
CRYPTO THESES FOR 2020

MESSARI RESEARCH

*The 120 People, Companies, and
Themes to Watch in Bitcoin,
Ethereum, and Beyond*

Table of Contents

- I. [History and Disclaimers](#)
- II. [Top 10 People to Watch](#)
- III. [Top 10 Narratives](#)
- IV. [20 Bits of Investment Advice \(This is Not\)](#)
- V. [Infrastructure Trends / Crypto Companies](#)
- VI. [Bitcoin Trends](#)
- VII. [Ethereum Trends](#)
- VIII. [DeFi Trends](#)
- IX. [Web 3 Trends](#)
- X. [Stablecoin Trends](#)
- XI. [Policy Trends](#)
- XII. [Top 10 Re-Readings To Get You Fired Up for the Decade Ahead](#)

History

Two years ago, I posted “95 theses for crypto,” a look at what was to come for 2018.

It was in part a rage post sparked by the insanity of the Q4’17 bubble. It was also how I organized my thoughts at the time, and considered how to play the coming token crash we thought was inevitable for many of the projects that had raised gobs of money without much (if any) traction to support their lofty valuations.

The theses ended up being my most popular post of all time. So I decided to do it again last year. The only problem: I was beaten to the punch by Arjun Balaji (now an investor at crypto fund, Paradigm), who posted his own **very good** “Crypto Theses for 2019” the day before I was set to post my follow-up. His piece got all the social juice, and as a result, my follow-up had about 5% the engagement of the previous year’s. That made me sad, and I still hate Arjun for it. (Half kidding.)

So here we are at the end of 2019, and I’m posting my 2020 thoughts a couple of weeks early with the hope we’ll win this year’s pundit publishing cycle. This, I’m sure, will eventually be the crypto twitterati equivalent of “who will be the first to have a Christmas sale in October.” I predict that next year, someone will write a prediction piece that comes out around Thanksgiving. The year after that it will come out on Halloween, etc.)

That said, it’s **great** to get this out before the holidays, because it is a beