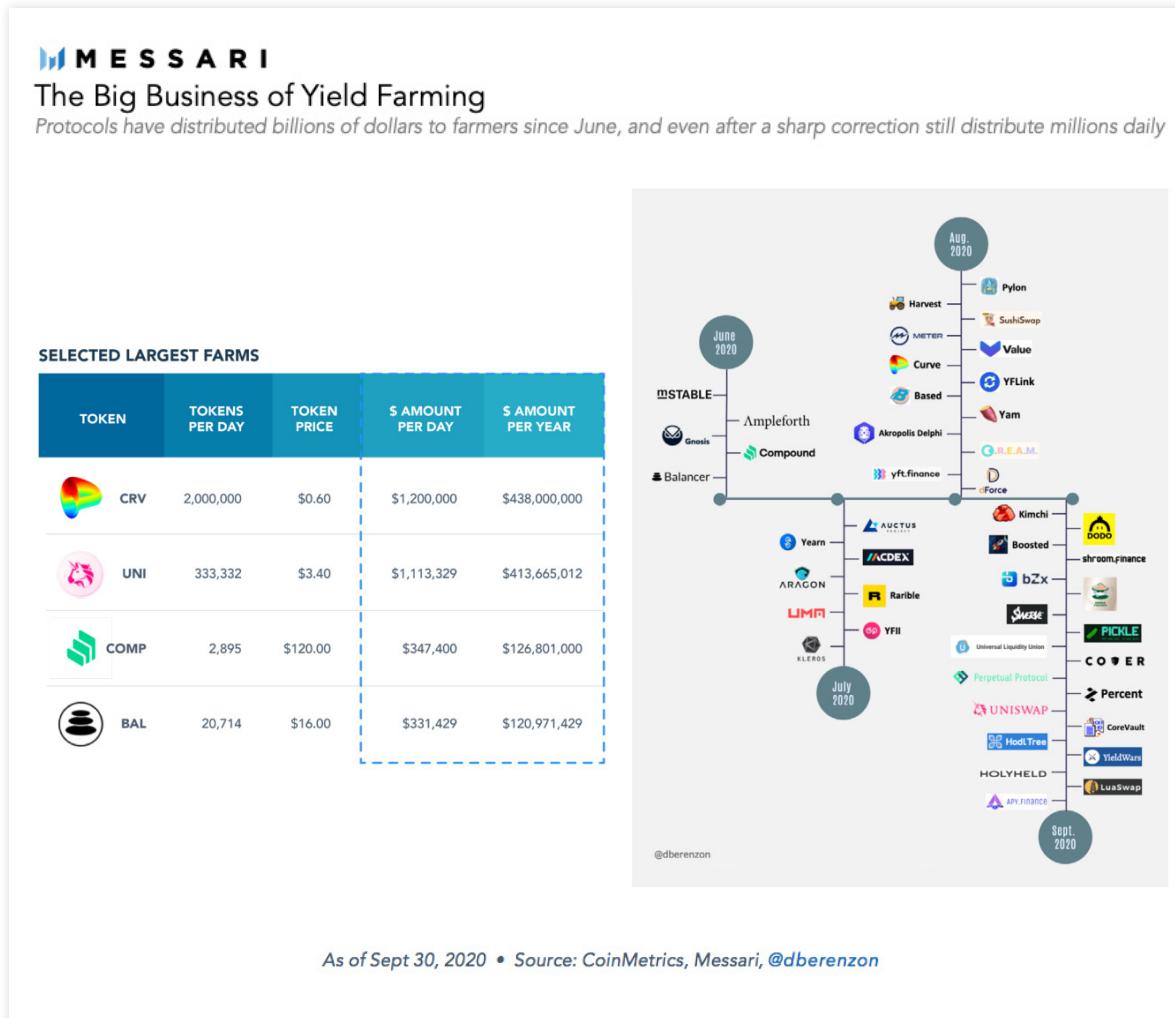
### 6.3 The Liquidity Mining Spark

In last year’s DeFi environment, there was Maker, and there was everyone else. Maker’s collateralized lending protocol was essentially the only game in town for borrowing against crypto holdings, and the protocol’s introduction of the Dai Savings Rate in November 2019 created one of crypto’s first and fastest-growing on-chain interest-bearing accounts.

But when [Compound](#) introduced “liquidity mining” this summer, they created a whole new game, and it set the entire DeFi sector aflame.

In most DeFi protocols, liquidity providers reap the lion’s share of system rewards. This makes sense: if you commit capital to make a market, you should earn maker fees. If you lend money, you should earn interest. But the issue is that it’s a sloowww process to build liquidity, and many would-be capital contributors may view the risk-adjusted returns they stand to generate in DeFi as insufficient—like picking up pennies in front of a steamroller.

Liquidity mining added a sweetener for early DeFi stakeholders, distributing tokens that conferred network governance rights (including the ability to extract marketplace fees from the protocol) to the capital contributors (“[yield farmers](#)”) who helped seed the early liquidity pools. Not only did liquidity mining juice deposits by orders of magnitude, it also turned DEX’s into capital cooperatives, and solved DeFi markets’ general “cold start” challenges. They distributed billions of dollars worth of liquid new tokens to network contributors over the summer.

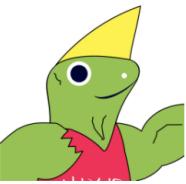


Liquidity mining is sort of like taking steroids. A couple of cycles may boost energy levels, but as a project, you'll still need to do the heavy lifting of building a useful and long-term viable marketplace and buzzing community. Otherwise, you'll end up worse off than when you started.

Uniswap and Compound demonstrated this perfectly. Compound deposits have grown 15x since its June launch, and its liquidity mining rewards will be distributed over the course of four years. Uniswap went with more of a cycled 'roids approach. Deposits corrected down 50% upon the expiry of its initial distribution cycle, but the early gains from the pump were obvious: Uniswap liquidity is **6x higher** than when it first launched the UNI token in August. With 80% of its max supply yet to be distributed, there is room for future cycles of liquidity mining steroids that help juice network participation and/or ward off competitive attacks.

This is how large treasuries should be used, but it's easier said than done to exercise restraint and plan liquidity mining cycles carefully, and grow slowly with the broader market. Interest revenue and market maker revenue are growing quickly today, but they're still small potatoes. Liquidity mining rewards should continue to help users speculate on the long-term size of their marketplaces, and help them get off zero.

Common sense caveat: you need people to believe in your network as a going concern in order to keep the yield farming game going. If liquidity mined governance tokens are fundamentally worthless, you can get headline APYs of 1,000%+ that last for an hour, and then turn negative as participants market dump. This has become the norm, which is why CoinGecko even built a **Degen mode**, the "if you're going to drink, I'd like you to do it here" of crypto dashboards.



## ⭐ DEGEN MODE: TOP (>1000%) YIELD FARMING POOLS BY RETURNS (APY)

- BRINGING YOU THE SPICIEST FARMS. USE AT YOUR OWN DISCRETION!  
- ONLY >1000% APY FARMS ARE SHOWN. NOTE THAT APY FIGURES ARE UNSTABLE ESTIMATES.  
- PROTOCOLS & CONTRACTS MAY BE UNAUDITED.  
- THERE WILL BE EXPOSURE TO SMART CONTRACT AND MARKET RISKS.  
- PLEASE REMEMBER TO EXERCISE CAUTION, EVALUATE THE RISK, AND DO YOUR OWN RESEARCH PRIOR TO FARMING!

OVERVIEW	MARKET CAP	IMPERMANENT LOSS CALCULATOR	APY CALCULATOR	DEGEN	Search...			
#	ASSET	POOL	AUDITS	COLLATERAL	IL RISK	VALUE LOCKED	RETURNS(ESTIMATED)	
48	DAO (DEA)	DEUS/DEA	N/A	DEUS	DEA	N/A	\$1,690,229.30	4219.97% YEARLY 0.48% HOURLY
91	AZUKI (AZUKI)	WETH/AZUKI	N/A	WETH	AZUKI	N/A	\$532,844.79	1218.44% YEARLY 0.14% HOURLY

Source: CoinGecko

Shenanigans like these are one of the reasons you hear about DeFi “Blue Chips,” networks where communities seem to be rallying around long-term viable projects, even as most still dabble in the degen casino. I coined the term “UNEASYs” (or stole it, I can’t remember) for Uniswap, Nexus Mutual, Ethereum, Aave, Synthetix, and YFI. Add Maker and Curve to the mix, and you’ve captured all of the **top protocols** by locked value today.

When I say I expect DeFi assets to re-rate 3-5x higher (in BTC terms) in the next market cycle, I’m talking about the “Blue Chips,” not Azuki.

## 6.4 Dynamic Automated Market Makers

Uniswap **proved the AMM model could work**, and liquidity mining proved that it could scale. What came next was a predictable set of iterations on top of the lower level lego blocks.

Uniswap AMMs are not without their issues. They’re capital intensive, since they require balances of two tokens to maintain a constant product. (For mathletes,  $X^*Y = K$  where Token Balance X \* Token Balance Y should always equal K.) They are also subject to something called “impermanent loss” where high market volatility creates imbalances in the AMMs vs. reference market prices and causes liquidity providers to lose money to arbitrageurs: less liquid **Uniswap pairs** can gap up or down vs. **Binance pairs**, and bots arb the spreads. Impermanent losses can often become permanent and offset the fees a market maker might otherwise earn.

So fixing that is important, and it became obvious some AMM functions could be tweaked to reduce capital intensity and protect the market makers underpinning the DeFi markets. Two particularly important upgrades to AMMs were brought to market from Balancer and Curve, and further iterated upon by AMM OG, Bancor.

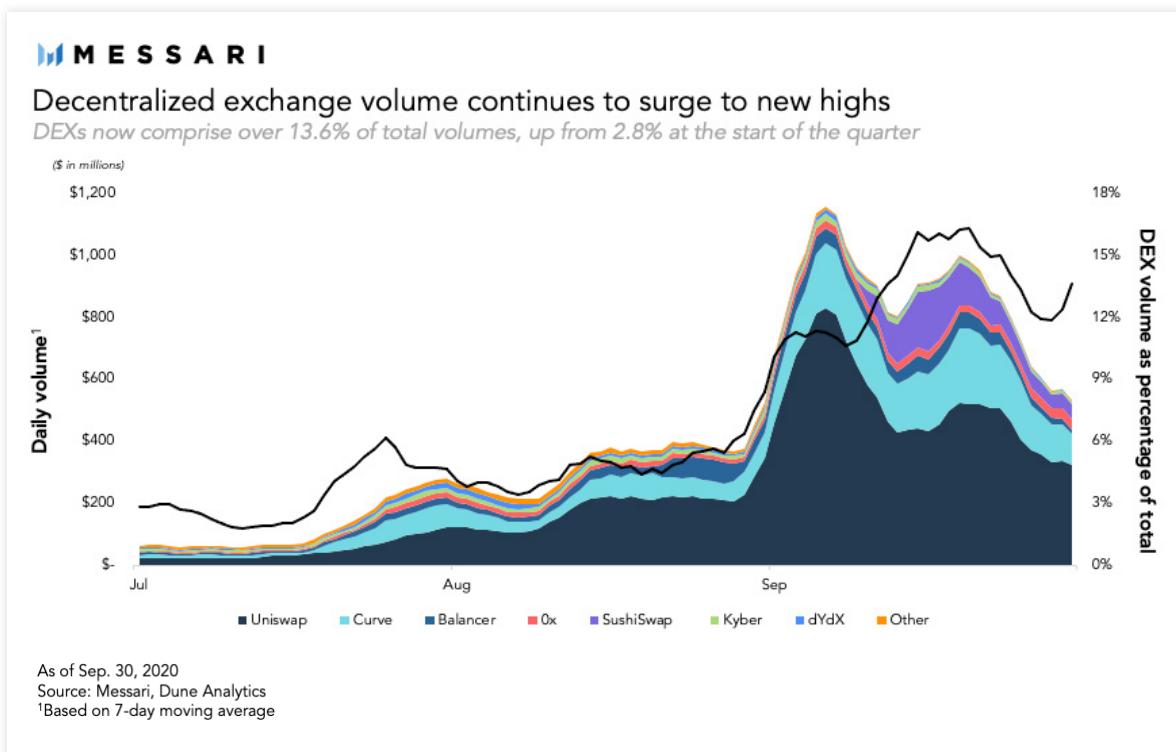
**Balancer** generalized the idea of a constant product market maker, making it easier to pool multiple assets in the same omnibus liquidity pools and reduce the probability of impermanent loss to arbitrageurs in high volatility environments (crypto’s default state). Instead of provisioning liquidity to the ETH-DAI, BAL-USDC, CRV-DAI, and BAT-ETH pools on Uniswap, Balancer liquidity providers could add ETH, DAI, BAL, BAT, and USDC to the same pool, allowing the same collateral to cross multiple market pairs.

**Bancor** introduced the v2 of its AMM with an emphasis on more liquid crypto trading pairs. It uses data oracles to dynamically rebalance its pools whenever they move out of whack with off-chain markets. Those upgrades could improve capital efficiency by 20x (per the team), but it comes with the risks that reliance on off-chain oracle data introduces to the equation.

**Curve** may be the most exciting new AMM to come to market. The protocol started with the realization that they could tighten parameters for trading pairs in which spreads were predictably lower: like-kind stablecoin to stablecoin transactions, and pegged assets such

as renBTC to wBTC. Curve made USDC, USDT, Dai markets 10x more liquid for DeFi, though they introduced risks in warehousing multiple types of idiosyncratic stablecoin risk in the same trading pools (if one stablecoin loses its peg, the whole system breaks). CRV was one of the most critical innovations of the year, and the importance of scaling liquidity for like-asset trading pairs will become even more obvious as platform interoperability (bridges to eth1.5+rollup chains and to layer 1 alternative wrapped assets) becomes a major trend in 2021.

There's already been some unbundling of Uniswap, as each AMM protocol provides their own liquidity mined token incentives, and aims to tighten spreads and improve the quality and strength of the DEX ecosystem vs. its centralized competitors.



**DEX market share**, and AMM protocol's market share in particular, will 2x again this year to a sustainable 2% of total global volumes, which sounds small only because the institution-driven rally for BTC and ETH will happen on traditional venues. For ERC-20s below \$100 million in market cap, DEX market share will climb to 10%. And for ERC-20 microcaps, DEX's will extend their early lead as the only market makers in town.

## 6.5 Smart Vaults

"Man, we really need, like, a Wealthfront for DeFi," said a man named Andre.

**Yearn.Finance** takes the cake as the top DeFi protocol of the year for [how it brought together](#) all of DeFi's unique lego blocks—and added some of its own. Yearn's predecessor, iEarn, started as an interest rate optimizer that developer Andre Cronje used to dynamically allocate his assets across various DeFi lending protocols according to the highest daily yield. As Cronje's suite of products expanded, he began to bucket everything under the Yearn. Finance brand, and introduced a "[completely valueless](#)" governance token called YFI to set the system parameters, and capture a portion of the fees generated by the network's various "smart vaults."

Yearn's asset management platform now manages \$450+ million and provides liquidity to AMMs (Uniswap, Curve, Balancer), lenders (Compound, Aave, dydx), and insurance pools (Nexus Mutual). It also may have a solution to the stablecoin scalability challenge via its [StableCredit](#) system, which combines elements of MakerDAO, Uniswap, Bancor, and Aave. I can't write anything about YFI without Andre making it obsolete in four days, but we'll continue to cover the protocol's torrid pace of new developments and integrations in [Messari Pro](#). (In the meantime, you can [watch this video](#) to understand how Yearn's vaults work under the hood.)

Yearn is for the lazy (get DeFi's yields and farmed rewards, but outsource the management for a performance fee), the entrepreneurial ("strategy creators" get rewarded for introducing new programmatic investment strategies that power each yVault), and the risk-averse (I just want a little yield and to minimize my gas fees and risks of total principal loss). And YFI is the token to own if you want a bet that expresses the thesis that a "Wealthfront for DeFi" will be a big prize.



**Go Pro for 20% off**

Access our industry leading research and  
Pro data tools

USE OFFER CODE **THESES2021**

[Start Your Free Trial](#)

Offer code cannot be combined with other offers

## 6.6 Unsecured Credit & Flash Loans

One of the most interesting new DeFi primitives is the “flash loan” where a user can borrow an asset, deploy the asset in a transaction, and then repay the loan as part of a single multi-step transaction. Flash loans can be used for arbitrage (programmatically exploiting price inefficiencies between various DEX’s within single blocks), collateral swaps (replace collateral in underlying loans without repaying the loan), and “self-liquidations” (can be thought of as DeFi refinancings without triggering taxable events), plus myriad potential future applications.

They make it possible to exploit inefficiencies with little to no working capital (besides gas fees), which makes DeFi more liquid. And their role in several DeFi exploits “is actually good news” that helps build system wide anti-fragility.

Flash loans are basically a series of sequential database entries that execute only if all of the entries can get processed in a single batched transaction (block). [Aave](#) is one of the initial originators of flash loans (dydx does ‘em too), and it charges a nine basis point origination fee for going to the trouble of providing borrowers with ephemeral liquidity. (Again, Finematics has the top [explainer video](#) on how these work.) Aave issued \$25 million in loans through the first six months of 2020, then \$500 million in Q3. They did another \$500 million in October and November. Not bad for year one.



Source: [Aavewatch](#)

Even if DeFi assets trade sideways in 2021, flash lending will increase 5x to \$5 billion in new originations as more white hat arbitrageurs and black hat market manipulators use the primitive to exploit DeFi market weaknesses. I’m 51% confident flash loans will be responsible for completely crippling at least one of DeFi’s top 10 projects in 2021. And they’ll likely have a partner in that exploit: bad data oracles.

## 6.7 Crypto's Data Middleware: Oracles

With Bitcoin, there is no reliance on any external data. Bitcoin transactions are native to the bitcoin blockchain, and the protocol is blissfully unaware and unconcerned with the world outside of its ledger and network of nodes. But how does [Augur](#) settle an on-chain sports bet, or MakerDAO liquidate an undercollateralized CDP based on an ETH price drop?

They use [oracles](#), middleware that connects blockchains to off-chain data sources.

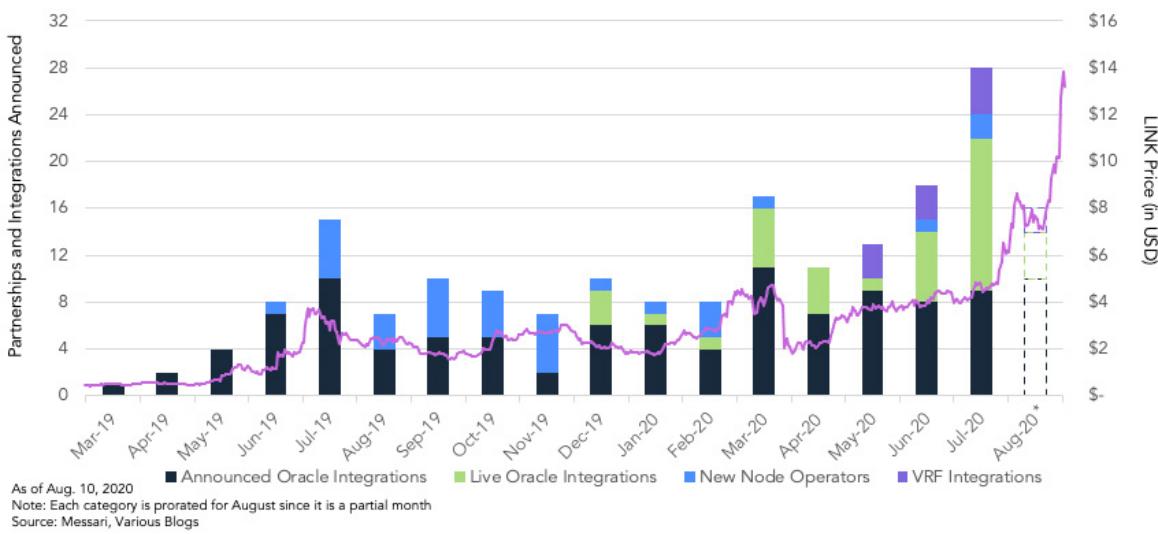
Augur's REP uses a "designated reporter" system that rewards oracles for providing accurate information on real world events, and allows for a dispute arbitration process whenever results include some sort of subjective interpretation. That's good for bets where lengthy settlement times are acceptable, but DeFi applications require more timely and continuous data to power markets 24/7. If you're building synthetic tokens that aim to provide exposure to something like a specific stock's price, you'll need a data oracle that spits out reliable reference prices for that stock. Even if you're pulling from other on-chain data sources (e.g., Uniswap exchange rates), you still need to manage risks associated with market manipulation (e.g., using a flash loan to blow up an illiquid market pair's exchange rate).

[Chainlink](#) curates feeds from multiple data resources, and serves as a critical data translator without introducing trusted third parties into crypto transactions. They make it more difficult and expensive to manipulate reference data. [We don't consider](#) Chainlink "DeFi" per se, but it's an important project given most DeFi exploits have had to do with bad reference data infrastructure and risk controls, and most protocol builders learn the hard way that it's tougher than it looks to maintain reliable oracles.

Chainlink has become the leading project most think of when they hear about oracles given the project's hundreds of integrations with crypto projects, and its ability to market the shit out every new partner it onboard, including layer 1 platforms like Harmony and NEAR, and many of the DeFi darlings listed above. There are other "decentralized oracle network" projects ([we've written about them](#)), but Chainlink has become the de facto choice for teams looking to outsource oracles, and it's hard to ignore the sixth largest asset by market cap.

## Monthly Chainlink Partnership and Oracle Integration Announcements

*Chainlink's growing integration pipeline has fueled LINK's meteoric rise over the last 18 months*



That's not to say I've been able to wrap my head around how LINK is traded as an asset: it's currently at \$5 billion in liquid float, with 60% of the remaining supply held in reserves to incentivize partners and capitalize the protocol's core contributors. It's in many respects a smaller (but still massive) version of XRP with respect to how it has traded and been marketed.

Zeus Capital, an anonymous short-selling research firm, wrote a widely circulated "exposé" on Chainlink earlier this year; 59 pages eviscerating the protocol, and its primary stakeholder, SmartContract, Inc. I won't link to the report because some of the conclusions were spurious, and some of the accusations bordered on libel. But the report did have a couple of substantive points. Namely, around Chainlink's broken [LINK economics](#).

Today, LINK is merely a "payment token." In other words, it's competing to be valued like commodity money you must hold to host oracle nodes and/or pay for reference data contract calls. But like most 2017 "utility token" projects, there's no reason to hold LINK for any period of time: if you really need LINK for payments, you can hold other more liquid "monies" and hop in and out of the less useful, less liquid payment token as needed. When it comes to staking LINK for network security, the issue is that ChainLink's fee model doesn't seem stable or scalable. Fees have been proposed, but not yet implemented on a per transaction basis, as any introduction of per call data fees would make usage prohibitively expensive.

I have a tough time backing into any model where the market for reference data contract calls amounts to a \$10 billion market. If you want a bull case: [here, I guess](#). I'm not a LINK bull.

## 6.8 Vampire Attacks: Legal Theft

The best and worst part about building in DeFi is that everything is open-source. It's fair game for a competitor to fork your code, drink your milkshake, and laugh at you while they do it.

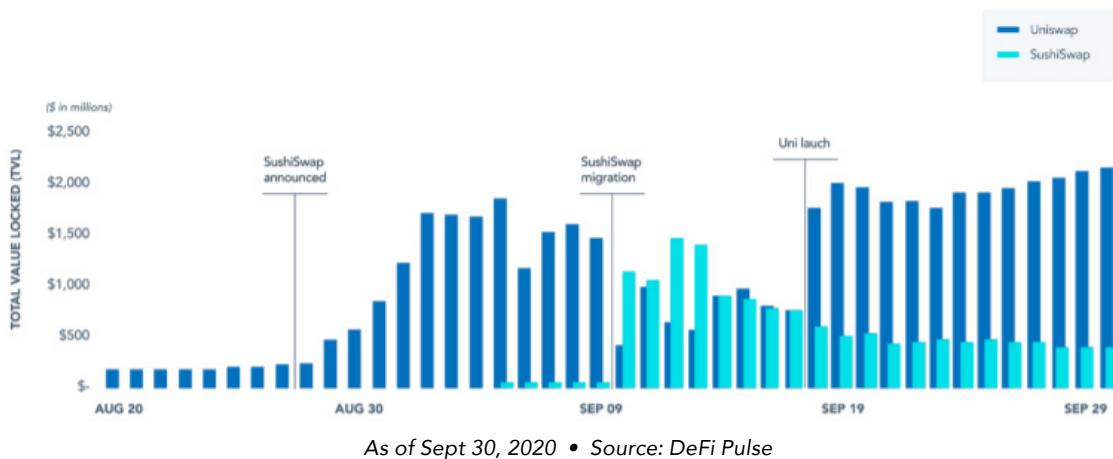
DeFi is not for the faint-hearted, and this summer, we saw some of the best and worst of what the industry has to offer. SushiSwap launched a [shameless fork](#) of Uniswap with a liquidity mining rewards program [aimed at enticing Uniswap liquidity providers](#) to defect to the new anonymously-released rival. An anonymous developer got the beat on Curve, finding the project's unlaunched token contract in its github repo, and launching the contracts themselves. Then [someone forked Curve with Swerve](#). Compound teamed up with the "vampires" at Cream because they viewed the new project as a complement acting in good faith: Cream supported a wider range of DeFi assets, crossed to new blockchains like Binance Smart Chain, and shared 2.5% of their supply with the "victims" at Compound.

Many vampires return to their graves rather quickly once they run out of speculator blood to drink (rug pulls!), but others remain (including, surprisingly, [projects like SushiSwap](#)), which [seem to be resurging](#), as they implement new, interesting features, and partnerships. (YFI's [fifth partner this week](#).)



### Total Value Locked in Uniswap vs. SushiSwap

After a seemingly successful "Vampire attack" SushiSwap has failed to retain liquidity compared to its predecessor



As of Sept 30, 2020 • Source: DeFi Pulse

There are benefits to vampire attacks. If capitalism is all about creative destruction, then DeFi capitalism is all about rentier destruction. A first mover network advantage no longer leads to a monopoly, but a temporary advantage that can be maintained only with legitimate commitments to community governance and fair (and early) stakeholder alignment.

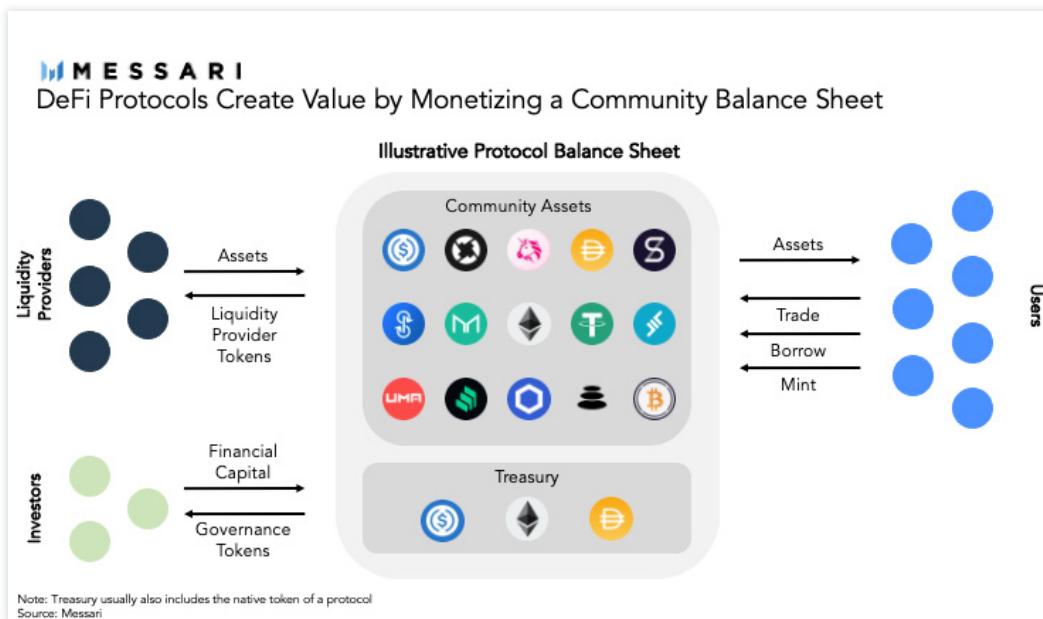
The primary vampire attacks we'll see in 2020 will come from "tokenless" projects that attempt to leapfrog their competitors by beating them to market with new token offerings. Wallets like Metamask seem like prime candidates to roll out a token if for no other reason than they will need to do so or watch competitors siphon users with token incentives of their

own. This happened originally with Binance and BNB. It happened again with Compound et al. with the yield farming boom. I say it happens with wallets (Zapper!) and self-custodial services next year.

There are [other ways to build defensibility](#) in DeFi. Branding, integrations, usability, goodwill, partnerships, good security are all important. But a sound treasury strategy is critical.

## 6.9 Treasury Governors

[Uniswap](#) showed you could build a phenomenal product, lots of community goodwill, and do everything right, but *still* get threatened by a motivated party willing to better split platform economics with users. Treasury governance and protocol politics are high stakes operations in DeFi with \$6 billion in community-governed tokens, and now hundreds of millions of dollars' worth of treasury assets.



How should these assets get managed?

In general, most networks have been remitting cash rewards back to their investors fairly automatically through "dividends" or token burns (same as the corporate buybacks, but not really), but it seems smarter to use funds to incentivize core developers first (execs), then long-term capital providers (board), then community contributors (team), well before the mercenaries (hedge funds). This should be obvious, but 2020 incentives still tend to outweigh mercenary capital at the expense of the other (more important) stakeholders.

That will change.

I'm most interested to watch the evolution of [PowerPool's CVP](#) (the "concentrated voting power" token, basically a proxy service for accumulating DeFi voting power) and Aragon (the original DAO manager) because there is a LOT of money on the line. It's not just governing monetary policy and protocol parameter changes, either; we're going to see more in the realm of [protocol M&A](#)

in 2021, something I predicted in [last year's report](#), and which has really picked up steam in Q4. (Aragon, Voyager, Harvest, and of course, YFI have been active here early.)

## 6.10 DeFi Bug Bounties

The list of DeFi exploits is long and growing, and many entrepreneurs seem content to make the same mistakes repeatedly in favor of rushing new releases. The good news is that this serves as a bounty program of sorts that reduces the risk DeFi will ever get "too big to fail."

In fact, one lending platform, [bZx](#), even offers bug-bounties-as-a-service. The team ran two hacking competitions in February 2020 (\$1 million in total), an initial DEX hack in July (\$550k), and a nice meaty \$8 million hack competition in September. I'm excited for the next one.

There's work being done to contain the potential damage posed by risky and untested DeFi applications. We're starting to get better at predicting the most likely attack vectors (oracle attacks plus flash loans being the typical 1-2 punch), and there are now tools to score risk per project. ConsenSys CodeFi launched a [Defi Risk score](#), and security researcher Gauntlet launched an [economic safety score with DeFi Pulse](#). That will help better price the \$100 million in smart contract insurance policies that exist today via Nexus Mutual, Opyn, and (soon) Cozy Finance. That should help de-risk the process of going "bankless."

ADVERTISEMENT

# Where Crypto Enters Finance

Bitstamp is the longest-running global cryptocurrency exchange. Since 2011, we've earned the trust of over four million customers and leading financial institutions.

## Leaders in Liquidity

Trade with low slippage and spreads, connect to real-time settlement networks and move funds instantly

## Institutional-Grade Trading Suite

Fastest APIs in crypto, efficient order execution ensured by matching engine from Nasdaq



[GET STARTED AT BITSTAMP.NET/PRO](#)

## Trade with Peace of Mind

Advanced custody and insurance coverage, 24/7 support with a human touch

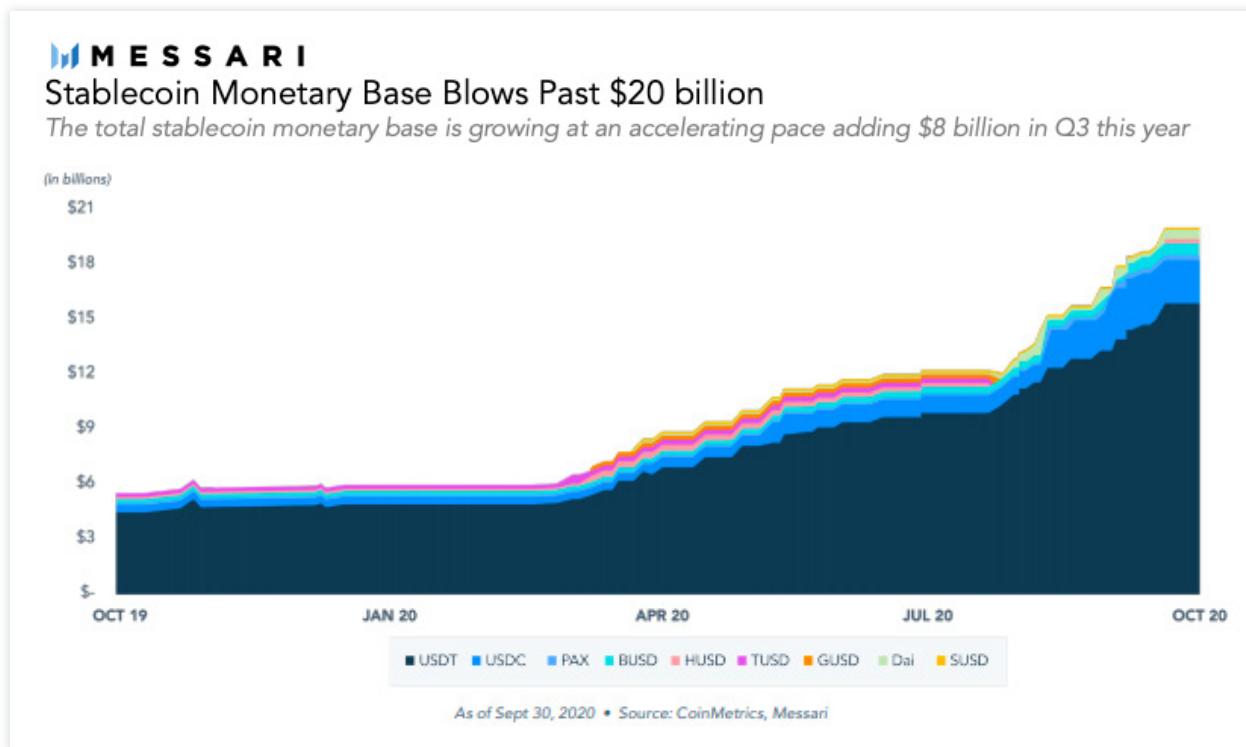


**Bitstamp**

# 7.0

## Stablecoins are Eating the (Crypto) World

The market for crypto dollars was nuts this year, and shows no signs of leveling off in 2021. Tether's supply expanded by 4x, USDC's by 6x, and PAX / bUSD / hUSD by 5x. Dai went full send, swelling by 15x and crossing the \$1 billion threshold, thanks to the DeFi boom.



Inter-exchange settlement may have been the dominant initial use case for stablecoins, but in 2020, crypto lending (on-chain and OTC) entered the chat. It's not just about liquidity and stable reserves anymore, either. Today's investors can earn structurally higher yields in crypto lending than in legacy markets, and many have gotten comfortable enough with crypto's idiosyncratic risks to feel it's a screaming buy to move "real" dollars into crypto dollars.

The proliferation of different types of stablecoins presents tradeoffs: availability, stability, censorship resistance. Pick two out of three.

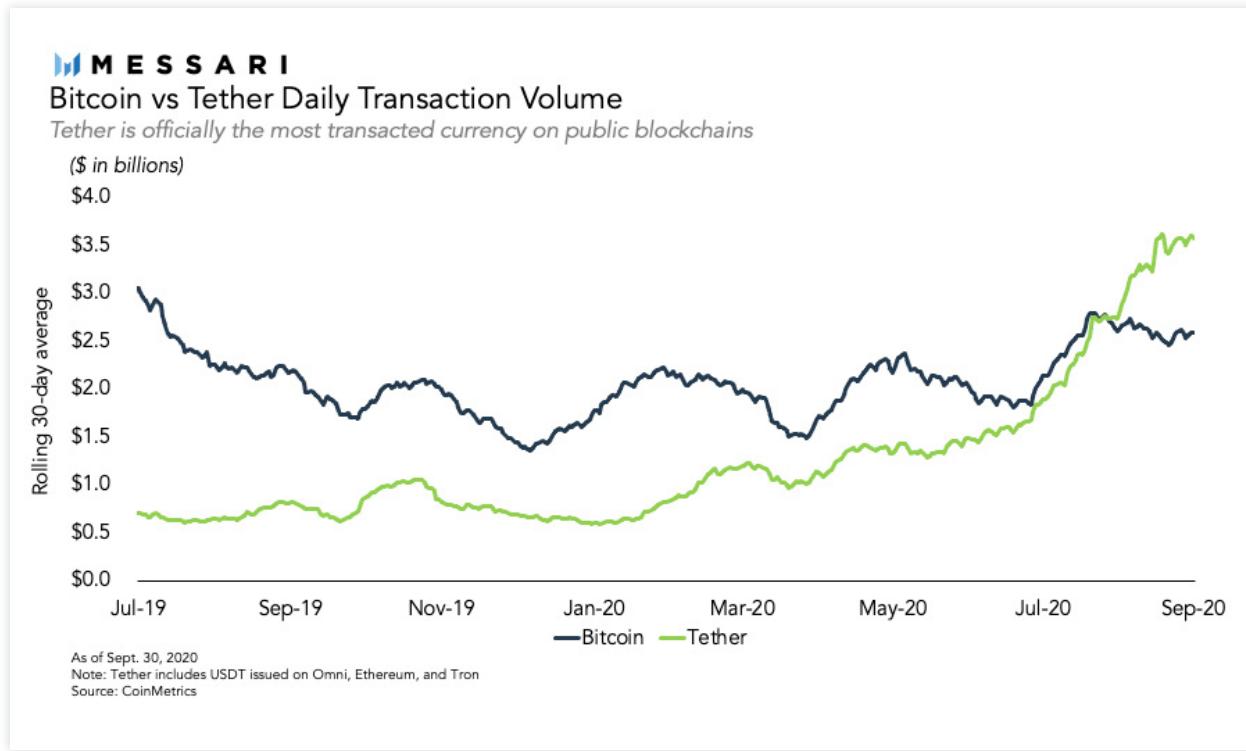
You can use the semi-censorship-resistant Tether for its liquidity, but you take the chance its centrally managed custodial accounts get seized at some point. You can use the fast-growing “regulated” stablecoins like USDC and trust in their long-term availability and liquidity, but run the risk certain activities and addresses get blacklisted by the currency’s regulated maintainers. Or you can use the algorithmically generated Dai and deal with smart contract risks, black swan liquidation risks, and the **regular deviation** of Dai from its dollar peg.



There are so many flavors of stablecoins to choose from, and Castle Island Ventures had an excellent primer on them to pair with Watkins’s **quarterly sector coverage**. I didn’t have “pumped for crypto dollars” on my 2020 BINGO card, but here we are.

## 7.1 USDT: Crypto's Biggest Threat

Like bitcoin, Tether should have died a long time ago, but rudely refuses.



As you read this, USDT (collectively on Omni, Ethereum, Tron, EOS, Algorand, and Liquid blockchains) is sitting at north of \$20 billion in circulating supply, despite issues from its affiliate Bitfinex, which has been embroiled in a [fraud dispute](#) involving Tether with the New York State Attorney General's office since April 2019. Bitfinex is also (allegedly) headquartered in Hong Kong, where [registration with regulators](#) will no longer be optional. Despite the legal issues, Tether grew a modest \$15 billion this year, more than 4x where it started.

Tether's high-profile battle is a gray swan event hiding in plain sight. Its bank accounts have already been frozen in the past, so future incidents wouldn't exactly be unprecedented. Still, barring meaningful developments in the [case in New York](#), Tether's de facto boosters (major global crypto exchanges) are likely to gloss over the currency's risks in the absence of obvious replacements to the near-universally accepted dollar-denominated reserve.

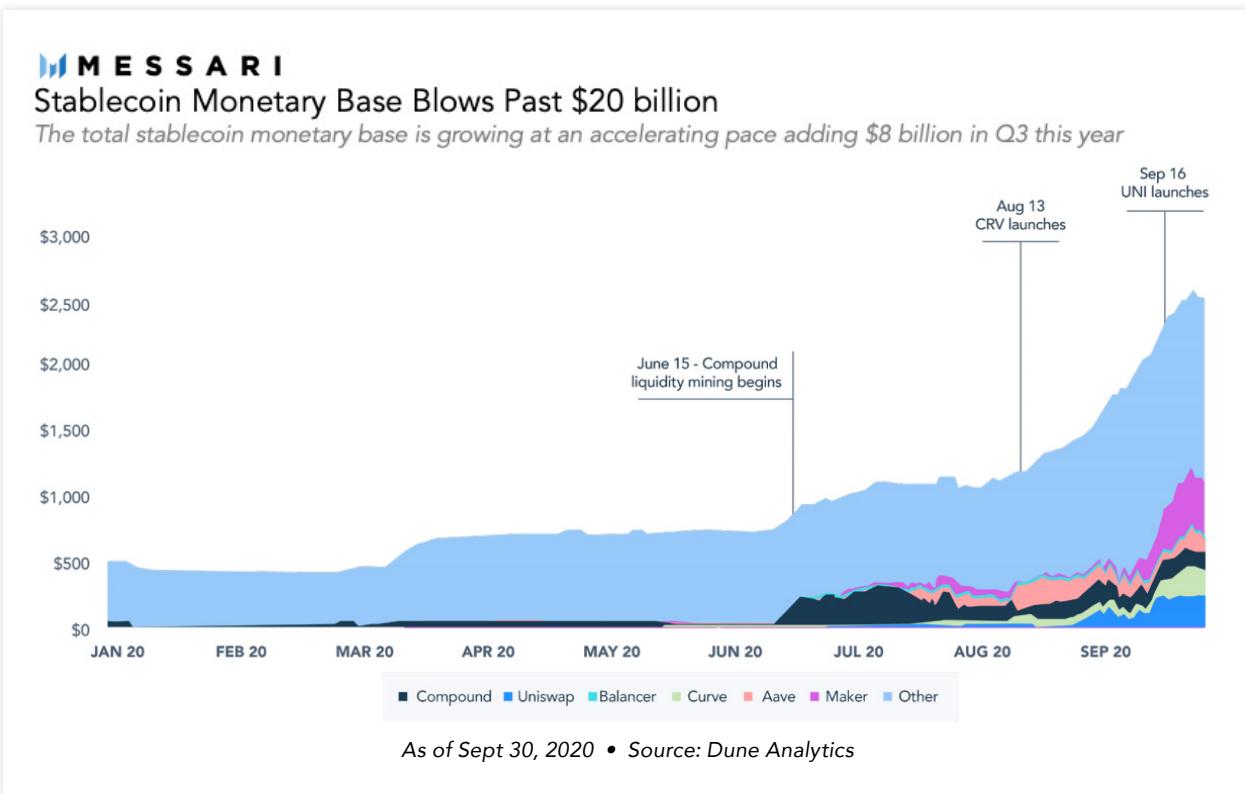
The muted market impact of the dual CFTC and DoJ lawsuits against BitMEX and the orderly rotation out of BitMEX to alternative venues may have lulled some to conclude the worst case scenario issues with Tether would spark a similar orderly move into other stablecoins. But it's one thing to send money from one platform's perpetual contracts to another's. It's quite another to port seized dollar reserves to new banks.

I recommend reading my full overview of Bitfinex/Tether from last year's [theses](#) (p. 28) for a more detailed understanding of how insane it is that Tether hasn't died yet. Tether will either have an existential crisis or double its supply again in 2021. There doesn't seem to be a middle ground.

## 7.2 USDC: The Multichain Stablecoin

Let's say Tether's issues do finally catch up to them, and spark a gradual, orderly migration into other crypto dollars. [USDC](#) is the most likely crypto dollar to capitalize on that rotation after a banner 2021, where deposits swelled 6x.

USDC co-creator Circle [raised \\$25 million](#) in partnership with Genesis Capital to bring better liquidity to the regulated crypto dollar markets and take advantage of booming demand in crypto lending. And you can see why: nearly a billion dollars of USDC was created to satisfy the hockey stick growth in DeFi demand.



The project was also given a blessing by regulators via the OCC's interpretive letter on banking support for stablecoin issuers, which drastically lowered perceived regulatory risk vs. its larger, shadowy competitor, and fueled USDC's boom in exchange support, and [cross-blockchain support](#) with blockchains like Algorand, Stellar, and Solana (more to come in 2021). And right before the closing edit bell, Visa is integrating USDC!

USDC was even used to [circumvent the Maduro government](#) in Venezuela and help the U.S. provide relief to the hyperinflation-stricken country. This is great for Venezuela! It's also great for crypto's perceived legitimacy and utility! But does the government even realize that they've inadvertently signaled how useful crypto dollars could be to route around dollar-dependent banking? I don't think they understand the symbolic implications, even if USDC itself proves to be a tightly regulated, surveilled, and censorable crypto dollar. The cat's out of the bag.

### 7.3 PAX: The PayPal Stablecoin?

I have admittedly paid little attention to Paxos in recent years, as it's felt like a bit of an also-ran in many of crypto's most important battles...exchange, custody, and stablecoin issuance. Perhaps that oversight was premature. They caught my attention with two major custodial partnership announcements this year: first with [European fintech Revolut](#), then with the year's biggest prize, [a partnership with PayPal](#) on its crypto roll-out. After a little digging, I realized Paxos was also a custody partner for the other large exchange-issued currencies, [bUSD](#) from Binance and [hUSD](#) from Huobi.

Shame on me for missing this. Everything now clicks.

Partnerships may or may not lead to an explosion of [PAX](#) supply in the regulated crypto fintech markets. Mid-tier fintechs, like Revolut, may default to using PAX, but others, like PayPal, will go the Huobi and Binance route instead. Partnering with Paxos to launch palUSD crypto dollars gives you a head start vs. completely rolling your own from scratch.

There's a strong case for PayPal to acquire Paxos as it rolls out its crypto suite. My money would be on a 2021 acquisition, if not for the fact that a) Paxos is one of those companies (like Gemini) with no founder urgency to sell, and b) there are other more available targets like [BitGo](#). China has DCEP. The U.S. will have a proliferation of non-bank financial crypto dollars years before we ever see an iota of progress on a similar scale central-bank digital currency.

### 7.4 Dai

As our new President-elect might say, Dai is a big f\*cking deal. But can it scale?

There's some debate on this. The issue comes down to a wrinkle in the Maker protocol that makes it difficult or impossible for arbitrageurs to reduce Dai spreads during periods in which it breaks from its peg. I tend to think Dai will continue to scale slowly, but it is held in check by its reliance on ETH-based collateralized debt positions. Let's look at why.

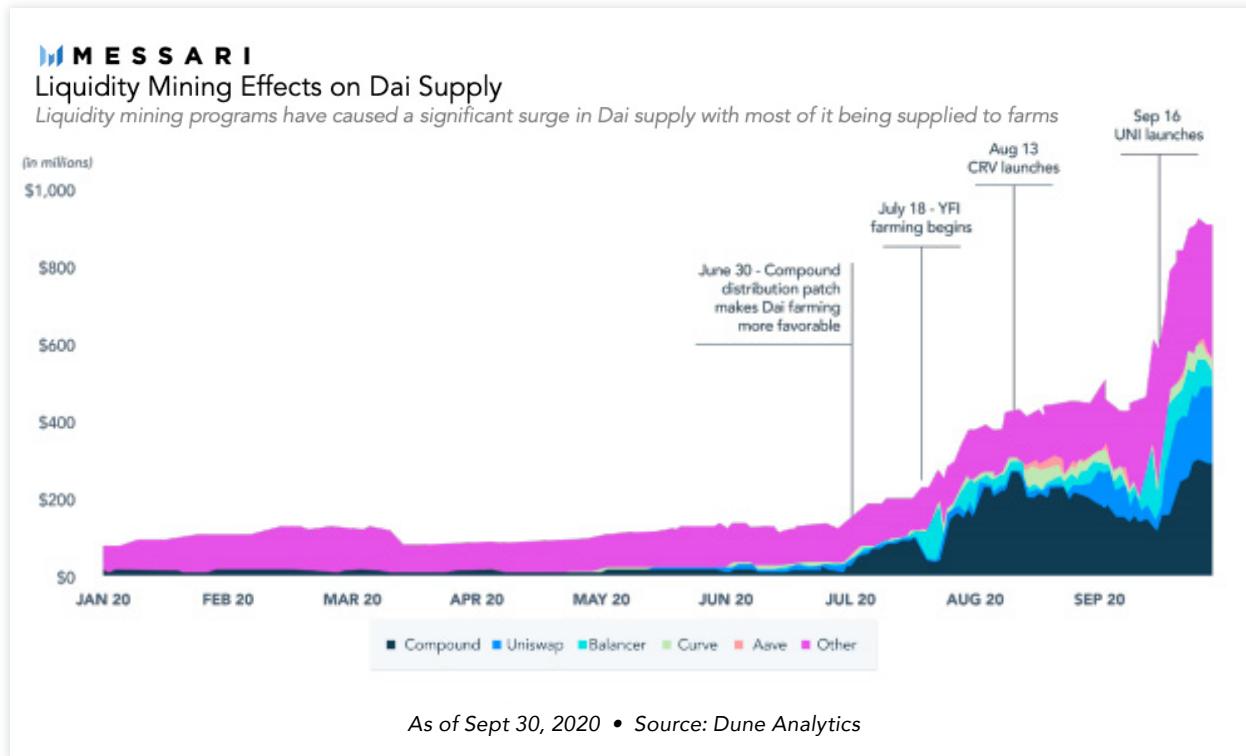
With Tether, an arbitrageur could see USDT at \$1.02, send \$1.00 to Tether, Inc. to create new USDT, then liquidate their position for \$1.02 of actual dollars (or another dollar equivalent) on

a crypto exchange. Or they could see USDT trading at \$0.98, market buy it on exchange, and redeem at Tether for \$1.00 of cash. There's risk around Tether and its creation / redemption process as a centralized entity, but the arbitrage 101 play has generally worked.

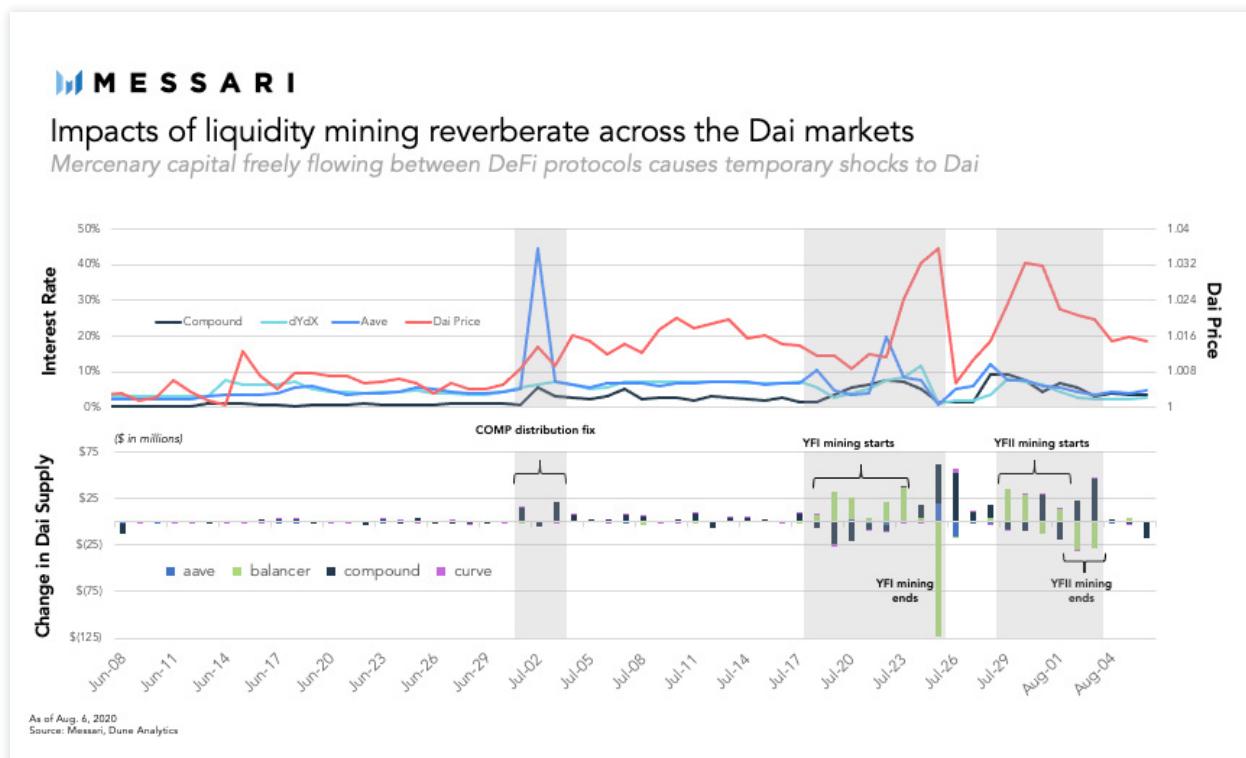
With Maker, things aren't so simple. Market demand can push DAI to \$1.02, but it will cost more than \$1 to create a new DAI given the protocol's algorithmically defined collateralization ratio, which is 150% for ETH. That means you can only create DAI if a) you are already net long ETH in a big way (otherwise your borrowing costs would eclipse your arb opportunity); b) the arbitrage opportunity on DAI is more lucrative than yield you could generate from collateralizing ETH elsewhere; and c) you believe you can profitably close the CDP later on when the price reverts to the peg, and you buy back DAI for less than you paid). Lotta ifs.

Most demand should flow to other stablecoins when Dai trades at a premium because of this dynamic. Dai has a first-mover advantage, the thinking goes, but there's a low ceiling for its future supply because **the professional arbitrage window will never open**. I disagree, I think. Natural demand for CDPs **will** continue to grow and keep the price of Dai somewhat in check, it just may dislocate for longer periods than people would like. This "slow arb" dynamic may even make DAI supply stickier in the long-term, as it's DAI pulling through CDP demand, rather than the more intuitive other way around.

How the f\*ck does that even happen when you can borrow from Compound and Aave with lower collateralization ratios, more collateral types, and more assets to borrow? Maker has looked uncompetitive as a lender, which should be bad news for Dai, but for the fact that those same competitive lending protocols have built yield farms that NEED Dai as one of their primary decentralized collateral options. For a while, **liquidity mining rewards** offset otherwise prohibitive costs to create new Dai. The effect was more extreme than in USDC.



People will buy a dollar for \$1.05 if they can safely earn \$1.10 with it. That's essentially what happened this summer as speculators bid up DAI in order to send it to liquidity pools that were yielding much higher rates.



As long as Dai completely dominates the fully on-chain stablecoin conversation (no others are even close), its demise will be greatly exaggerated. That first mover is hard to displace.

## 7.5 aDai or cDai or yDai

Something that might jump out at you if you're perusing the coin ranking sites is that "cDai" is larger than Dai itself. Has Compound gone fractional?

No. You deposit 100 Dai into Compound's money market protocol, and get 100 cDai, interest-bearing depository receipts, and claims back on the Dai you've locked in Compound. But your buddy may deposit 1 ETH as collateral and borrow 100 Dai (which you just deposited) against that collateral, then re-deposit the Dai to get 100 cDai. It's a quasi-Maker CDP mechanism running on a parallel protocol.

Or you can keep recursively borrowing and lending Dai to yourself through Compound because the yield on COMP liquidity mined tokens (juicing the AUM) is higher than the accumulated interest you pay to the protocol (in excess of what you owe yourself) on total

Dai borrowings. Deposit 100 Dai. Get 100 cDai. Borrow 90 Dai against the 100 Dai you just deposited (according to Compound's collateralization rules), redeposit, get 90 cDai. Borrow 81 Dai, redeposit, get 81 cDai...ad infinitum until you pay more to the protocol than you earn, and it don't make sense to borrow no mo'.

If you're lost, it's because your stupid.

Just kidding. These lending protocols and their incentives can get **superfluid** (and systemically risky?), and very hard to track. Suffice it to say, there's still only 100 actual Dai locked in Compound, but maybe 200 cDai outstanding because the Dai was the recycled hot potato in the protocol's equation, even if other collateral backstops (e.g., ETH) are also in the pool. But the system is NOT fractional since there's always more total collateral than claims on deposits.

This is true for cCoins (Compound) and aCoins (Aave), though it's almost a certainty that we'll see efforts to fractionalize stablecoin lending with the emergence of decentralized credit scores.

## 7.6 yUSD: Smart Dollars

Maybe the most fascinating stablecoin application of the year was the introduction of "smart stablecoins," yield-bearing tokens received by liquidity providers in exchange for their deposits into DeFi yield optimizers. Projects like Yearn.Finance have **changed the game** in this regard.

As explained in **Section 7.5**, users can deposit DAI in exchange for interest-bearing cDAI that represents a user's share of the Compound DAI pool and its accumulated interest on loans. But smart dollar vaults go further, automatically selecting the lending protocol and pool with the highest interest rates (Aave vs. Compound), and dynamically adjusting the parameters over time. Then they go even further, pledging those interest-bearing, yield-maximizing yDai tokens to AMMs to earn fees and liquidity mine even more tokens, which accrue again to yUSD.

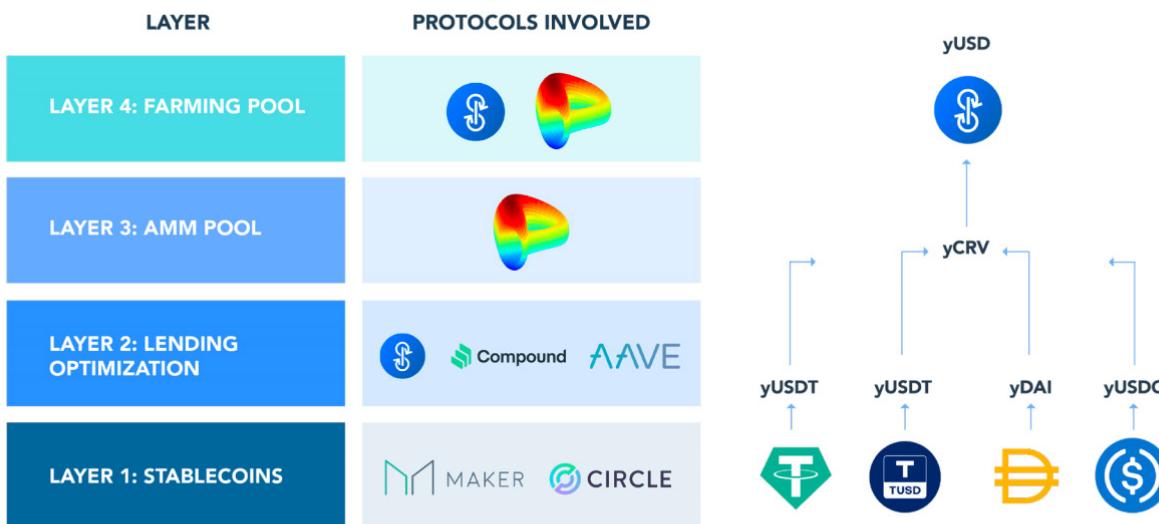
**As Watkins described it**, "*yUSD can be thought of as a super stablecoin that systematically generates yield from the highest yielding lending protocols, Curve trading activity, and CRV yield farming. It has provided users with ~50% APY since it launched two months ago.*"

Does that sound too good to be true? DING DING DING!

yUSD is also one of the riskiest stablecoins, as Yearn's vaults ensure users will assume the compounding smart contract (and economic security) risks of Yearn, Curve, and the other lending and stablecoin protocols that undergird yUSD. Its users also assume the risk of any pegged stablecoin's loss, as one lost peg would also cause the yUSD to lose its peg.

## The Layers of Risk in yUSD

yUSD is an incredible product, but also one of the riskiest stablecoins available on Ethereum



Source: Messari

I'm sure some team will launch the equivalent of FDIC insurance in 2021, tranching out default risk to speculators, and offering "safer," more reliable yields up to certain deposit caps than might otherwise accrue to simpler lending protocols. Compound and Aave are two projects already incorporating insurance funds into their protocols, so this can't be that far off.

But these innovations also feel like the early introduction of systemically risky leverage that will eventually cause the market to implode. If I were a regulator looking to make the case that DeFi developers were virtual asset service providers, I'd start here. I'm not saying I'm happy about that, just that it would be my move if I were evil and sitting on the other side of the chess board.

On the flipside, if you're a black hat hacker, there are \*massive\* and accumulating incentives to break these markets before they become "too big to fail." The spoils for cracking DeFi's big short would make **George Soros blush**, and I think we'll see a nine-figure exploit in 2021.

## 7.7 Ampleforth & Yams

I'm told variable supply stablecoins are interesting, but I don't understand them. That's despite Finematics's best efforts to explain [Ampleforth](#) and [Yam](#), and a good friend working on one of the year's most interesting (read: weirdest) projects.



Source: [DegenSpartan](#)

Here goes: it's good to have an elastic money supply that caters to an exploding population. Otherwise, your unit of account becomes hyper deflationary, and no one wants to spend it (e.g., bitcoin). On the other hand, elastic money supplies have a way of only ever **expanding**, which makes them inherently dilutive. We need a way to redistribute monetary tokens when the overall money supply expands to ensure early holders aren't diluted by systemic inflation. "Rebase tokens" are synthetics that gradually stabilize as demand increases.

Rebases use price oracles to compare the price of the underlying with a target peg. In high-demand environments, the token price trades at a premium, and the periodic rebase uses the stock dividend playbook to issue new supply and bring the unit price back down to earth.

So say you buy 1,000 AMPL for \$1.00 each; AMPL trades to \$1.50 that day; there's a rebase, and the protocol issues a 50% AMPL dividend.

In an instant, you theoretically have 1500 AMPL at \$1.50 each (f\*ck yeah!!), and your \$1,000 investment is now worth \$2,250. But this is an obvious accounting gimmick, and AMPL should immediately get sold below the dollar peg to get you closer to the \$1,000 original investment.

People won't pay \$25 for a \$20 pizza just because you make it a 10 cut vs. an 8 cut. I'm oversimplifying here, and there are other parameters, but this is the gist of it.

The system has tended to work, though, because a) crypto markets are less efficient than stock markets; b) even in stock markets, gimmicks like splits seem to work; c) if there are gradual inflows, then you'll (in theory) have more positive rebases than negative ones; and d) there are ways to earn yield on these collateralized assets in the meantime.

Yam Finance, named (intentionally) after the Thanksgiving vegetable, tested this theory as part of its "monetary experiment" over the summer. The protocol amassed **\$750 million in deposits within 48 hours of its launch** (pushing the YAM price to \$167, wtf) just 10 days after it was built. The contract was unaudited. There were bugs. Hilarity ensued. But it could have worked, maybe, and other projects like Empty Set Dollar, have exploded thanks to similar mechanisms.

I don't understand them either.

## 7.8 Libra

No updates, constant delays (though a soft launch is expected "early next year"). Yawn.

**Update:** they're [calling it "Diem" now](#), so all systems go.

## 7.9 Celo, Terra, Reserve

Libra's regulatory pain was Celo's and Terra's gain, as the non-Facebook alternatives marched to market. My sense is that the relatively muted response to these assets so far was the result of four factors: 1) Maker's relative underperformance; 2) the obsession with "smart dollar" gamified DeFi yield and "rebase" tokens; 3) the split attention between Maker, Terra, Celo, Reserve, and other programmatic stablecoin issuers, which made it harder for any to truly stand out as winners; and 4) the absence of broader protocol support and interoperability.

Celo and Terra seem poised to make the most significant gains in a eth1.5 + rollups / wrapped assets / "internet of blockchains" new normal, and are addressing #4 in particular.

**Terra** has quietly become one of the most commonly used blockchains in the world. It supports the largest non-USD pegged stablecoin (TerraKRW), and regularly generates higher transaction fees than any other blockchain outside of Bitcoin and Ethereum. That's thanks to its Chai payment gateway, which sports millions of MAUs via its partner Korean e-commerce giant. The app has facilitated \$3.5 billion of transactions so far this year with (\$25 million in fees accruing to Terra holders, which gives Terra a compelling economic model. That gets even more interesting as the project gets better integrated across DeFi (Cosmos, Solana, Ethereum, and more are on the roadmap for 2021), and this might be the play to make if

you're interested in an Eastern alternative to algorithmic stablecoin issuers, as it's not just dominant in Korea, but backed by major Chinese exchanges like Binance, Huobi, and OKex. Terra also scales! Unlike Maker, arbitrageurs can redeem and mint Terra stablecoins 1:1 for their underlying collateral.

Then there's **Celo**, which nailed the valuable "Libra minus Facebook" meme. Celo uses phone numbers as public keys (killer) and doesn't require an internet connection, making it an attractive utility for the developing world. They've got a rockstar list of backers from Reid Hoffman to Jack Dorsey, and funds like a16z, USV, and Polychain, and Celo issuer cLabs [acquired](#) blockchain interoperability specialist Summa this summer to work on bridges with Keep/tBTC, Cosmos, Ethereum, and Polkadot. Like Terra, it may have been availability, not utility that held Celo back this year. We'll see.

ADVERTISEMENT



## 7.10 CBDCs

We don't cover central-bank digital currencies much at Messari, because our bias is to focus on things that will be actionable for investors this year vs. 2030.

Progress on CBDCs moves at a glacial pace, but China's DCEP may be an exception, rolling out beta tests in 2021 that I expect will eventually have global geopolitical ramifications exceeding bitcoin's. The Block's Ryan Todd wrote [an excellent, comprehensive report](#) on the subject (see, I can be nice), but if you want my tl;dr takeaways, here:

- CBDCs may help central banks compete against tech giants for payment dominance
- They could facilitate negative interest rates, UBI, and more aggressive surveillance
- They could reduce (or reinforce) dollar dependency in smaller regions (USDC's use by the US government in Venezuela could be a beta test of our FedCoin?)
- They could improve uptime and interoperability across the banking system

That's not nothing, but it will take decades to come to fruition. I'm too impatient to write about the financial intranet.

# 8.0

## Crypto Credit 2021: Leverage Is a Helluva Drug

Last cycle, crypto credit markets basically didn't exist.

CME futures were approved in December 2017. Genesis Capital launched its lending desk in early 2018. FTX was founded in 2018. Binance's margin, lending, and futures all rolled out in the same \*quarter\* summer 2019.

Today's market makers, prop trading firms, and crypto hedge funds have more (highly liquid) toys to play with, which has led to better system-wide stability, and tighter spreads across both CeFi and DeFi. Indeed, 2020 was a banner year for perpetuals, basis trades, collateralized OTC lending, flash borrowing, and yield tokenization. The explosion of crypto credit could also mean that many would-be sellers next year opt to borrow against collateralized holdings rather than execute taxable sales.

Unfortunately, I only know three things about the crypto credit markets: 1) DeFi and CeFi credit market infrastructure has gotten 10x more robust since the beginning of the year (and things are getting competitive); 2) Genesis Capital's [quarterly reports](#) are a goldmine of information; and the company is a bellwether for the crypto credit markets; and 3) I really needed to find a better pundit for this section. An in-the-weeds trader?

Fortunately for you, I'm taking a breather from this monstrosity of a report, and handing it over to [CMS Holdings](#) for 10 sage bits of tweet-length crypto credit wisdom. If you don't understand a word, that sounds like a "you" problem. Maybe you should reconsider trading against Dan.

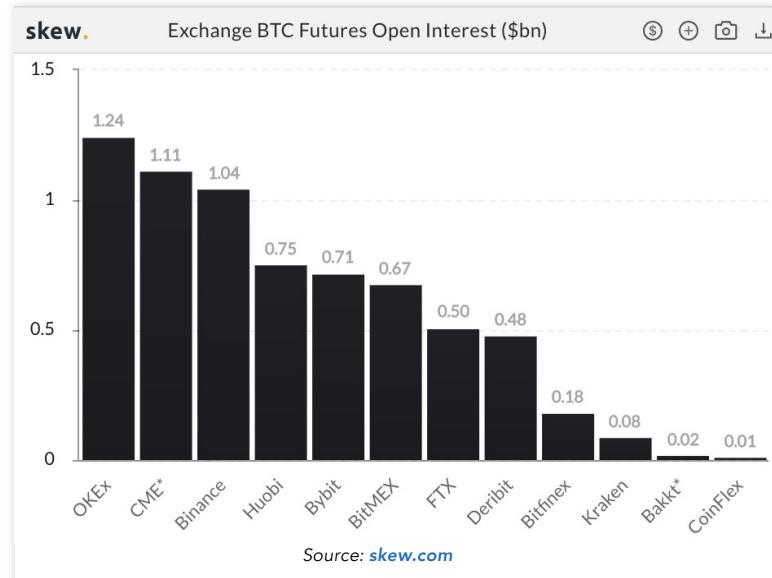
## 8.1 Record CME Growth



**CMS:** Crypto credit markets have ballooned in 2020 both on chain off chain futures / swaps I assume the p2p books as well but I don't check em that much this is the new normal and will likely only continue a thread...

**TBI Notes:** CME has become one of the primary sources of futures trading for "legit" desks like Renaissance and Tudor. OKEx and Binance may still be the biggest platforms for crypto basis trading, (long spot bitcoin, sell futures to collect the spread), but it's CME that has risen up the futures leaderboards. More established (tightly regulated) investors don't want credit exposure to Chinese exchanges, and opt for platforms their lawyers, auditors, and regulators know instead.

CMS says CME can also be up to 20x cheaper on fees for certain trades versus its crypto counterparts, And CME is one of the primary vehicles legacy investment funds use to acquire BTC in "[exchange for physical](#)" settled trades.

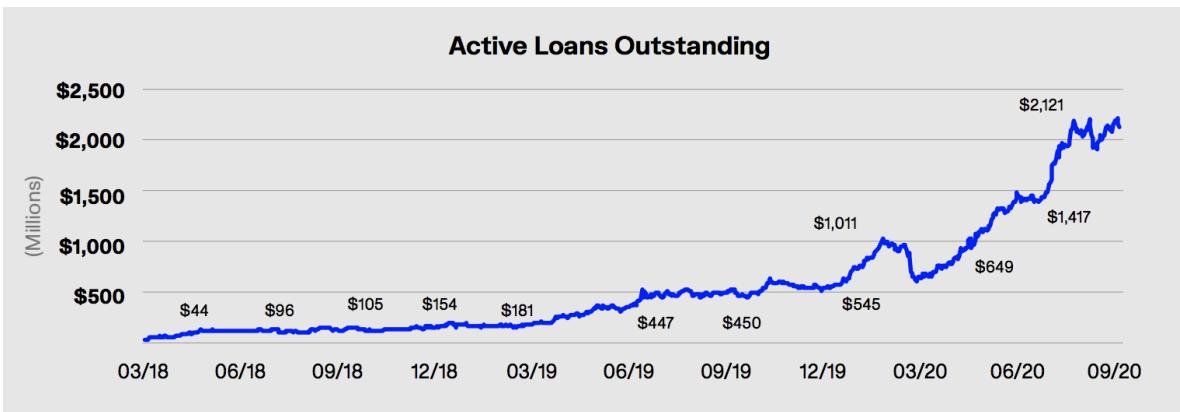


## 8.2 Credit Wealth Effects



**CMS:** In dollar terms they have all exploded in size because the price of all this shit has gone up and this is great for courting VC investors about your lending book, but also hugely important because it allows crypto to net suck more fiat for borrow out of more traditional lenders.

**TBI Notes:** It's not just about higher yields. It's about the wealth effect of crypto's rally unlocking billions of dollars that had previously been un-collateralizable. You can borrow more cash against 100 BTC today than you could a few months ago, and a few months before that, and crypto loans outstanding looks like the BTC price chart:



Source: [Genesis](#)

### 8.3 Lender Economics



**CMS:** Genesis and Blockfi in particular have just slapped on accelerating new ATHs quarter after quarter for their lending books these businesses are primarily driven by two trades, basis and grayscale issuance.

**TBI Notes:** Vertical markets lead to healthy competition. I had back-of-the-napkin net interest margin (the difference between lender lending rates and borrowing costs) at 200 bps (2%) at the beginning of the year. CMS thinks it's closer to 100-125bps now—still pretty healthy given you can consider most of that over-collateralized debt "prime." In crypto, people usually want to be net long, so the market trades in contango. It only goes backwardated on big moves lower, driven mostly by massive "shock" liquidations like [the one we saw in March](#). In terms of credit vs. spot market size, we're still 3-4 orders of magnitude away from crypto lenders reaching parity with securities lenders in terms of relative size vs. the underlying market. So NIM will drop further in 2021, but open interest will also jump another 2-3x (sans rally), so lenders won't care.

## 8.4 Basis Trading: Cash-Collateralization In. Coin-Collateralization Out.



**CMS:** Basis trading captures the difference between the futures price and cash price of the asset, you can do this with perp too making a bet of future financing via funding but either way this business is big and crypto generally trades contango so draws cash borrow.

**TBI Notes:** Coin-collateralized venues (BitMEX) have fallen out of favor, and cash-collateralized venues are in. BitMEX has been the biggest loser this cycle, thanks to a mix of regulatory heat (**DoJ charges**), and the increasing realization from traders that crypto-collateralized venues can blow up your balance sheet in an instant. Several funds **were obliterated** in the Black Thursday Flash Crash in March from their crypto-collateralized positions. The rise of stablecoins, like USDC, have also helped accelerate demand for cash-collateralized basis trading.

For Genesis's [more technical commentary](#) on basis trading trends:

"We suspect the long contracts are institutions buying BTC delta without a care for implied funding, while the short contracts are trading firms collapsing the basis against a long spot leg. The increase in OI indicates there is more spot BTC out there on the balance sheets of firms willing to short the CME basis. Since the CME cannot take BTC as collateral, there should be more BTC out there in the market as a result of these basis positions."

"Clients have historically worked closely with Genesis and are now lending both excess USD and BTC generated from the short CME basis trade back to Genesis, ultimately increasing our asset base as well. The implication of this expansion on forward curves should be more compression and more moderate implied yields - perhaps today's 12-15% annualized near month basis is equivalent to February's 30% annualized. Unlike previous regimes where unregulated offshore exchanges fueled the majority of calendar futures trading, we expect the CME growth story to continue into 2021."

## 8.5 Arbitrage & Boring Ass Delta Neutral Trading



**CMS:** This business is super enticing to delta neutral traders who hate risk and love perfectly hedging every aspect of their life.

**TBI Notes:** Lenders will borrow at 3% and lend at 4%, whether they are arbiting the difference between DeFi and bilateral markets, or the fixed yield curve against perp funding rates. Anything that's out of whack will get traded into whack, and there are massive electronic trading shops who are delta neutral, like B2C2, FalconX, and the bigger prime brokers. You have to wonder why some legacy trading shops would even get into this industry if they didn't want to put on at least **some** risk given crypto's exponential historical moves up, but we should welcome those boring ass legacy firms with open arms if they help drive down rates and spreads for all of us.

## 8.6 Grayscale Collateral Risks



**CMS:** The 2nd big trade is gbtc for myriad reasons some tax some lazy some access some tradition these products trade at a big premium to spot & have 6/12 month creation process that causes the premium to persist so you borrow coin / create shares / smash premium / get boat.

**TBI Notes:** The only thing that could blow up the big crypto lenders right now would seem to be a collapse in GBTC premiums. That's due to the credit exposure BlockFi and Genesis take on in the Grayscale creation trade, as they have large lots of GBTC shares as pledged collateral whose credit-worthy status hinges on the premium never turning into a discount. At GBTC discounts to the Trust's NAV, creditors taking on that exposure would go underwater. But this really only becomes an issue if Grayscale deposits were hacked or a non-Grayscale ETF was approved, Grayscale's products were rejected, and the new ETF stole share and destroyed the GBTC premium. That's unlikely. My money is on BlockFi and Genesis risk managers there.

## 8.7 BitMEX Rekt Funds



**CMS:** So those are the two big drivers of CeFi growth, but there's others of course desks use borrow to facilitate trading activity in a ton of different ways and market makers need borrow to keep liquidating on you on different venues and then there's DeFi and FARMING

**TBI Notes:** [Tetras](#), [Adaptive](#), and [Cambrial](#) blew up this year. How do you blow up in a year like this if you're responsible? Well, there's two general rules to crypto fund management: never go short, and never post crypto as collateral to levered longs. That applies in DeFi as well, where "farming Pool 2s" are the on-chain equivalent of Adaptive's disastrous levered long trading strategy on BitMEX. Seriously, don't go short unless you've got an exceptional risk management team. Even then, why? The only key to making money in the crypto fund world is not blowing up. Can't blow up if you're smart with leverage.



## 8.8 DeFi is the Tail Wagging the Dog



**CMS:** I'd wager this is still small but the DEFI rates can't exist in a vacuum, they're currently subsidized by tokens in many instances but at the end of the day if a rate differential exists with CEFI guys are gonna arb it which has definitely drawn borrowed capital into DEFI.

**TBI Notes:** Genesis noted in Q3 that a significant inflection point in their loan portfolio occurred thanks to DeFi demand, as BTC loans dropped from 51% to 41%, and stablecoin and "other" asset borrowing spiked in its place. Yield farming may have distorted yields for a short period of time, but they also pulled through demand for the crypto credit markets more broadly, not just amidst tinkerers. That gives you a sense for how big the DeFi mini-bubble was, and how much wilder things might get in crypto credit if DeFi has a "2017 ICO"-like actual bubble that gets out of hand in 2021.

## 8.9 So Many Options



**CMS:** Options have exploded primarily on Deribit which has resulted in a large amount of options overlays trades which has given yield options to holders as well.

**TBI Notes:** What. A. Chart. Buyers of volatility are usually crypto funds looking for insurance that helps them maintain "beta-driven" market upside while still trading their unique strategies. Sellers can be overwriting positions or creating more exotic trades. Most options trading is reflected on [Deribit's options platform](#). TBD on how the CFTC will ultimately feel about them.



Volume of Bitcoin Options



## 8.10 DeFi's Yield Curve



**CMS:** Anyway end result of all this is we're getting cheaper borrow EOD because more cash is coming in to lend rates in crypto are still high and this ultimately should help all you degens lever up cheaper faster larger as the end beneficiary.

**TBI Notes:** This is just a [beautiful graphic](#) from Messari community analyst Roberto Talamas, showing how the DeFi yield curve has developed since Yield protocol's beta launch. In short, DeFi and general credit markets are getting more liquid and closer each day to reflecting the industry's equivalent of a "risk-free" rate, as most of the action has been at the short-term side of the maturity curve. The [fixed rate yield curve for DeFi is coming](#), and it should cause another leg up in retail DeFi lending in 2021. Fixed rate borrow isn't exactly a paradigm shift, but like everything else in crypto, the speculators will help bootstrap the frontier markets, and that will drive down yields to the point these products become 10x more accessible.

# 9.0

## Synthetic Assets: All About Accessibility

"I don't want to be my own bank. Or fight a revolution. Or flee the country. I just want the number to go up, and to get rich when it does." Well then, this section is for you.

### 9.1 The Grayscale Trade

It's not just DeFi! If you stake BTC and ETH for six months, or LTC, ETC, or BCH for a year, you too can farm shares at triple digit APYs!

Those "yields" aren't DeFi farms, though, they're off the backs of equally unsuspecting investors. The SEC's refusal to approve a bitcoin ETF has led to the exploitation of an esoteric loophole now known throughout the industry as "[The Grayscale Trade](#)," where the asset manager's investment vehicles serve as manna from crypto fund heaven and ticking time bombs for public markets investors. They've also led to 5x growth in Grayscale's AUM this year thanks not only to BTC's 2.5x performance and ETH's 4x performance, but to double the volume of new *share creations* this year than in the rest of the firm's history combined.

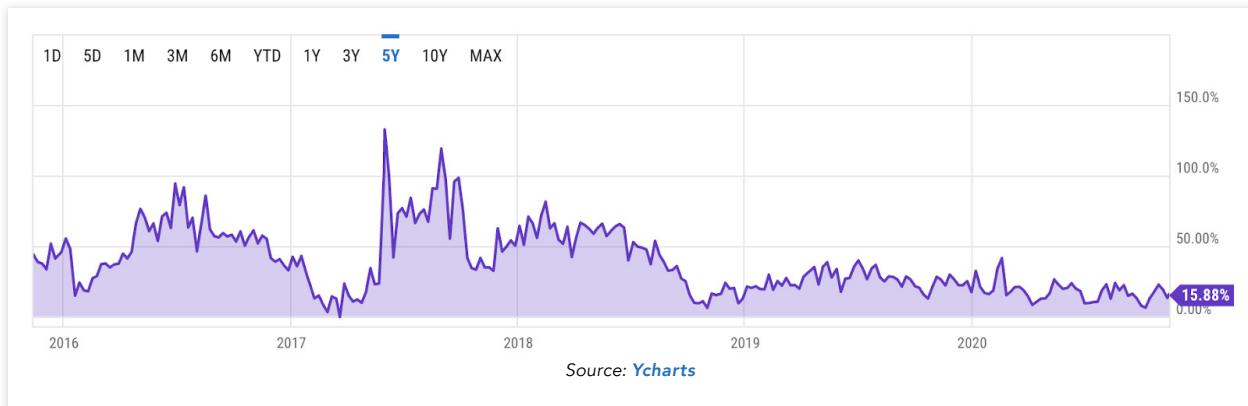


Here's how the worst-kept trade secret in crypto actually works:

1. Accredited investors are eligible to create shares in Grayscale's closed-end trusts by sending either crypto or dollars to Grayscale and receiving new **restricted** shares in the defined trust. Those shares are subject to a six or twelve month lock-up.
2. Some creditworthy customers that already do business with Grayscale's affiliate and authorized participant, Genesis Trading, are able to **create shares on credit**: borrow from Genesis, fund a Grayscale Trust, receive new restricted shares in the trust, and pledge shares back to Genesis as collateral. It's sorta like DCG's version of a flash loan.
3. Grayscale makes money on the AUM, Genesis makes money on the loan interest, and the investors (hope to) **make money on the premium between the floating shares and their underlying net asset value** after the restricted period.
4. GBTC's premium is usually in the 10-20% range; ETHE's is in the 50-80% range; LTCN, BCHG, ETCG have been all over the map, but are **usually in the black** by multiples, not percentages (the exception was following one of Ethereum Classic's 51% attacks).
5. **Repeat ad infinitum** until the relevant premium drops below your opportunity cost of capital, which is hard to do if you're also applying leverage to the trade through Genesis.

A number of trading firms have been hammering this trade for **years**, and yet GBTC's and ETHE's premiums have persisted, and at times, swollen. Closing this price gap is slow-motion "arbitrage," I suppose, but it's also an indictment of the SEC, who has prioritized the letter of the law vs. its spirit. In no way is GBTC's existence and the SEC's ongoing ETF obstinacy consistent with their mandate to protect investors. It's shameful.

There are some legitimate perks to the publicly traded trusts' shares (e.g., investors can buy shares via tax advantaged accounts like IRAs), but for the most part, they're the real "rat poison squared" for retail: losing positions as funds arb down the premium over time, and losing positions if these vehicles ever get converted into bona fide ETFs and the premium gets eliminated entirely. The unwashed masses' rat poison is your yield. Just like DeFi. <grin>



I could see Grayscale doubling AUM next year even without much of a price rally. With a price rally? Grayscale does \$1 billion in annualized EBITDA at \$100k BTC. (Not a typo.)

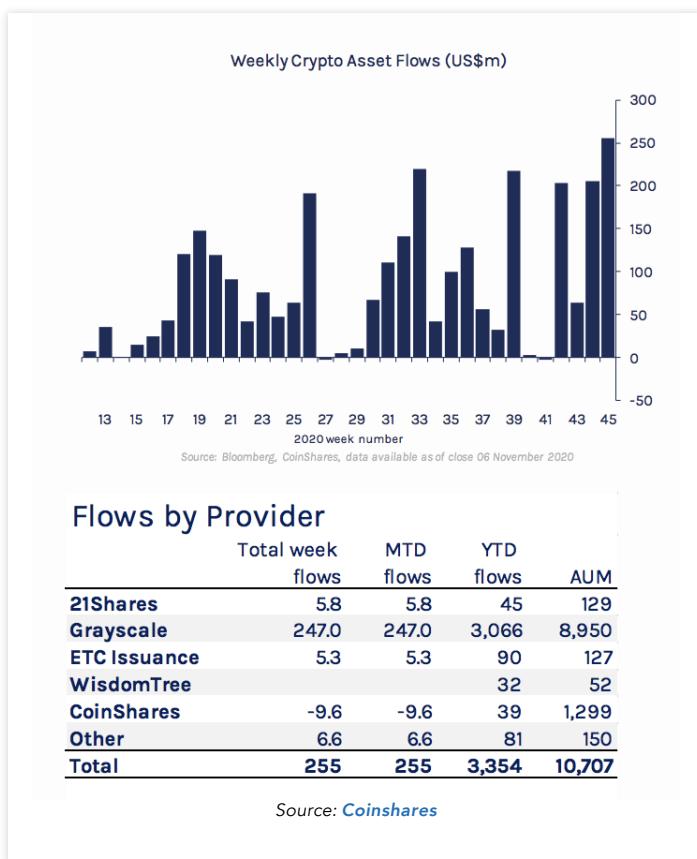
It's a helluva dynamic while it lasts: a natural monopoly on publicly traded crypto vehicles in the U.S. and absolutely no AUM leakage.

## 9.2 Crypto ETF(s) Approval

The irony of how badly the SEC's ETF rejections have backfired is that Grayscale will almost certainly win the race to market (by a mile) once a sensible leader takes over from [outgoing SEC Commissioner](#) Jay Clayton in 2021. With nearly 3% of all BTC and ETH in circulation locked in Grayscale trusts (and accelerating), it's insane to think we won't finally see the long awaited Bitcoin ETF listing sometime next year.

The DoJ's money laundering lawsuit vs. BitMEX and the subsequent decline in that exchange's market dominance, combined with the Q4 rotation out of Chinese exchanges, should also work wonders in supporting the ETF argument that everyone except the SEC already appreciates: properly surveilled (and Western) markets are [driving price discovery](#) these days.

The only remaining question is how quickly other competitive ETF applications will be approved after Grayscale. Bitwise has done yeoman's work educating the SEC on global crypto market structure, and has the bona fides to make a good steward of publicly traded funds.



CoinShares already counts \$1 billion under management for its European traded ETPs and would seem like [the most competitive player to take on Grayscale](#) once the floodgates in the U.S. markets open up. Once these funds are allowed to compete, its play will be to drive down fees on single asset trusts, and craft more exotic baskets of actively managed portfolios.

On potential *actively managed* ETFs, crypto managers would do well to study Cathie Wood's ARK Investments, the very first ETF to hold GBTC shares, and one of the fastest growing asset managers of all time.

ARK crushed it this year, doubling AUM, and watching its flagship fund \$ARKK double in price as well. ARK [launched in 2014](#), around the same time as Grayscale. Shockingly, it's grown even faster.

Long ARK Invest. Long Grayscale/CoinShares/Bitwise. Short the SEC.



### 9.3 Yearn Strategy

We already covered Yearn and other DeFi assets at length, but it's worth noting another one of the special products in the yearn.finance family: yVaults, two sided marketplaces that match liquidity providers with "strategy creators." yVaults allow farmers to deposit funds of their choice and let the yVault strategy do its work generating good yield, and limiting brain damage tied to actually crafting strategies in a market of exponentially increasing complexity.

YFI currently charges a 5% performance fee and a 0.5% withdrawal fee on yVaults, then sends 10% of that to strategy creators and the remainder to its community governed treasury (which can also be staked to YFI pools to further juice returns). But the system parameters are always subject to change based on token-holder voting, and [yVault strategy creation may soon be one of the fastest ways to reap rewards](#) usually reserved for passive index managers, as many of the vaults have [already accumulated \\$50-100 million](#) in locked value.

ADVERTISEMENT

**Where Crypto Enters Finance**

JOIN 4 MILLION CUSTOMERS

**Bitstamp**

It's TBD on how much yVault AUM is sticky, and how much revenue actually accrues to creators in the long-term. But in the near-term, yVault fees are about to hike 4x (up to a 2% management fee and 20% performance), which makes the headline numbers look juicy: a \$100 million pool that yields 10% will generate \$2 million in management fees (straight to the protocol) and \$2 million in performance fees off of the \$10 million in yield, split 50-50 between YFI holders and strategy creators. There is a LOT of upside for creating winning strategies that accumulate billions of dollars of AUM.

Could we see our first single employee unicorn via yVault's strategy creation mechanism?



## DeFi Protocols' Take Rate

*YFI has among the highest take rates across DeFi*



As of Aug. 23, 2020

Note: YFI take rate only includes 5% performance fee. It does not include its 0.5% withdrawal fee

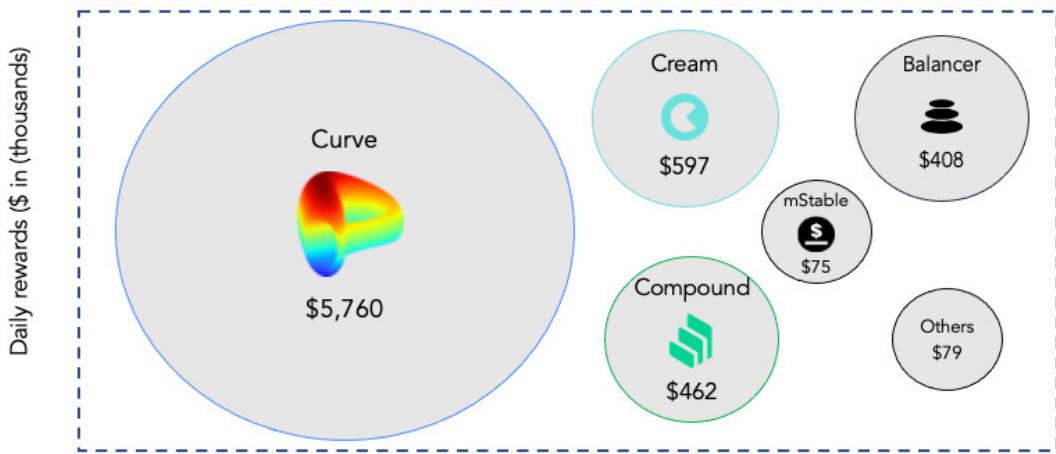
Source: Token Terminal



## Total Daily Yield Farming Rewards

Liquidity mining programs currently provide more than \$7 million in daily liquidity rewards - equivalent to \$2.6 billion a year

Total: \$7.3 million



As of Aug. 21, 2020

Note: Others include MCB, RARI, JRT, ANT, PNK, AUC, AMPL, MFT  
Source: Messari

At \$10 billion of "assets under strategy" (Grayscale's AUM today), an individual creator with a 10% yield strategy would net a \$100 million annual performance fee. That's as alpha as it gets for young quants, if they bet early and right on this market.

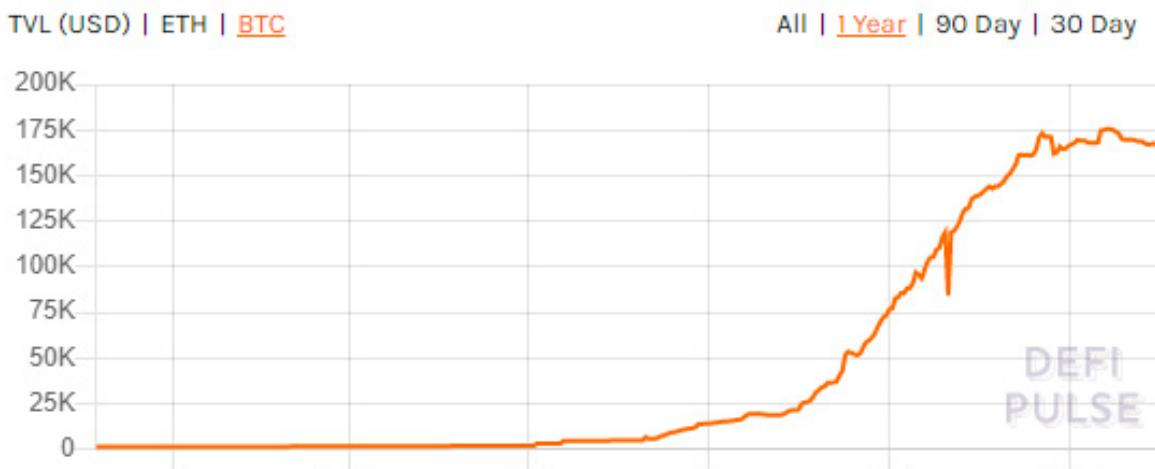
## 9.4 Play Safe and Wrap It Up

When I looked a couple of weeks ago, there were 10 synthetic cryptoassets with \$100+ million market caps, excluding bank deposit-backed stablecoins: synthetic bitcoin like wBTC (\$2.3b+) and renBTC (\$300mm+); Compound and AAVE assets like cDai (\$1.7bn), cETH (\$750mm), Aave LINK (\$500mm), and Aave ETH (\$300mm), and algorithmic stablecoins like Maker's Dai (\$1.1bn), and Terra's TerraKRW (\$100mm). This trend is just getting started.

Expect to see these and other synthetic assets dominating the screens of your favorite coin ranking sites in 2021, because everything is getting wrapped, ported, and leveraged in crypto's credit-fueled boom of 2021.

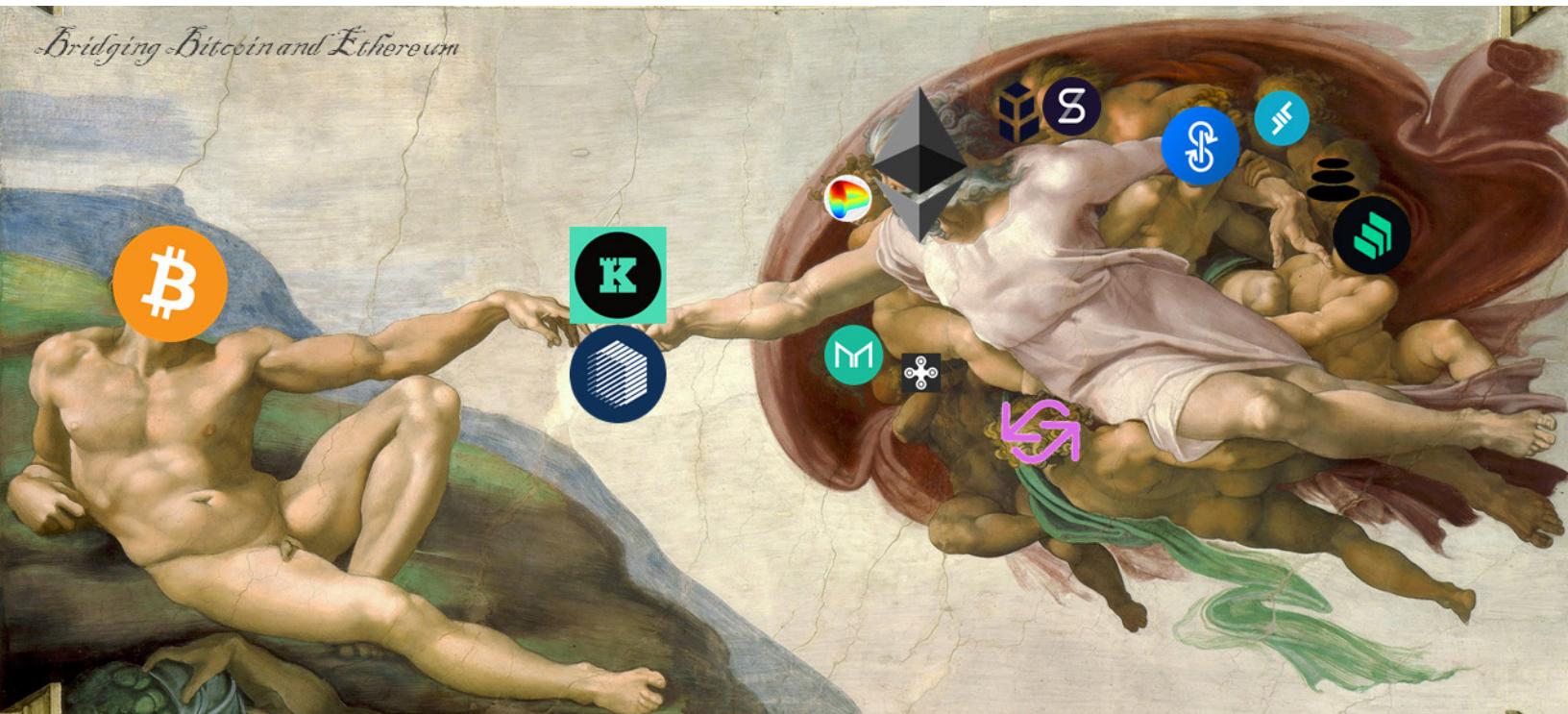
There may be a lot of hand-wringing regarding the complexity and systemic risks layered into the DeFi lending markets this coming year. But one trend I'm excited about that seems marginally safer is the popularization of **cross-protocol** swaps. BitGo has **dominated** the wrapped bitcoin market to date, and TokenSoft's **Wrapped.com** partnership with Anchorage should emerge as a legitimate competitor. They're creating new types of cross-chain swaps like wrapped ZEC and wrapped FIL, and much more. (Disclosure: I'm a TokenSoft investor.)

### BTC Locked in DeFi



Source: DeFi Pulse (at current prices, there is \$3.1 billion of BTC on Ethereum)

Watkins also [wrote a primer](#) on what's to come with decentralized custodial networks like Keep and REN, and it's been exciting to slowly watch the "internet of blockchains" truly get connected (again, thanks to DeFi) with these tools. One concern I have is that blockchain-interoperable assets become a beast to monitor as they get locked as collateral or (gasp) stored in zk-snark-secured shielded pools. It could create "Big Short" levels of complexity that become difficult to disentangle until things unravel in the next market comedown. Triple entry accounting ledgers are only really useful if someone knows how to connect all the bookkeeping software.



There's been about \$3 billion of major assets wrapped so far across blockchains (mostly in the BTC → ETH corridor). That could grow 5x next year, before factoring in a potential price rally, and still come up short of the synthetic shares that ETP managers already custody. Between ETPs, cross-chain wrapped assets, and DeFi collateral, we'll have \$25 billion in synthetic cryptoassets by the end of 2021, up from less than \$100 million in 2016.

## 9.5 I Predict Prediction Markets

I'm convinced Augur could announce a cure for cancer, and REP would fall 5%. Gnosis has shipped a ton of cool product, but not much towards their original vision for a decentralized prediction market, and the GNO float trades at a fraction of its balance sheet capital.

Polymarket looks promising, if early. But I've said that about similar markets. Remember [Veil?](#) Maybe prediction markets haven't had their breakout moment yet, or maybe they just...aren't as interesting as we originally thought, and there are better ways to express bets or take on risk within crypto?

I loved this from [CMS Holdings](#) right after the election:

*"For all the hoopla around prediction markets the last three days were basically the World Series for them and they punched slightly under link/usd activity globally I'd wager. People love to watch but they don't dip their toes in enough."*

Oof.

There's maybe no better sign prediction markets are having a tough go than Augur featuring a Balaji quote on their homepage while [his investment in a rival platform](#) gets announced. Who could have predicted that?



Source: [Augur](#)

## 9.6 Synthetic Stocks

I'm old enough to remember last summer when Abra got [a big no-no from the authorities](#) for offering synthetic exposure to the U.S. stock market.

Don't get me wrong: I LOVE the concept of being able to invest in (or short!) stonks next to my crypto holdings, but I don't get how FTX will be able to list synthetic, fractional stocks of U.S companies for very long, even if they're blocking U.S. customers. Apparently, [the exchange is working](#) with German and Swiss-based financial firms to offer exposure to stocks like Facebook, Netflix, Tesla, Apple, and a dozen or so others (as a trial run?), and they are doing modest volume in their first month.

If anyone can figure out a path to tokenizing actual U.S. securities and live to tell the tale, it might be the FTX / Alameda team, but let's see if they add more markets before betting the farm on their success. I'd also like to see whether there is any real action in the synthetic stocks over the weekends (where you'd expect 24/7 synthetic tokens to provide some marginal utility). But so far, they've been [oddly quiet outside of standard market hours](#).

Synthetic securities that bring better global accessibility to existing exchange-traded stocks are more interesting than security token offerings (which I still hate). But it's probably not an earth-shattering development for crypto, as I'm confident that stonks will prove more boring in 2021.

## 9.7 Exchange Securities Tokens

Sometimes, I forget we already have our own little quasi-security market for crypto infrastructure companies. I'm talking about the "buyback-and-burn" exchange tokens, like BNB, Huobi Token, and FTT. BNB gets all the press, burning **\$70 million a quarter**, even if it no longer explicitly ties those burns back to platform earnings. But Huobi may be a better directional bet if you want exposure to the Chinese crypto market (recent issues notwithstanding). I liked Multicoin's **investment thesis** on crypto exchange tokens, which showed how HT's buyback ratio as a percentage of network market cap was the industry's best (by a lot).

Exchange Token Comp Analysis			mm tokens		% Floating	Fully Diluted Mkt Cap (mm)	Floating Mkt Cap (mm)	Trailing 12 month burn (mm)	Fully Diluted Buyback Ratio	Floating Buyback Ratio
Token	Platform	Last Px	Fully Diluted	Float						
FTT	FTX	\$3.05	344.97	115.93	33.60%	\$1,052.16	\$353.57	\$10.97	1.04%	3.10%
BNB	Binance	\$17.67	179.88	147.88	82.21%	\$3,178.48	\$2,613.04	\$151.00	4.75%	5.78%
OKB	OKEx	\$5.06	300.00	279.33	93.11%	\$1,518.00	\$1,413.40	\$69.15	4.56%	4.89%
LEO	Bitfinex	\$1.14	985.24	978.13	99.28%	\$1,123.17	\$1,115.07	\$17.43	1.55%	1.56%
KCS	KuCoin	\$0.78	171.25	81.25	47.45%	\$134.20	\$63.67	\$2.97	2.21%	4.66%
<b>Comparable Company Averages</b>					<b>71.13%</b>	<b>\$1,401.20</b>	<b>\$1,111.75</b>	<b>\$50.30</b>	<b>2.82%</b>	<b>4.00%</b>
HT	Huobi	\$4.22	290.99	233.37	80.20%	\$1,227.98	\$984.82	\$175.50	14.29%	17.82%
<b>Huobi's Burn Premium Over Sector Average</b>										<b>5.06x</b>
<b>4.45x</b>										

Chart 10: Sources - Exchange websites, Maple Leaf Capital, [CoinGecko](#). (for assets that started burning within the last 12 months, we took the full history and prorated out to 12 months)

Source: [Multicoin](#)

The general value capture models of exchange tokens could carry over to Web3 wallets as well, more of whom may begin to charge "convenience fees" on the transactions they facilitate. Metamask could be the early play there, having recently entered the DeFi aggregator market with their "**swaps**" product (which they serve up to millions of existing end users). Argent, MyCrypto, and even Brave's BAT (through a repurposing of the token's usage) could monetize via convenience fees as well (or better in-wallet gas optimizers) if they tokenized their products. I'd expect one (if not several) web3 wallets to roll out liquidity mining programs next year that incentivize behaviors like staking and voting self-custodied assets.

## 9.8 On-Chain Indices

Anyone can become an index creator or asset manager these days (though I'd get legal advice before you get too far ahead of yourselves).

Set Protocol's \$DPI, a collaboration with [data aggregator DeFi Pulse](#), tracks a market cap weighted basket of DeFi "blue chips" and may be my favorite index right now. It's accumulated \$35 million in assets as of this writing, and tracks 11 assets for a 1% annual fee. Maker, Aave, Synthetix, yEarn, and Uniswap are 2/3 of the index, but it also includes Balancer and Ren, and participates actively in some staking. [PieDAO](#) offers blue chip DeFis (and LINK) exposure, and stakes deposits via a Balancer pool. (I'm sure there will be others that have popped up in the week between this draft and post-publication.)

I haven't forgotten about [Melon](#), either, which was the OG decentralized on-chain asset management protocol before it got absolutely smashed in the bear market. MLN has enjoyed a 10x resurgence this year, after fixing a flawed token economic model. Jack covered Melon [in full in a Pro research report](#) recently, but the gist is that Melon now earns a 20bp protocol management fee based on platform AUM—it's a tried and true model that should work if on-chain indices get big. (Disclosure: I have a small allocation of my portfolio in MLN.)

## 9.9 DAOs: FOMO in & Ragequit

I wrote earlier about the crypto wealth effect and the "death" of traditional VCs when it comes to the crypto markets. A big part of my conviction here has to do with developments in the for-profit DAO space, where groups like [MetaCartel](#) and [the LAO](#) have created community investment vehicles that pool experienced community members with money (ostensibly the people you'd expect to outperform in due diligence and specific industry value add).

DAOs have much more flexibility to invest in novel strategies beyond equity investing and even basic token investing. They can make OTC markets for unlisted assets, invest in managed trading funds, sponsor teams in competitive crypto gaming leagues, buy and securitize NFTs, and generally monetize any new trend the crypto-native asset class spawns next (e.g., NFTs and [Flamingo DAO](#)).

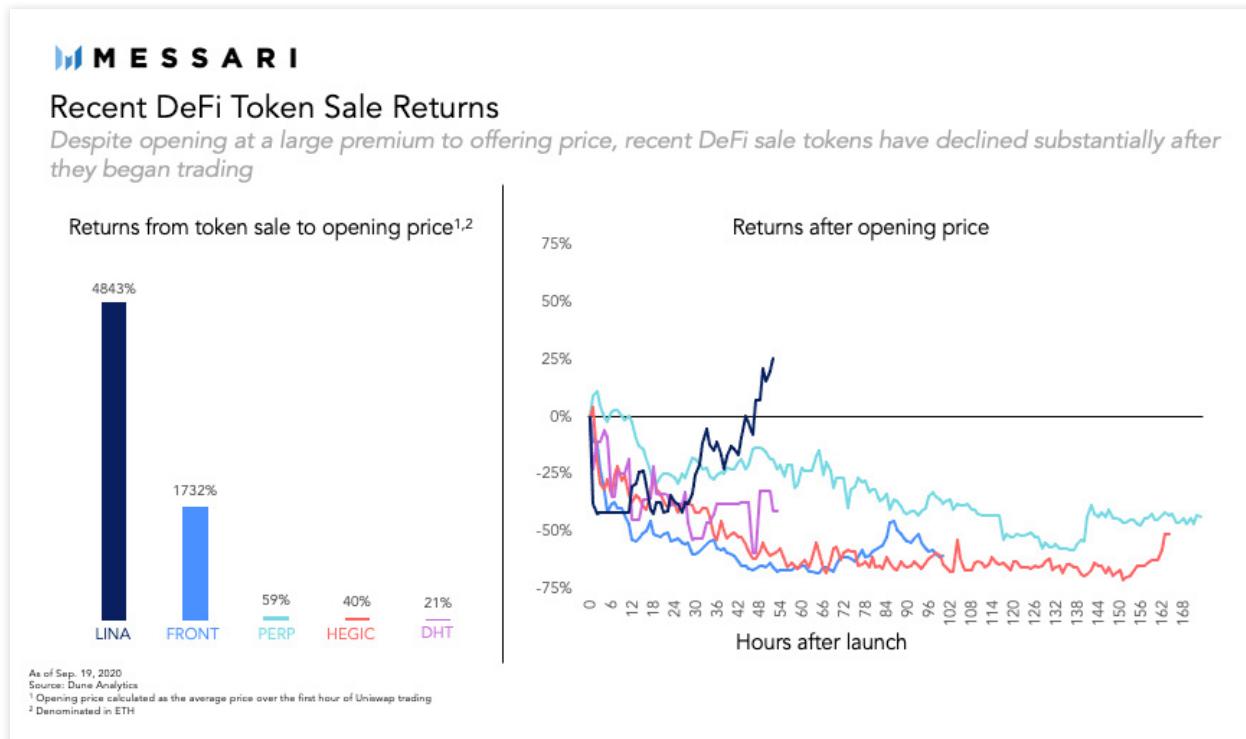
These early communities are active, too. So far, the LAO and MetaCartel have [maintained](#) 55%+ voting rates (one of the best when you factor in the respective DAO's membership size), but you can envision a future in which these vehicles begin to split rewards by members' level of participation. Totally passive? Pay a carry. Top producer? Earn that carry. In between? You fit somewhere on that sliding scale. Those mechanisms could align early stage community funds and ensure they do not devolve into mob rule (even if there are "ragequitting" mechanisms that preserve the right to defect from the mob).

What separates these for-profit DAOs from their catastrophic early namesake is their legal strides (the LAO's documentation is open source under OpenLaw) and their exclusivity: you need to [get jumped](#) into the MetaCartel, or you're shit out of luck. (Hopefully, this thesis helps me secure my spot.)

## 9.10 Bonding Curves and the IDOs of March

The novel structure of the UMA and bZx "[initial DEX offerings](#)" provided a glimpse of what you might expect if you give entrepreneurial teams the latitude to raise money in a sale with a \*guaranteed\* floor price, while also attempting to sell tokens in a more democratic and decentralized way.

Because these sales get initialized by seeding a token pair to an AMM, the token can \*only\* be purchased upon initial launch, and because this is crypto, they'll very likely get front-run by bots. This happened with UMA, which listed its token at the same price its seed investors had previously paid, only to watch the price rally 8x within minutes. (It's still up 4x from that "frothy" peak after initial trading.) And the aforementioned bug bounty protocol, bZx, witnessed its IDO get front-run in the first 60 seconds, netting a flash-borrowing bot a cool \$500k worth of profits in the token's rapid 12x price spike out of the gates. (Goldman Sachs's offer to the bot is pending.)



In a parabolic uptrending market, you can safely assume you will have a bad time if you try to participate in the greater fool market making of an initial DEX offering. But in a calmer market, and with good, sober projects, it's a perfectly fine distribution mechanism.

I actually think this sort of thing is a \*great\* mechanism for seeding tokenized equity markets, where early trading should naturally be a bit more subdued. I thought Fairmint would have a break-out year this year, but I forgot the cardinal rule that security tokens-looking projects will always take longer than you think they will. That said, I'm doubling down on the prediction I made last year that "**continuous securities offerings**" are one of the only security token plays that excite me right now.

# 10.0

## Infrastructure: Crypto Exchange Unbundling

Most crypto services boil down to exchange, custody, and information. If you want to buy or sell, send or receive, lend or borrow, or create or redeem a blockchain-based asset, then you need a centralized exchange or a smart contract with similar capabilities. Then you'll need somewhere to store those assets (by yourself or via a hosted service), and stake and vote as needed in crypto's participatory economies. Finally, you'll need quantitative data to feed your services, events monitoring to ensure your custodial setup stays in sync with network developments, and general research and education tools for buy/sell/hold updates.

This year's primary crypto infrastructure question is simple: do you believe exchanges will continue to aggregate all of these critical functions under one umbrella? Or are they at risk of being replaced or unbundled?

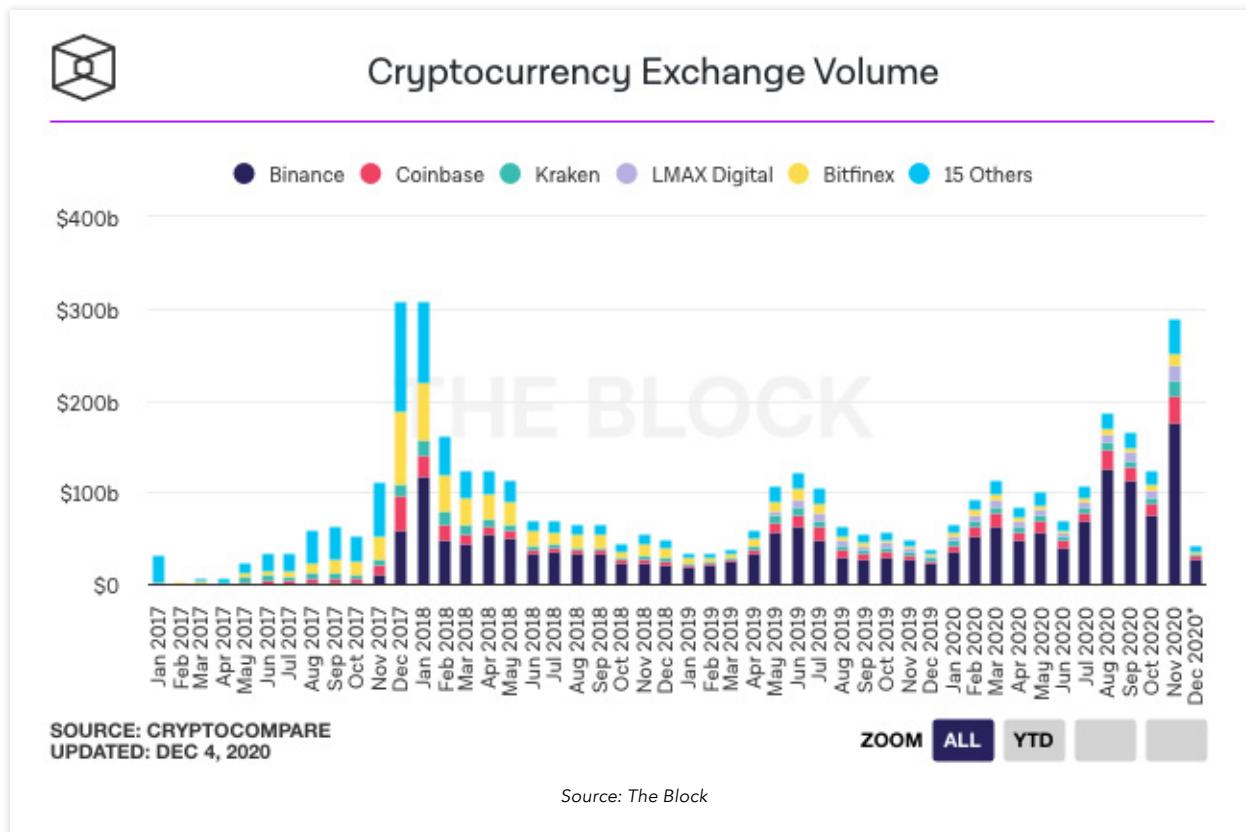
---

### 10.1 Exchange Aggregation Theory: The Case for Bundling

It's expensive to bet against the bundlers.

Binance kept its top position as the industry leader in trading volumes and acquired data giant CoinMarketCap for \$400 million to strengthen its top of funnel. FTX was one of the fastest growing and most innovative exchange operators of the year, and it [acquired](#) Blockfolio for \$150 million for many of the same reasons. Kraken-backed Cryptowatch entered the list of top data sites. And Digital Currency Group leveraged CoinDesk's (virtual) events business for a financial advisor event that introduced its prime brokerage and asset management services to new clientele. Oh, and DCG even went the other direction too, acquiring an [exchange](#) of its own in Luno.

That's just on the data and information side of things, to say nothing of the myriad new products these behemoths introduced in lending, staking, derivatives, etc.



Exchanges remain at the center of the crypto universe for three reasons: 1) they make all the money in an industry fueled by trading fees; 2) they haven't yet been forced to unbundle certain functions for technical and regulatory reasons; and 3) most users are lazy, and trust exchanges as de facto custodians regardless of the warnings against that practice. There's a sense that if Coinbase gets hacked; we're in for a dark winter anyway.

Still, exchange dominance is not a foregone conclusion. This is a great chart for "be your own bank"-ers, but a concerning one if you're an exchange operator. Exchange bitcoin reserves are down 25% since March:

### Bitcoin: All Exchanges Reserve

The amount of BTC held in all exchanges' wallets.



Source: CryptoQuant

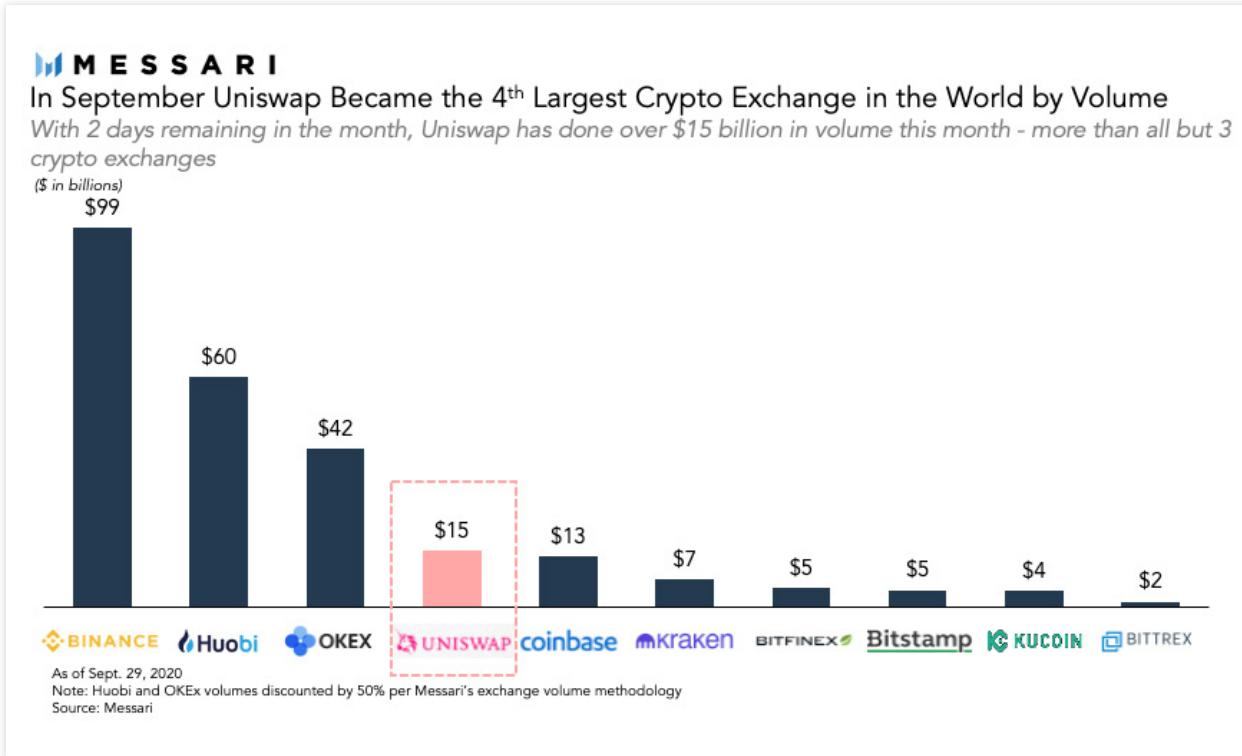
Bitfinex remains embroiled in court with the New York Attorney General; BitMEX's DoJ charges (not to mention its [performance issues](#) on [Black Thursday](#)) were a killer for customer confidence, and it's unlikely the company will ever recover its 2019 heights; the major Chinese exchanges received visits from or were detained by the CCP, another good way to lose business; Coinbase and Kraken lost ground (relatively) to Uniswap due to incomplete market pair coverage; and I get the feeling that even CZ is feeling the heat from regulators and competitors to have made such an aggressive move against Forbes for its recent article on the company's [regulatory arbitrage strategy](#).

I am more bullish on exchange "unbundling" in theory than in fact. The Cambridge Cryptoasset Benchmarking Study found [there are now 100+ million identity-verified users worldwide across exchanges](#), triple what it had reported less than two years earlier. New regulations may [reshape](#) the exchange rankings, but as a class, these businesses will continue to dominate the space, and lead the M&A charge again in 2021. They'll acquire smaller regional also-rans, and add new revenue lines via tuck-in whenever opportunity knocks.

Another billion dollars in M&A seems likely as we enter the institutional cycle of crypto adoption, and these giants ward off competition from new entrants from legacy institutions.

## 10.2 Exchanges Unbundled: CEX vs AMM for Retail

In three years, Uniswap has grown from a [proof-of-concept](#) built by a novice developer (former mechanical engineer) and funded by an Ethereum Foundation grant to a top ten global trading “venue,” and a multi-billion dollar token project. The DEX pioneer famously eclipsed Coinbase and Kraken in September during the height of the (Phase 1?) DeFi mania, when DEX volumes reached their zenith at 16% of overall exchange traded volumes.



Uniswap’s “Immaculate” token launch unexpectedly rewarded early community members with ~ \$600 million of airdropped value while locking in more liquidity from market makers. Those community incentives are great, but I don’t think that fully explains Uniswap’s 2020 rise. The DEX was already rocketing in usage even before its summer liquidity mining scheme.

Instead—for Uniswap, AMMs, and DEX in general—it’s all about their magical user experience.

I know I’m paying higher fees for the privilege, but the DEX trading experience is cleaner, the long tail assets I want to trade are more reliably accessible, and I don’t need to worry about opening multiple exchange accounts and taking multiple instances of counterparty risk every time I want to make a bet. I open Uniswap, select an asset, click trade, and the assets appear on my Ledger. AMMs are even getting better where they’ve been weakest: fees and slippage are shrinking with innovations in gas fee optimizations, AMM curvature, options and insurance, and various structured product solutions that better tailor investor risks.

I haven't yet met a DeFi skeptic who has tried one of these simple portals and remained an unabashed critic. I'd imagine DEXes will continue to siphon liquidity from CEX when it comes to smaller market pairs, and new on-chain instruments (vault tokens, indices, etc.)

### 10.3 Exchanges Unbundled: Prime Brokerage

Prime brokerage services from crypto companies and more traditional financial players alike are beginning to replace exchanges as the initial touchpoints for investors, especially institutional investors. Square, PayPal, and other consumer fintechs go OTC or least-cost route between exchanges to fill their coffers for customers, while larger funds head to Grayscale or the top prime brokers (e.g., Fidelity, BitGo) to do the same. The exchanges themselves are increasingly missing out on the most valuable touch point they have with new customers: initial deposits.

That's why Coinbase acquired Tagomi this spring. B2C2, FalconX, and Galaxy upgraded their prime brokerage services, and it seems like just a matter of time before giants like JPMorgan and Goldman Sachs acquire their way into the market as well. The mega-exchanges will continue to provide the rails, but fees will slowly come down in the process. I wonder how many CEXes will ultimately matter in five years as value continues to leak to brokers vs. the utilities at the center.

### 10.4 Exchanges Unbundled: Qualified Custody

It's easier to decentralized exchange than it is to decentralized custody, which is one reason I'm short exchange revenue and long custodial revenue in the medium-term. Today, there are two primary facets of institutional custodial services in crypto: secure storage, and staking.

Remember that chart about exchange bitcoin deposits in [Section 10.1](#)? The numbers aren't plummeting because more retail users are beginning to self-custody crypto on hardware wallets. It's because Fireblocks, Fidelity, BitGo, Anchorage, and other qualified custodians are locking up assets for institutional clients. Assets that, in many cases, may never see the light of day again.

Fireblocks and Anchorage are particularly interesting. The former derisks the "hot wallet" problem of crypto custody, making it safer and easier to make on-chain transactions. The latter received coveted SOC-1 certification from auditor EY, and is taking on BitGo for preeminence in "wrapped asset" custody via its partnership with TokenSoft. Then there's the staking services, like Bison Trails, which provide the infrastructure to help these custodians ensure customer deposits can earn yield while they're held safely in storage.

Unless a major exchange is acquired this year by a legacy financial institution, I have one of Anchorage, BitGo, or Fireblocks setting the 2021 high-water mark for M&A sticker price, with any one of them eclipsing the previous \$400 million marks set by Poloniex and CoinMarketCap.

## 10.5 Exchanges Unbundled: Web3 Wallets as Sovereign Banks

I'm constantly torn by the tension that comes with being an early bitcoiner. Should you trust third parties with your custody, and put your fate in their hands, which sort of goes against the founding ethos of crypto? Or should you "be your own bank," and risk losing your assets due to user error or subject yourself to "\$5 wrench" attacks?

The answer lies somewhere in between. A little bitcoin split in a dozen secure locations. A little held by the institutional-grade custodians. A little on crypto exchanges. And probably a little in web wallets and self-custodied hardware wallets. Today's wallets are GOOD, and will likely offer the upside of providing Uniswap-like retroactive rewards for early patronage. MetaMask is the most widely leveraged [browser wallet](#), with Ledger as the most [widely used hardware solution](#), and the interfaces on these and other crypto wallets are excellent.

[Zapper.fi](#), [Argent](#), and [DappRadar](#) have created A+ portfolio monitoring tools, and offer more intuitive portals into actual user participation in these portfolios than ever before. I recommend trying several over the holidays, in case I'm correct about these businesses becoming tokenized, and to familiarize yourself with the tools you need to access the next trend in DeFi next year. Wallets will be the "banks" through which users can quickly access the more exotic (risky!) early stage projects that come live through DeFi channels before they ever hit major exchanges.

## 10.6 Quants: A Company for Every Metric

"Do your own research" has never been easier or more fragmented. When it comes to crypto information, it's frustrating to navigate, but the data sets and the tools are there.

Binance has cleaned up [CoinMarketCap](#), and I particularly like the (long overdue) circulating vs. max supply changes on the homepage that provide a short-hand glimpse of how much selling pressure is to be expected for an asset over a certain period of time. On the other hand, CoinGecko killed it with its DeFi [support](#) this year, and now rivals CMC because of its speed and depth of new asset coverage. [Dune Analytics](#) has become a "github" for Ethereum queries and project specific dashboards, and [The Graph's](#) decentralized indexing server looks more like a Google for blockchains every day.

[Coin Metrics](#) remains the king of creating and cleaning on-chain data points across major blockchains (though [Glassnode](#) isn't bad either), while [Nansen](#) is our go-to for tracking token exchange flows and whale addresses, and [Token Terminal](#) and [DeFi Pulse](#) have started to bring tangible financial metrics to light for relative DeFi valuation comparisons. Out of the old guard, [Etherscan](#) and Blockchain serve as the block explorers of record. And Flipside has taken on the herculean [task](#) of attempting to normalize and rate assets by parsing the "real" activity in their developer libraries and on their blockchains.

[Kaiko](#) is our partner on high-fidelity historical and real-time markets data sets, while [Skew](#) has become the gold standard for accessing derivatives data.

If only someone could tie everything together....

## 10.7 Educators: News, Research, Marketing

The challenge with an exponentially growing market is twofold. First, it's critical that introductory materials remain incredibly simple when it comes to onboarding new users, since most people's knowledge of the industry is still at a middle school-level at best. We still need to walk people in, step by baby step. Second, it's impossible to cover the broad swath of innovations in the market even as an insider. I've covered this industry with freakish obsession for seven years (can you tell?), and Messari happens to have one of the largest, and best [research teams](#) in the industry. This report took me almost a full month to write, even with the full firepower of the most comprehensive information platform on the market.

It's hard to keep up, but there has never been higher quality information available to parse through the industry's esoterica. When it comes to news, you've basically got [CoinDesk](#) and [The Block](#) with the occasional side of [Decrypt](#). If you're looking for analysis, those platforms are now complemented by [Delphi](#), Messari, and a host of independent Substackers.

For 101 Bitcoin and macro content, Pomp was [on fire](#) this year, while macro investor platforms like Raoul Pal's RealVision joined the fray. I learned more from [Lyn Alden's posts](#) on monetary policy than I did in my undergraduate economics courses. Cami Russo's daily newsletter, [The Defiant](#); Ryan Sean Adams's [Bankless](#); and others have been excellent for tracking the emerging DeFi ecosystem. The Finematics [video library](#) of DeFi explainers has been the most valuable learning library I've used this year for scaling up on new DeFi projects.

If you know where to look, the educational content is there, and it's gotten very good.

## 10.8 Governance Tools

When people spoke about governance rights as key elements of 2017's utility tokens, they were usually blowing smoke. Things are trending in a different direction today. Protocols are "merging," and token economic parameters are up for discussion and amendment; governance platforms like [Boardroom](#) make it easier to participate in the voting process; and [tokens like CVP](#) serve as modern day proxy services.

Just about every project now has some sort of community governance, with non-binding [discussion forums](#) and voting resources, and binding voting procedures that dictate whether certain proposals pass. Tracking this is complex: a proposal hits a forum; there's signaling in the forum via an initial temperature checking poll; and then there's a formal vote (which can be weighted according to token holdings, "executive" rank or something else). But the whole process is a bit of a black box, and it's hard to study governance retroactively and analyze for best practices as a result.

The real governance "infrastructure" will likely be the courts, though. Real courts.

Arca's [activist play](#) with Gnosis provides one example. The firm has been [pressuring](#) Gnosis and its partner ConsenSys to [buy back GNO float at a premium to spot](#) because the original sellers hold more liquid treasury than the token is worth, and many of Gnosis's product releases sit far outside of the project's scope as outlined in early token sale documents. The

legal risk around token project communications continues to create tight-lipped founders (out of justifiable fear their good-faith disclosures may prove self-incriminatory), which means we're still battling the same opaque and "decentralized in name only" status quo we were three years ago in many cases. A good place to study actual decentralization is to simply "[follow the money](#)," and then the voting. We'll be doubling down on both in the new year.

## 10.9 Blockchain Monitoring

The dirty little secret in crypto is that most crypto networks are centralized at precisely the worst level: the network infrastructure layer. Crypto's [gini coefficient](#) (which measures the distribution of wealth) is... bad, but that should improve over time. Same with its mining and staking centralization issues.

It's the actual node infrastructure centralization that is particularly alarming. For a long time, Infura made the (Ethereum) world go round. That's changed, as companies like [Alchemy](#), [Bison Trails](#), [BlockDaemon](#), and others build crypto's equivalent to AWS, Google Cloud, and Microsoft Azure to host the lion's share of blockchain infrastructure as hosted services. It's still possible to run bitcoin and ethereum nodes yourself, but the odds are good you'll be interacting with nodes run by regulated enterprises or forensics companies like [Chainalysis](#).

Speaking of those guys! Hate it or love it, ~~the underdog's on top~~ blockchain forensics is big business. "Necessary evil" infrastructure that gets institutions comfortable with crypto and gives us a fighting chance in the battles ahead with privacy and self-custody.

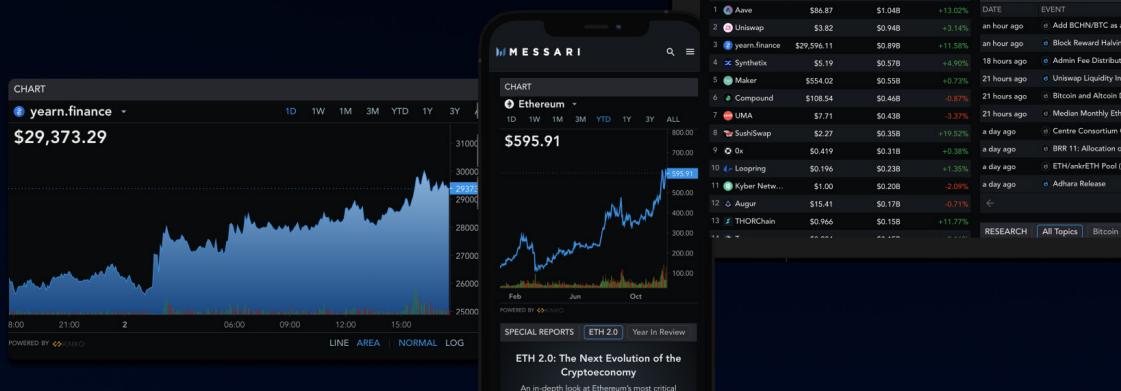
Chainalysis is [crypto's latest unicorn](#), having helped its 350 government and institutional customers check compliance boxes, and even track and seize assets. The company's "asset realization program" should piss a lot of people off. It's basically [crypto civil asset forfeiture](#) for which the company is getting paid a vig to "help agencies and insolvency practitioners handle, store, realize, and monitor seized assets" through the forfeiture process. It makes you wonder if the even bigger business for crypto forensics companies is on the tax remediation side of things.

My fear with the growth of forensics companies (and the coming global tax investigations into crypto users) is that people won't actually know how to reconcile their books with those spit out by the software providers used by tax authorities. In any remediation, a company getting a cut of incremental IRS collections would use less favorable accounting methods than a taxpayer-facing crypto tax software company, and have incentives to overstate the taxpayer's alleged shortfall. Fighting the difference will get expensive for taxpayers. (LAWYERS ALWAYS WIN.)

My pet theory is that crypto seizures will serve as a generational crypto transfer from OGs to big investors. Major money managers might not be able to source virgin coins from miners, but they'll at least get the born-again virgin coins from DoJ auctions. Bad for crypto anarchists, perhaps, but removing dark market holders and tax cheats and replacing them with institutional whales who bid on bitcoin via KYC'd [auctions](#) will help cripple crypto's "BTC can't be traced and is used for illicit activity" nonsense narrative. These aren't just seizures; they're epic institutional onboarding opportunities!

## GAIN AN EDGE OVER THE CRYPTO MARKET

RESEARCH | DATA | TOOLS



### 10.10 Messari: A Bloomberg for Crypto

We think crypto is a tool for free people, free thinking, and free markets.

In fact, it's the most powerful enabling technology for those forces since the dawn of the internet. And we help people make sense of it all.

The new **Messari** home page has quickly become my second screen, providing a watchlist, sector-specific views, fast charting, protocol events monitoring, and news and research curation in a single dynamic interface. Essentially, the mythical "Bloomberg for Crypto."

Our asset profiles are best in class; and we work collaboratively with top crypto teams on parsing the specifics of their projects, and keeping their profiles updated to reflect changes to roadmaps, key stakeholders, economics, governance, etc.

Our **charting tools** and **community screeners** make it easy to create and share evergreen resources that track KPIs across hundreds of data points. And our **real volume monitor** is one of the only ones that accurately reflects the industry's markets data without the hyperbole of foreign exchange wash trades or market pair double-counting.

Our 2021 roadmap is nuts too, so join Pro and never miss a beat. (If you're still reading page 110 of this report, and **don't sign up for a month** at least, I think I actually kinda hate you.)



**Go Pro for 20% off**

Access our industry leading research and  
Pro data tools

Offer code cannot be combined with other offers

USE OFFER CODE **THESES2021**

**Start Your Free Trial**

## Web3 & NFTs: The Digital Resource Economy

The flurry of hype we saw around non-fungible tokens (“NFTs”), digital resource tokens, and social monies late this summer was a brief glimpse of what’s to come next year in non-DeFi crypto applications.

Here’s how I think about the tokens that sit in the middle of my cryptoasset barbell, which [I first referenced in Jan 2018](#) (“non-worthless utility tokens: truly rare, mythical, beasts”): there’s computing substitutes, virtual work tokens, and digital IP tokens.

Computing resources like bandwidth and storage—those are fairly easy to price, and it’s easy to see why decentralized alternatives may be needed. On a long-enough timeline, everyone is at [risk of censorship or deplatforming](#). You may delete Facebook. Or get suspended for wrongspeak on Twitter. Your Medium article may get paywalled. YouTube may ask you to take down your xenophobic February 2020 coronavirus video warning people to avoid crowded places and wear masks. Your CDN may decide to censor your website.

Trillions of hours worth of valuable work (data) can be incinerated with the flip of various centralized switches. Not just behind China’s Great Firewall, but in the West too. A “new internet” starts to sound like more than a [Silicon Valley punchline](#), and these crypto-powered markets provide the “Airbnb for hardware” that will power it.

Digital art and collectibles are early, but obvious as well. You can see them and play with them, and as VR and AR ecosystems explode before our eyes, it’s intuitive that these gaming-driven worlds will spawn massive virtual economies for crypto players.

Reputation, follower counts, and network strength are all intangible but understandable representations of the value of the “work” we do online. There’s provable time, effort, and resources that go into developing that IP, even if the value is tricky to extract. Who wouldn’t want help monetizing their otherwise wasted hours shitposting on Twitter?

Web3 assets and NFTs encapsulate the essence of what Naval meant when he wrote that with blockchains, **markets would replace networks**. After DeFi, this will be the next great ecosystem of crypto investing in 2021 and beyond.

---

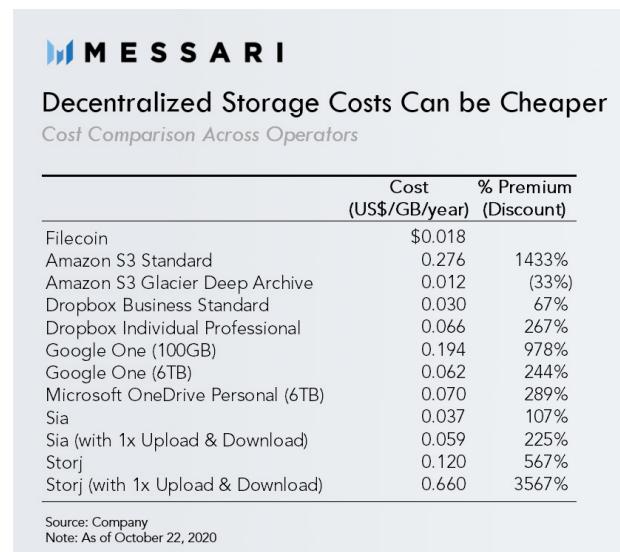
## 11.1 Filecoin, IPFS, and the Uncensorable Web

The biggest remaining risk to crypto right might not be “government shutdown,” but the fact that we lack decentralized hardware networks. Crypto’s ultimate scaling challenge will be breaking through state firewalls, their primary tools for stifling dissent and restricting “exit.”

Let’s talk about IPFS and **Filecoin** first, and then the rest of the decentralized hardware stack. Filecoin is a helpful starting point for multiple reasons. First, as of the time of this writing, it’s currently priced as if it’s the world’s third most valuable computing platform, behind bitcoin, and just barely behind Ethereum. At \$30/FIL, the implied fully-diluted network value of the project is \$60 billion. Dropbox, for reference, is an \$8 billion company.

Would I buy that valuation today? No, and as an early investor, I am (gradually) selling the rally. But Filecoin’s early success does highlight the value of breaking from the U.S. internet giants, and routing around censors. That prize is significant for a reason; we shouldn’t live in a world where our internet infrastructure lies completely in the hands of those who are otherwise engaged in a data grab of historic proportions. IPFS (the protocol) and Filecoin (the asset securing storage) could emerge as the encrypted and uncensorable backbone of the web.

You provide the IPFS network with provable commitments of storage capacity, and Filecoin’s novel new “proof-of replication” and “proof-of-spacetime” schemes does the rest, ensuring that storage is not “double spent,” and that the network has plenty of redundancies. Protocol Labs, Filecoin’s creator, estimates that storage costs are 15x cheaper than Amazon’s standard S3 storage.



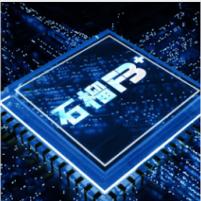
Filecoin isn't the only game in town, but its rivals (SIA, Arweave, Storj, etc.) are a fraction of the size, with 0.1% of the hype despite years of operations.

A good chunk of the game Filecoin won pre-launch was in its early network development, particularly in Asia, where committed miners scrambled to provision staked storage capacity to the early network. (Mira breaks down the [decentralized storage market](#) in greater detail.)

**M E S S A R I**

### Early Network Investment

Filecoin Mining Machine Price



**6Block F3+ Filecoin high-performance mining machine**

Price: **41300 USD**

Includes 1 set of machine + 1 year hosting, operation and maintenance cost

Sealing speed: 1000GB/day/set, 0.76 hour/sector (continuous optimization)

Effective storage: 336T

Estimated storage time: 210 days

Software service fee: 18% of Filecoin mining output

Hosting: T3+ level IDC

Contract duration: Signed once a year, property rights belong to the user

Stock: 999

Quantity (Limit: 50) - 1 +

Total Price: **41300 USD**

I have carefully read and accepted [Sales Agreement](#).

[Preorder Now](#)

Source: 6block, Twitter @juanbenet  
Note: As of October 15, 2020

### Miners Mostly From China

Largest Filecoin Mining Companies



How much would you pay to fully secure the internet from censorship? Filecoin provides today's [market rate](#) for that figure.

## 11.2 Other Decentralized Hardware Networks

Filecoin shows how you can intuit the addressable market potential and target network size for decentralized digital resource marketplaces. The unit economics of computing ([Golem](#)), video transcoding ([Livepeer](#)), VPN Network access ([Orchid](#)), long-range IoT device networking ([Helium](#)), or geolocation services ([FOAM](#)) can be similarly calculated on the back of a napkin, even if the winning protocols are not clear; or the path to capture those addressable markets is non-linear, and riddled with challenges and setbacks.

The non-storage digital resource market could get rerated 10x higher in the next market cycle if any of the primary networks can deliver applications that gain end-user adoption. Right now, Helium and its long-range IoT networking marketplace [seem like the early favorite](#) to breakout.

## 11.3 Content Scoring: Reddit, Twitter, and New Entrants

I wrote last year that I was cautiously optimistic about Twitter's Bluesky, [an attempt to decentralize the platform](#) that I thought might have some promise given Jack's embrace of bitcoin and free speech. That optimism was unfounded, as ten months after the original announcement, Jack said the company had still [yet to find a leader](#) for the initiative.

At least Zuck went all out on pushing Libra forward before getting stonewalled. Twitter doesn't even seem to be trying. Which is a shame, because I'd imagine Twitter could be the \*most likely\* social platform to successfully decentralize itself, and maybe even increase the value of its business with a data token. Three reasons this could be killer for Twitter in particular:

1. **Defensive transition:** Twitter, Facebook et al. are in society's crosshairs, fairly or not. One of the best (and fairest) proposals for regulating them is [Albert Wenger's idea](#) to tie Section 230 protections (prevents platforms from getting held to publisher standards) to whether a company provides a library of open end-user APIs. Forcing social giants to compete on the client layer would increase quality (even if most would still default to Twitter's client), reduce censorship, and potentially open the door to sharing platform economics with users.
2. **More data, better data, more value extraction:** every single user on twitter could build a better product than Twitter has. Just ask them. I'd even pay for multiple clients with the same Twitter API backend: maybe one with a smarter CRM, one that served as a better research tracker, one for anonymous trolling, etc. The point is: demand is there, and you could take the same core building blocks and network that Twitter has developed, and find new ways to both create and extract valuable platform data.
3. **User curation and credibility scoring:** In a twist of irony, Twitter's "blue check mark" system works as a pretty good negative quality filter. Twitter does a good job of curating tweets, but not people: the prioritization of media and celebrities for verified status often means generalists get recognized before specialists. Some of us do our own instinctive curation of source quality whenever we scroll, but it takes time to refine filters, and we end up mean-reverting anyway as the algorithm re-conditions us on "what's important." [Reddit's trial of "community points"](#) (per subreddit scores that could be earned for quality contributions, used in governance, and traded on Ethereum) was a glimpse of how a user curation system might work at scale. We really need to see more of this experimentation on Twitter too.

It's all setting up for what Balaji called the [rise of citizen journalism](#): valuable, platform-agnostic content that's specialist-produced, and curated according to value vs. clicks and time on site.

## 11.4 Citizen Journalism & Convexity

There are a few troubling trends in media: the first is increasing polarization and politicization of news; the second is that it's rare for a generalist journalist to outperform subject matter experts when reporting for any given topic; and a distant third is that the media industry lacks monetization models.

I doubt the last one is actually true (it's not that there's no money in producing valuable information, but rather that the media has largely lost product-market fit outside of infotainment), so let's focus on the polarization and specialization problems.

Regarding polarization, I liked Vitalik's framing of [Convexity vs. Concavity](#), a good lens through which to view politics and media (and crypto!) today. Convexity values moderation, compromise, nuance and case by case-thinking. This is an underserved market. Concavity is maximalism, focused on establishing and defending precedents, and avoiding slippery slopes. This is a saturated and cancerous market.

Our information diets today are chock full of soy and sugar and concavity.

One way to look at the "citizen journalist"-driven alternative is as another tech-driven accelerated trend. Some concave politicized content will always exist, but it will also be easier for free-thinker consumers to seek out nuance, thanks to better content scoring systems (see [Section 11.3](#)), and for free thinker producers to find self-selecting audiences that hungrily flock to them, as we've seen in the podcast-centric "Intellectual Darkweb."

Most convex thinkers will be specialists, but you'll have some virtuoso / polymath generalists who excel in learning, synthesizing, and curating. ([Eric Weinstein](#) comes to mind.) But "virtuoso" does not apply to 99%+ of any population by definition, which shows you how many of today's journalists will either wash out or bleed further into infotainment—the recursive snake eating its tail. Remaining "real journalists" will either be the radical truth-tellers (though the platonic ideal of a journalist has probably disappeared outside of comedy) or specialists.

The information marketplaces of the future will be staffed by those who narrowly specialize and write out of duty and indirect economic incentives vs. as a pre-selected occupation. Companies will produce their own media with skin in the game, while legacy media tribalizes further according to the tweaks Facebook and Twitter developers make to their algorithms.

If you want convexity, the future is a decentralized DNS + RSS + Tokens.

## 11.5 NFT 101

Let's better define one of crypto's most important primitives: the [non-fungible token](#). NFTs basically take data and turn it into liquid intellectual property. [That data could be art](#), virtual goods for games, reputation scores, raw bundled personal and commercial data, etc.

We produce a staggering amount and diversity of online content, and the good stuff will ultimately get packaged into parcels and relicensed through global peer-to-peer marketplaces. That seems rather intuitive and obvious, actually. It's just a matter of time.

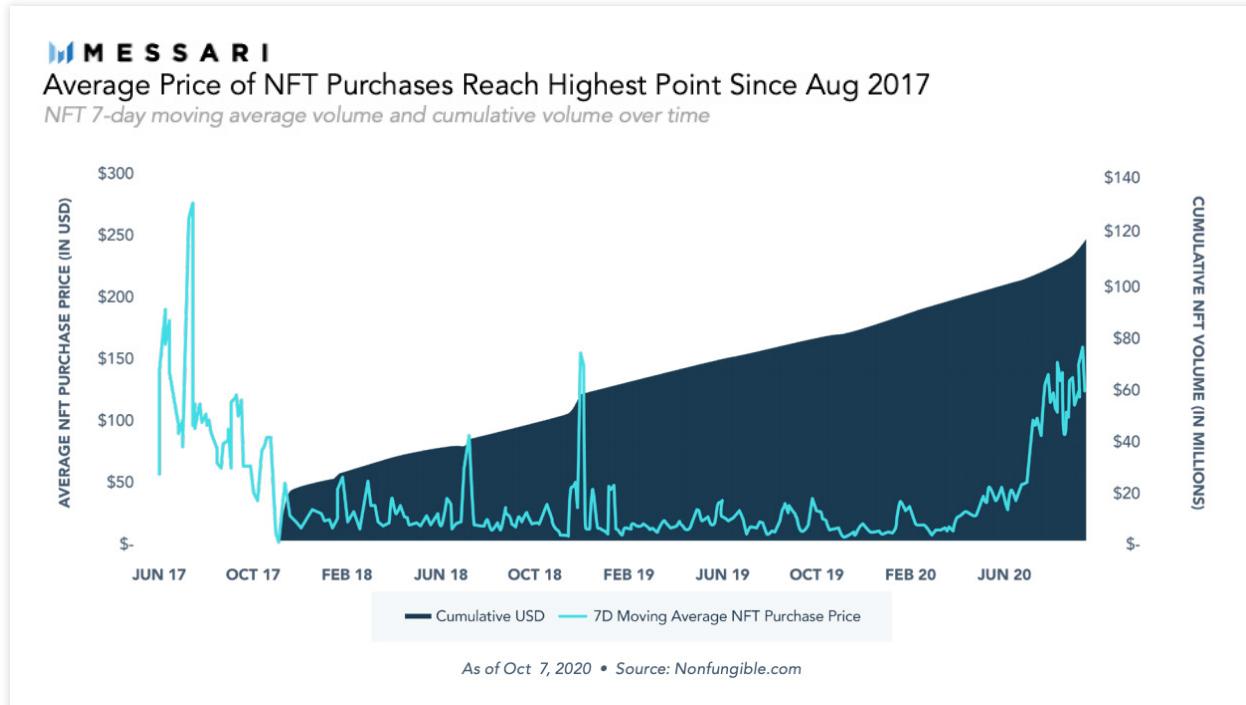
How long will these markets take to develop, though? I've been pitched on digital art platforms and digital rights management for music artists since 2015, and bringing those products to market has been slowwww. My sense is that we'll see NFT "killer apps" in order of tangibility: virtual goods in **gaming marketplaces**, then **social monies**, then **VR platforms** (and their applications), then intangible data relicensing.

NFTs change the default ownership of digital IP from the platform to the creator, which is why they seem powerful and inevitable. We're keeping our eyes peeled for open, creator-owned platforms where there's even a little bit of smoke.

Technically, there are three types of NFTs:

- ERC-721 NFTs are discrete individual collectible assets that have their own unique attributes (like the original "CryptoKitties" from Dapper Labs)
- ERC-1155 "semi-fungible" tokens offer classes of assets (**pioneered** by Enjin; think of a gaming marketplace that sells 1,000 interchangeable digital swords)
- ERC-998 "composables" are NFTs that may own non-fungible and fungible assets (e.g., a VR home that comes fully furnished with some fungible amount of food tokens)

Compared to the rest of crypto, NFTs are small potatoes. Low eight figures of sales since their birth in late 2017, even for the big platforms like CryptoKitties, Decentraland, etc.



Still, this is a sector that's going to get big fast, as VR/AR evolves, and more MMORPGs offer interoperability between games. I'm still wrapping my head around the potential of these primitives, but here's a great [primer on NFTs from OpenSea](#), and a post on [their investability from Mason](#).

## 11.6 There's Always Money in the (Digital) Banana Stand

If NFTs are securitized digital IP, the marketplaces are the investment banks. These platforms do the securitization work, govern the rules of the marketplaces, and collect their vig any time an asset is produced, traded, or tweaked.

When it comes to NFTs on Ethereum, the gas prices are too damn high, so there's an opening for more NFT-friendly blockchains to win this market. Many of the most promising NFT apps have frequent, low value transactions, and need a Layer 2 blockchain like Matic or a brand new NFT-motivated blockchain like [Flow](#) (built by the Dapper Laps team) to power their ecosystems. If you bet on NFTs as an innovative class of digital consumer goods, you might look first to the platform protocols that are jockeying to capture fees from unique digital asset creation, modification, and trading. But like DeFi, we ask: where will fees (and value) accrue? The platform protocol or the specific application marketplace? Here's my early read....

### I'M LONG:

- **Digital art marketplaces and collections:** Some \$64 billion of artwork changed hands in 2019, with a tiny fraction of that in digital art. Still, that market is growing quickly, and marketplaces like [SuperRare](#) show the money (15% primary sale and secondary commissions) in producing toys for those who would like to flaunt their virtual status. The [AI Generated Nude Portrait #1](#) sold for ~\$14,000 this year, a good sign for emerging artists that may dominate the digital art realm. Most people won't be collectors, but I'm excited for the equivalent of a VR/NFT Louvre, and pimping out my personal virtual man cave with exclusive art because I'm that much of a winner.
- **Memetic lotteries:** At some point, there will be social platforms that bill themselves as memetic lotteries. Become a gif, tweet a viral image, start a viral dance: win the lottery. Pieces of content that hit certain thresholds could be packaged automatically as NFTs, and then licensed out in a way where economics from impressions split between platform and creator. Imagine actually "winning Twitter" one day. Instead of everyone getting \$5.46 shared with them from Facebook, wouldn't you be more excited to potentially win a \$20k lotto with a viral post? This sort of NFT could also be useful in identifying talent. Serial winners vs. fifteen-minute-of-famers would be easier to spot.

## I'M SHORT:

- **Collateralized NFTs:** Bro, it's too early to collateralize your digital art, and create a subprime MBS-equivalent with CryptoKitties. These new markets haven't demonstrated any real liquidity or ability to retain value over time, and this is a dead end for the foreseeable future. But you can still take out ETH-denominated loans on platforms like [NFTfi](#), which sounds like liquidations-as-a-service to me. I'm only interested in this type of financialization once we're spending meaningful time in virtual realms. We might look for the first wave of these markets in real VR game economies (land, property, and virtual stores like casinos with the potential to generate cash flows). But mortgaging a VR casino requires the VR platform to work, the VR casino to get built, and the players to produce revenue for the house before the collateralization play makes much sense.
- **NFT Yield Farming:** The same yield farming craze that hit DeFi this summer quickly made its way to the NFT space as well, with Rarible's RARI and Axie Infinity's AXS token launches and liquidity mining programs sparking some early interest. Thanks, I hate it. If I'm yield farming COMP, it's because I want to generate yield on my dollars, and because I think yield farming will pull forward demand in crypto money markets. But yield farming in NFTs is like pushing on a string: you need people to care about digital cats before you token incentivize those marketplaces. The predictable short-term swell in trading activity and NFT prices from these liquidity mining programs was temporary. Borrowing my earlier DeFi analogy, these programs were like steroids without the lift.

One last note on marketplaces: I'm not sure whether vertical specialists or broad aggregators will win. There are specialists in curated digital art (AsyncArt, KnownOrigin, MakersPlace, and [SuperRare](#)), fashion and photos (Foundation and OurZora), and games ([Axie](#), Enjin); and some broadly-focused aggregators like OpenSea. On the one hand, OpenSea is working with the largest addressable current market. On the other, I'm not sure most people will go to the same marketplace to buy domain names, financial products, and virtual toys. Who's going to crack the Amazon online bookstore? Will that specialization allow any differentiated winners to emerge?

## 11.7 Social Money & Community Tokens

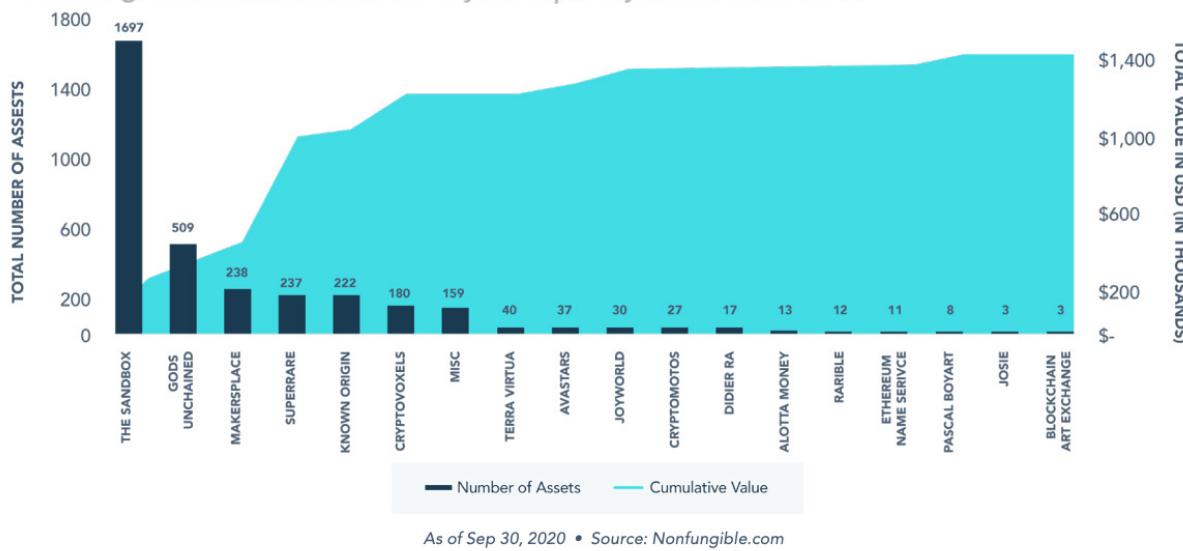
The social money / community token trend feels like one of those toys that will be absolutely hated by the crypto cognoscenti, but will be obvious in hindsight. I love them.

Today's experiments include things like [WHALE token](#), created by one of the largest collectors of digital art. Is this community token a worthless piece of shit, or did WHALE successfully index the budding (and otherwise illiquid) digital art market? You can use WHALE to rent the artwork from the creator's vault, or pay for their consulting services; or stake your own NFTs to the vault as part of a liquidity mining scheme. Pretty cool. (I know this slightly conflicts with my comments in the previous section, but I contain multitudes.)



## The Whale Vault Portfolio Now Holds 3,443 Assets Totaling \$1.4 Million

*NFT categories in WhaleShark's Vault by total quantity and value of assets*

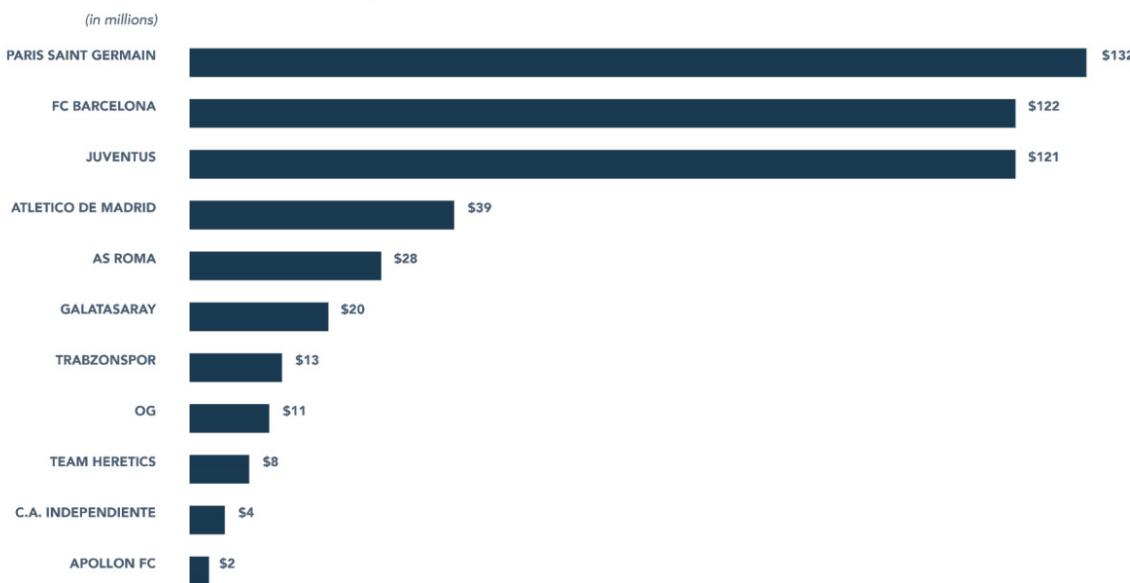


How about [Chiliz](#), a fan engagement platform, whose individual “fan tokens” and platform token have swollen to a collective nine-figures market cap? It’s already partnered with ten international football clubs (see how worldly I am, using “football” like that?), like FC Barcelona and Juventus, to engage token holders with rewards like signed merch, tickets, events with players, and social recognition. The company behind Chiliz, Socios, may build an e-sports league that leverages the token in the future as well. Seems cool.



## The Top Three Chiliz Fan Tokens Fully Diluted Value Exceed 120 million

*Chiliz fan tokens by fully diluted market capitalization*



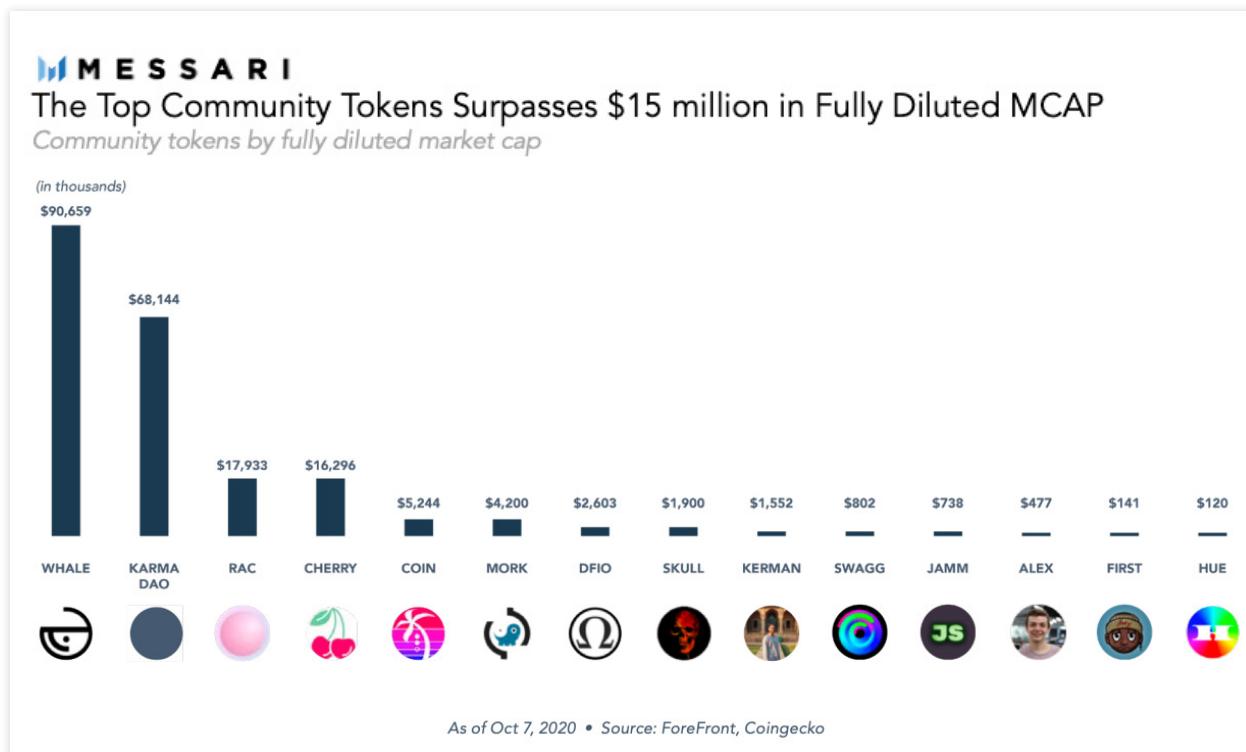
Meanwhile, platforms like **Roll** (disclosure: I'm an investor) could help blast open the design space for the monetization of human capital. **One obvious one:** funding open source developers, where devs issue tokens, hold some, distribute some to other contributors, then prioritize bug fixes and feature upgrades by token purchasers (e.g., big companies). It's a spin on the freemium business model, and may help further monetize open source development work.

If you don't like this theme, I don't know what to tell you.

Blockade Games's CEO Marguerite deCourcelle has \$COIN for access to her Neon District e-Den. Alex has, well, \$ALEX to let you "control his life". Pretty soon, more celebrities will ditch their proposed income sharing securitization schemes, and figure out what Akon already has: the real money is in social currencies.

Guys, there's literally a **TikTok housing project that just went public**, so the time is right for us to think about ways to introduce crypto monetization schemes for the nouveau important without forcing them into becoming serfs at LA's "talent houses." What happens when those influencers don't want their tweets, snaps, and stories farmed anymore? They'll launch "social currencies," whose potential applications (and aggregate values) are limitless.

We'll see some eight-figure celebrity tokens (**RAC already has** on a fully diluted basis), and nine-figure brand tokens in the next two years.



## 11.8 VR Interior Design

We might be one breakout product away from VR/AR tech going mainstream. The Oculus has gotten scary good, but you still feel like a loser wearing it. My guess is that COVID-induced lockdowns and travel bans have given the VR/AR industry rocket fuel, as more socialization (meetups, conferences, Vegas!) moves online, potentially permanently, but people grow wearier of Zoom by the day.

It may soon become a status symbol to have custom VR digs (complete with digital art collections and custom 3D designs as I alluded to in my winner's man cave). 3D interior designers become one of the most sought after contractors for the citizens of the metaverse.

Decentraland, The Sandbox, and Cryptovoxels have been the most popular apps in [crypto's metaverse space](#), but it's not for their graphic design or game prowess thus far. It's about the proof-of-work (capital) virtual settlers have ploughed into the new frontier, which creates a schelling point around which like-minded groups can congregate and build new community applications.

A common critique of these projects is something like this: "[Decentraland may be a pretty cool experiment, but could the game developers simply beat them at their own game?](#)"

I used to think that, but it's no longer so obvious to me. No central game developers that I know of have really embraced the laissez-faire approach of crypto's metaverse creators, and let the VR frontier run wild. Decentraland, on the other hand, [launched an Aragon DAO](#) responsible for governing auctions and whitelisting new NFTs, its [MANA](#) can be used as MakerDAO collateral, and parcels of LAND can be mortgaged on Ripio (again, I think VR land marketplaces may be the exception that proves the NFT collateralization rule). Open economies could attract a new tribe of "gamers" outside of gamers. I think this because I'm not a gamer, and yet, I've been spending more time thinking about and dabbling in the metaverse.



As for tangible predictions, I think virtual worlds like [Axie Infinity](#) and Decentraland will go vertical as well, tripling to \$75 million next year.

## 11.9 VR Interior Desire (Sex, Fear, Greed)

So you've [built yourself a virtual world](#). Now what do you do there?

Sex workers are usually ahead of the curve. My sense is that [SpankChain's](#) native currency "booty" was too fungible. Do you really want the sex worker or patron experience to seem *fungible*? Not very sexy. NFTs could help elevate status for sex workers and their supporters alike, and I'd imagine you'll see more status games (and velvet ropes) in VR-powered sex applications. I haven't done a ton of research here, but I will the next time my wife takes the kids to my in-laws.

Sex is great, but have you ever been able to play poker with your friends mid-pandemic?

I don't know about you, but I'm fiending for Vegas in the cloud, and I could see VR gambling being an order of magnitude bigger than "online gambling" because the combination of voice, 3D movement, and avatars feels more like actually hanging out. [Decentral.Games](#) seems like the most promising VR gambling application, and its casino has one of the rare NFT-tied liquidity mining programs I like (because it's tied to real money gambling!), and historically owning shares in early crypto casinos has been a winning play (SatoshiDice, ICOs, Yield Farms, etc.)

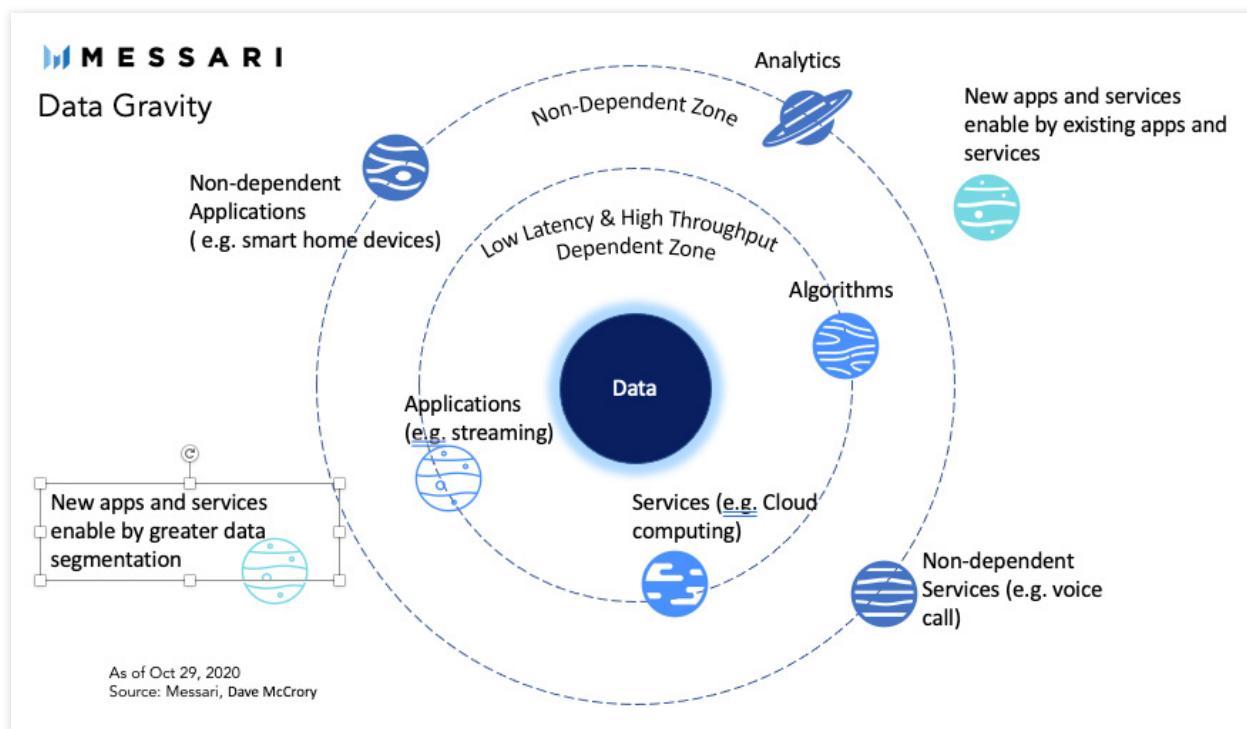
There's a whole crop of VR users who might be exiting to the cloud for less controversial reasons—they may just want to socialize pseudonymously. Something more than Twitter, but less personal than conferences (assuming they ever come back). There's an entire class of NFTs dedicated to persistent online identity and reputation. The most notable are around domain names ([Ethereum Naming Service](#), [Handshake](#), Unstoppable Domains), with naming services as the third largest "asset class" in NFTs after gaming and digital art. Those usernames may look like vanity plates today, but they'll be persistent identities in crypto VR.

## 11.10 Data Marketplaces & Gravity

Most data in its raw form is pretty useless. It only gets interesting and valuable when there's a lot of it, and it's labeled and parsed for valuable insights into trends, users, or behaviors.

Here's the problem: starting any "big data" project from scratch gives you a cold start problem—there's not enough data, and when there is, **it doesn't have much "gravity."**

Marginal data is less valuable to a crypto network than it is to a tech monopoly, so even if we're splitting the spoils with users, it won't be much.



There's three potential ways that crypto might be able to scale miscellaneous big data markets though. The first is on providing data to user-centric platforms: think Gmail (filter your promotions, and get you to inbox zero) vs. a newsfeed (optimized to hog your attention and sell you shit you don't need). The second is through the use of data marketplaces, like Ocean's, that have **built automated market makers for data sets**, and created markets for otherwise illiquid (but valuable!) data sets like self-driving car data, genomics data, or browsing data. The third might be something that revolves around data competitions.

**Numerai's Erasure** does implicit quality assurance on its platform's data sets, by introducing encryption and something better than a money-back guarantee: "slashing" for bad data.

I have absolutely no idea which of these data marketplaces will be first to hit escape velocity, but when they do, they'll grow the data services pie, and skew economics further towards the data creators and curators vs. the platforms.



## Bridging Opportunities in Global Crypto Markets

When Satoshi breathed life into the concept of Bitcoin, it opened the doors of opportunity and fundamentally shook down our deep-rooted beliefs about currencies.

As the interest in investing in cryptocurrency rises, crypto lending - one of the most compelling services within the cryptocurrency world - was born. Lending enhances liquidity, improves market efficiency, and ultimately fuels innovation for the entire industry. It was under this vision that Babel Finance, a global leading cryptocurrency financial service provider, was founded.

Lenders play a critical role in promoting market efficiencies and they do this in different ways. When Babel Finance first started out in 2018 by Flex Yang and Del Wang, the Asian mining market was largely in disarray. It was a difficult time to get capital and the interest rate was notoriously high, at more than 20%. Babel Finance believed that providing affordable financing to crypto miners would enable them to thrive and alleviate the hardships they would have otherwise faced in getting this much-needed capital.

Babel Finance's belief paid off. By supplying stablecoins to miners and Bitcoins/Ethereum to Western crypto financing institutions, Babel Finance is effectively bridging Eastern miners with Western financing institutions, opening the doors to exciting opportunities in global markets.

Fast forward to today, the market lending rate to Eastern miners currently sits at a comfortable 6%. Babel Finance's total originating stablecoins loans to miners hit US\$543 million since 2018, which makes it Asia's largest. In addition, the outstanding loan to miners is currently US\$207 million (including US\$22 million in equipment financing), injecting robust liquidity and improving the efficiency of the crypto market.

On the other side of the world, Western crypto-financial institutions have also enjoyed the growth of the Asian market thanks to Babel Finance's help with sourcing Bitcoins from Asia. As of today, an equivalent value of

more than US\$500 million in BTC/ETH has been supplied by Babel Finance, to help the world's leading firms to capture the top two 'worst kept trade secrets' - Grayscale arbitrage and DeFi Farming.

The work of improving the market's efficiency doesn't stop here. Babel Finance also works closely with Asian trading firms to lower funding costs and at the same time, improve capital efficiency. For example, Babel Finance assisted an arb & delta neutral trading firm capture a stunning opportunity in early December. Babel Finance lowered the annualized basis spread, effectively adjusting the spread to a more sustainable level. It was a win-win deal for all.

The good acumen of market movements and a swift allocation of resources enabled Babel Finance to lend as much as US\$30 million in less than two days to the arb & delta neutral trading firm so that they could lock in this golden opportunity.

Babel Finance is making a bigger impact today. Recognizing the fact that many crypto investors lack access to professional products and services enjoyed by the investors in the traditional financial industry, Babel Finance pushes for innovation across all of its product lines.

As a global top options trader with a monthly average trading volume of more than 100,000 BTC, Babel Finance provides its clients with multiple lines of professionally structured yield enhancement asset management and hedging products. A record high in Asia of more than 100,000 BTC has been subscribed to Babel Finance's crypto asset management schemes in the last half-year.

Babel Finance believes every great invention such as Bitcoin relies on a group of actors who are responsible for taking care of and maintaining the smooth functioning of the ecosystem in good faith. The crypto market is still young, but the demand for deposits and originated loans continue to grow. Looking ahead, Babel Finance has only one goal: always put its clients first and have their best INTERESTS in mind.

[Learn More](#)


We have your best INTERESTS in mind

# 12.0

## The Final Boss: Exiting to the Network State

Crypto has made it to the “final boss” in the monetary game of thrones. So let’s dissect a fan favorite bit of FUD (fear, uncertainty, doubt): can countries ultimately “ban” bitcoin and crypto? How and where would they even start? Bitcoiners may scoff at this subject, but I believe valid points of concern remain. To begin, we should agree on the precise scope of what constitutes “crypto,” how sovereign threats differ by region, and identify the attack vectors and magnitude of the potential threats.

---

### 12.1 Money as Bookkeeping

An interesting place to start this discussion goes back to “what is money?”. Whether you believe in money as a commodity, a form of state issued legal tender, or a byproduct of the credit system, you’re right. But for policy purposes, my favorite reconciliation of the “what is money?” question comes from Placeholder’s Mario Laul (who has written an [impressive catalog](#) on crypto governance more generally): money is a [social institution](#) for bookkeeping.

What we’re really arguing over is NOT whether the state has a monopoly over money; it does, and we can and should expect to continue rendering unto Caesar that which is Caesar’s.

Instead, we should be focused on whether it remains legal to maintain and recognize books outside of the state’s watchful eye.

*That’s* where we begin to get into Bill of Rights territory in the West (Money is speech! Encryption is defensive arms! Surveillance is unreasonable search!), and maybe irrelevant territory in the East. But if you’re talking about commodity money, the West has generally been unconcerned with whether you pay for a service with gold, bartered services, or Chuck E. Cheese tokens—only that you report transactions and associated taxes as a result.

It's here that crypto's volatility has been a blessing, as it seems difficult for states to argue that 12-year-old digital commodity money is a threat to monetary sovereignty. When seizures of gold deposits were blessed by FDR in the '30s, gold represented a de facto form of legal tender; the physical gold was relatively stable and backed national currencies.

To forcibly seize bitcoin, though, would be tantamount to book burning—a government-attempted manipulation of a global ledger of record.

[Laul writes](#) that whether the ledger asset accounted for on a blockchain is commodity money, like gold (or bitcoin), stablecoins that represent claims on bank deposits; or central-bank digital currencies, the "communal, institutionalized memory" is the innovation. I'm not sure that's something even the U.S. with all its might can strip away, so long as bitcoin nodes exist in space and time. The millions—and soon billions—of people who trust Bitcoin do so because they trust the institutionalized memory encoded on its ledgers; the "21 million unit" hardcap was simply a carrot to incept that memory.

## 12.2 Western Bias & Chinese Fear

One of the biggest takeaways you may have from this report is that it presents a Western view of the crypto industry. That's true for a few reasons.

First, Messari is a U.S.-based company.

Second, let's level set: crypto is global in relevance, but Western in its origins. Satoshi was anonymous, but almost certainly from the West, so were the early cryptographers who gained early exposure to and contributed to bitcoin; Ethereum was developed by Westerners; Ripple and Stellar were born in Silicon Valley; Tether and USDC creators hailed from the States even if their usage and domiciles are now "global"; Sergey Nasarov (Chainlink), Charlie Lee (Litecoin), Charles Hoskinson (Cardano) are all American. The Western bias is warranted.

And let's not beat around the bush! The third reason there is Western bias in this report is that I'm skeptical that a free and open crypto ecosystem will ever truly take root in China, and the rest of the major Eastern crypto markets (Japan, Korea, and India) are too unique for me to draw generalized conclusions (though we dive deeper into each Eastern market [via our Pro research](#)). Far from painting the East with a broad brush, the reverse is true: I stick to Europe, Canada, the U.S., and even Latin America, because their differences there seem smaller, and their approach to crypto more generalizable.

We certainly can't (and don't) ignore China altogether, but at some point, we're going to have to come to grips with the fact that China is just as likely to emerge as a dominant player in the crypto economy as it is to become a ticking time bomb that actually threatens it.

Perhaps many Chinese citizens are into crypto, but the probability of crackdown at any given time is high, and there is no size a Chinese crypto incumbent could reach that would make them too big to jail. If the [detention of Huobi and OKEx executives](#) this year didn't convince you of that, the [public taming of Jack Ma](#) and the Ant Financial's cancelled IPO should have.

I don't think you need to venture into tin-foil hat territory to acknowledge that crypto undermines the degree of control and state surveillance the CCP currently enjoys. I scratch my head at those who doubt the capacity of such a government—one that literally built a great firewall around its internet—to seize bitcoin mines, jail executives, and criminalize bitcoin custody by decree. I'm not saying it will happen; I'm just saying that there are no constitutional checks in China that prevent it from happening, so it's tougher to handicap the risk vs. the West.

In the meantime, we need to believe China when its leaders tell us they are going to replace dollar hegemony by [winning the CBDC market](#), and replacing the U.S. in [massive global trade deals](#). Until then, the bigger crypto question becomes: what's going on in the West?

### 12.3 A Western Temperature Check

As long as there are [good machines like Ray Dalio](#), who remain blissfully unconcerned about the rise of the surveillance state, I'll be concerned about crypto's legal status in the West, too. There are generally five attack vectors where we need to shore up our defenses around crypto "bans": private transactions, self-custody, banking integrations, network participation (i.e., staking and node operation), and synthetic usage.

I'll look at each of these in turn, but first a bit of good news: I am encouraged by the emergence of the "[crypto insurgency](#)" in D.C., and I view a Biden administration with a divided U.S. government as a goldilocks scenario for Bitcoin's ability to continue hiding in plain sight and grinding out progress in our decades long turf war. A divided Congress limits potential legislative damage, while regulators at the OCC (Brooks), SEC (Peirce), and CFTC (Talbert) ensure that crypto-friendly voices will remain prominent at the relevant regulatory agencies.

The Biden Administration, for its part, will have its hands full rebuilding the executive branch, and addressing higher priority items like eliminating the coronavirus threat, getting the economy back on solid footing, and advancing its domestic social agenda and global diplomacy reset. Perhaps a divided government will curb the pace of fiscal stimulus, but the Fed won't suddenly fall asleep at the wheel after a year of unprecedented monetization, especially as former Fed Chair Janet Yellen takes the helm at Treasury.

In the meantime, it's on us to ensure federal and state legislators don't nuke the industry.

We'll continue tilting at windmills to "educate the electeds" if for no other reason than to [slow them down](#) from their worst impulses. It's one of the reasons we're excited to work with the [Chamber of Digital Commerce](#) on its educational campaigns for Congress (including its most recent initiative, [Crypto for Congress](#)), and have continued to support [Coin Center](#), which has been doing herculean work on the privacy front.

Which is where our greatest threats may lie.

## 12.4 The Enemy at the Gates: FATF

The fear over the use of encryption extends far beyond the use of cryptocurrencies, as more authorities around the globe grapple with the challenges posed by end-to-end encryption. Apple has gone to battle for its users here. Will application providers like Signal and Whatsapp be able to [defend themselves similarly](#)? How about regulated crypto enterprises who follow the relevant Bank Secrecy Act laws, like AML/KYC, but now face a choice as to whether they can even support "anonymity-enhanced cryptocurrencies" at all?

[Last year](#), I wrote about Zcash as a canary in the coal mine for the state of crypto's support of encryption. I still believe that's true, as it is the only cryptocurrency that preserves near perfect privacy for selected transactions, but also provides surveilability similar to bitcoin when it comes time for users of that protocol to interact with the regulated financial system. The future of crypto privacy hinges on whether authorities take the unprecedented step of extending the "travel rule" from know your customer to "know your customer's customer's customer, etc., and thereby taking on risk associated with "losing" traceability of an asset's chain of custody if it were to have ever touched a foreign address, peer-to-peer exchange, mixer, gambling application, or other unfavored source.

Essentially, it's blacklisting 90% of the \$100 bills with cocaine on them. (It's funny that cash is the primary culprit of bad activity, and yet congresspeople are trying to force [fully-backed stablecoins to register as banks](#). It's fucking hilarious.)

In theory, these are constitutional law questions. In fact, how many crypto services will take a chance on flouting [thinly veiled warnings](#) like this:

*"The Department of Justice considers the use of AECs to be a high-risk activity that is indicative of possible criminal conduct. In most circumstances, the Department does not liquidate seized or forfeited AECs, as doing so allows them to re-enter the stream of commerce for potential future criminal use. Companies that choose to offer AEC products should consider the increased risks of money laundering and financing of criminal activity, and should evaluate whether it is possible to adopt appropriate AML/CFT measures to address such risks."*

Law firms have scrambled to address the cliffhanger presented by this loaded comment: [how indeed can companies support AECs](#) in light of their apparent risks. My answer is simpler: AECs present significantly worse usability than banks for laundering money because of the need to interact with regulated financial edges, which (as we just discussed) have gotten pretty good with their forensic accounting. Again, it's [better to use banks](#).

## 12.5 Swiss Banking in Your Pocket

It didn't take long for Compound's legal head Jake Chervinsky to be proven right. Jake wrote the [must-read thread on privacy and self-custody](#) earlier this year, which he called out as the real battlefield for the industry. We can deal with the challenges presented by exchange regulation, and how they monitor and facilitate secure private transactions without jeopardizing compliance. But we can't survive a blacklisting of self-sovereign wallets and contract addresses.

According to Coinbase CEO Brian Armstrong, [that enemy is now at the gates](#).

The outgoing Treasury Secretary seems keen to "rush out" new regulation that would block withdrawals to unknown addresses from regulated crypto wallets, essentially necessitating a whitelist of remittance recipients, single-use personal addresses (best security practices), unverified merchants (who would be impossible to register en masse), and smart contracts (which are not individuals and are not controlled by individuals once deployed). This would conveniently replicate modern banking's accessibility issues, and create a two-tiered system of crypto financial services. At best, they'd be cumbersome and ineffective, simply adding a single step to crypto transactions where a hosted wallet user would attest to their ownership of a registered self-custodies wallet before going about their merry way in DeFi.

Armstrong noted this would kill emerging use cases for crypto outside of the U.S.-blessed walled garden. USV's Fred Wilson framed these wallets as the [new web browsers](#), interfaces that open up access to a decentralized financial system to start, but ultimately reduce reliance on our tech overlords as well. Coin Center posted a piece called "[How I Learned to Stop Worrying and Love Unhosted Wallets](#)" from a former DOJ anti-money laundering chief, who considered the unintended consequences of unhosted wallet restrictions, namely that more crypto transactions would get pushed to the shadows, and non-custodial crypto wallet infrastructure would witness a boom in investment.

This shouldn't be surprising. [FATF noted](#) that "lack of explicit coverage of peer-to-peer transactions...was a source of concern," while the Bank for International Settlements called "full anonymity [through private wallets] not plausible." The Swiss effectively prohibit self-custody by requiring owners to verify ownership of their private keys (FATF likes that); Singapore has incorporated similar policy. Spain is [forcing disclosure of all crypto holdings](#), which is the logical next step beyond the IRS's convenient tax form question.

As Fred said, “it will take everything the industry has to push back on this temptation.” Usability, privacy, and fungibility are effectively dead without some serious reversals in this battlefield, and I’m worried Ben Hunt [will ultimately be right](#): “in five years it will be illegal for an American citizen to transact in Bitcoin outside of a federally registered exchange and without a federally registered account.”

## 12.6 Bitcoin Banking

God, I love banks. The bitcoin banks, that is.

Last year, I [highlighted the existential risk](#) the regulated banking system posed towards crypto. At the time, there was basically just Silvergate and a smattering of other small regional banks serving the industry’s regulated edges. Now, there are several different \*types\* of banks entering the fray. The “challenger” banks like Silvergate are doing well (the Silvergate Exchange Network processed \$36 billion transfers in Q3 of this year); Wyoming’s banking regulators licensed Caitlin Long’s [Avanti](#) and [Kraken Financial](#) as Special Purpose Depository Institutions capable of accessing the Federal Reserve’s deposit window (while [offering full auditability of their reserves](#)); Paxos Trust Company now serves as the bankend to several of the largest stablecoin issuers and new fintech entrants; and the OCC [opened the door](#) for major banks to enter the crypto custody space race and bank synthetic, regulated stablecoin issuers.

Once the major banks enter the custody fray, bitcoin may be here to stay. Wall Street will bring new risks (rehypothecation, address whitelisting, etc.), but at least we won’t lose our ability to apply for a mortgage or access a checking account simply because a bank discovered our Coinbase account.

## 12.7 Illegalizing Participation

ASIC mining’s concentration in China is suboptimal, and Iran’s [spiking interest in the sector](#) is not great, Bob. But those are known headline risk issues more than they are practical risks. Instead, I worry more about the unintentional criminalization of network participation. There are a few forms this sort of regulation could take.

**Mixers:** In particular, I’ll be looking at the language in the rulings that stems from the Helix money laundering case. The “crime” was somewhat obvious and in your face (the Helix proprietors explicitly partnered with DarkNet market operators to tumble bitcoin transactions, so there wasn’t much plausible deniability to go around that “code was protected speech”), but the DoJ didn’t seem to discriminate against Helix for operating a custodial vs. non-custodial mixer, either. You can imagine the U.S. will care less about “who has permissions to the mixers (or smart contracts)” than “who profits from them.” [Keep an eye on language here.](#)

**Staking clients:** How about the “unlicensed” operation of node and staking clients, which could be deemed money transmitters under more aggressive interpretations of the law. (Do you tip to “transaction processor” if you hit a certain scale in staking?) I think that’s unlikely,

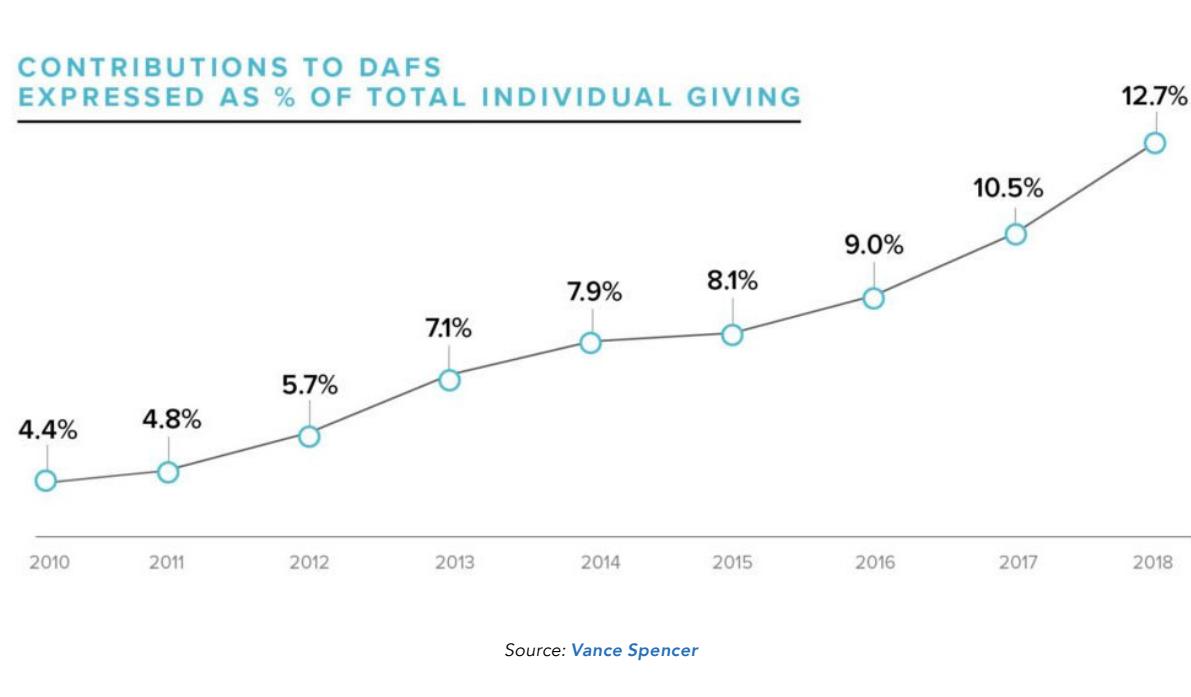
as is the idea that staking-as-a-service companies run into securities law issues, or that most governance tokens get painted with a broad Howey brush. BUT, let's look at the facts: staking includes a) an investment of money with the risk of financial loss (slashing), b) under what the SEC has already ruled "a common enterprise," c) that includes liquid "staking rewards," which are sorta dividends to passive token holders that otherwise d) delegate their validation and staking responsibilities to third parties.

The [Blockchain Association](#) argues that "classifying staking service provider arrangements as investment contracts does not advance the intent of the securities laws," but when has that ever stopped the SEC from doing something short-sighted in crypto?

## 12.8 It's Good to Be Well-EnDAO'd

I just spent several pages railing against the existential threats policymakers pose to crypto, so let's stick it to them, and avoid sending them taxes, shall we?

Not many people know this, but before I got into bitcoin, I started a charitable payments startup that built a donor-advised fund. The specific startup details aren't important, but what you should know is that DAFs are tax-efficient charitable vehicles in the U.S. that allow donors to contribute tax-deductible donations of non-cash assets like stock or property, and write off the full market value of the gift *while also avoiding capital gains tax*. These are sort of like mini-foundations in that you can shelter the money now, but grant from the vehicle over time. And not only is it 100% legal, it's a big business that was pioneered by Fidelity (who also accepts various types of crypto donations for its DAF).



I actually shopped the idea for a crypto pivot of my startup ("Good-Bits!") around the investor space when I first started jetting around bitcoin conferences in 2014, but it was too early; I joined DCG instead, and wound down the DAF. I've always loved the concept of what a crypto-powered foundation could look like though, and now we have an early answer [thanks to Vance Spencer](#) (Framework Ventures) and his colleagues at [Endaoment](#). If you live in the U.S., talk to your tax peeps and fork over some moon gains to support your favorite charities this holiday season, and keep the taxman away from as much of your money as legally possible.

## 12.9 The Network State

Finally, I've been fascinated with the concept of "exit" ever since I watched Balaji's [seminal presentation](#) on the subject in 2013. How do we retain the right to peacefully quit a given system when it no longer aligns with our values?

When you leave a company, you can join another or start a new one. When you leave a social network, you can join another or start a new one, though that's much harder. But when you leave a state, you need to move to another existing state; there's no more unclaimed dirt, so starting a new state isn't really possible. If you want to move from SF to avoid all the human excrement and needles, you have to pick a new city, like Austin. If you don't like the U.S., you can renounce your citizenship, emigrate, and pick another country, like Portugal. But you're still opting in to another state or country's rule of law.

Does crypto provide the missing tools to make it possible for people to [form a new country](#), a real country that might actually be recognized by the U.N., for instance?

The historical options for exit: elections, revolution, and war, as well as modern libertarian proposals around seasteading, space colonization, and micronations. But Balaji is thinking of how to boot up a more serious "nation-state" by starting with a community in the cloud (through online or VR networks), that later physically consolidates in enclaves across various cities (Balaji calls them "cloud embassies"), and that ends with a purchase of actual dirt. There's no modern precedent for it, but that doesn't mean it's impossible. It's got me thinking.

There seem to be three primary challenges in bringing this to fruition: 1) going from digital to physical co-location, which might get easier or more attractive over time as states and countries experience currency failures, economic dislocations, or significant social and political unrest; 2) determining admissions standards and "dual citizenship" rules (perhaps the most solvable problem, as you can treat these communities like a university at first), and some countries like Estonia already offer [e-residency as a service](#); and 3) ensuring that the new population is gender-diverse. No one will want to emigrate to the LARPy nation of nerdy dudes, so diversity would literally have to be enforced. (This might be the winning case to make even the most chauvinistic bitcoiners when it comes to promoting women's participation in the space.)

At the end of the day, separating money from state *is* the core invention that would make it possible to emigrate to a new sovereign state with new laws (and tax policies).



## That's a lot. Thanks for reading.

Jeffrey Epstein didn't kill himself, but I might if I ever have to write again.

Just kidding (maybe). I love crypto. I hope you enjoyed reading this as much as I hated writing it.

Happy Holidays, and To The Moon!

– [The TwoBitIdiot](#)



MESSARI PRO

## Professional grade crypto data & research

Exclusive long-form daily Research • Advanced Charting features and metrics

Advanced Screener features and metrics • Downloadable CSV Data

Go Pro for 20% off

Access our industry leading  
research and Pro data tools

USE OFFER CODE **THESES2021**

Start Your Free Trial

The screenshot shows the Messari Pro mobile application interface. At the top, there is a navigation bar with tabs for "Watchlists", "Chart", "Screener", "Feed", and "Intel". The "Feed" tab is currently selected. Below the navigation bar, there is a search bar and a "WATCHLISTS" section. The "WATCHLISTS" section displays a table with the following data:

NAME	PRICE	MCAP	% CHG
Bitcoin	\$18,870.15	\$350,778	+39.86%
Ethereum	\$588.71	\$66,438	+54.59%
Polkadot	\$5.23	\$4,618	+30.28%
Cosmos	\$5.31	\$1,108	+15.93%
Uniswap	\$3.82	\$0.948	+66.64%
yearn.finance	\$29,596.11	\$0.898	+186.68%
Zcash	\$74.74	\$0.798	+37.73%
Synthetix	\$5.19	\$0.578	+100.69%

Below the table is a chart for Bitcoin with a price of \$18,870.5. The chart shows a significant spike in price around May 2021. To the right of the chart, there is a news feed with various crypto-related events listed. Some of the events include "Add BCHN/BTC as a Price Identifier (UMIP 23)", "Block Reward Halving", "Admin Fee Distribution", and "Uniswap Liquidity Incentive Plan".

Offer code cannot be combined with other offers

# About Messari

Messari is the industry's leading market intelligence company focused on the digital asset ecosystem. Our **tools** and **research** solutions provide customers with actionable insights to confidently make decisions in the fast-moving cryptoasset space. Since our inception in 2017, we've built strong relationships with the industry's top thinkers, investors, and builders from today's most promising projects. Learn more at [messari.io](https://messari.io)

## Disclaimers

The contents of this report were created by employees of Messari, Inc. This report reflects the opinions of the authors and does not represent the opinion of Messari, Inc. The authors may hold cryptocurrencies named within this report.

This report is meant for informational purposes only. It is not meant to serve as investment advice. You should conduct your own research, and consult an independent financial, tax or legal advisor before making any investment decisions. Past performance of any asset is not indicative of future results. Please see our [terms of use](#) for more information.

Advertising and sponsorship do not influence editorial decisions or content. Third party advertisements and links to other sites where products or services are advertised are not endorsements or recommendations by Messari. Messari is not responsible for the content of the ads, promises made, or the quality or reliability of the products or services offered in any third party advertisement.

M E S S A R I

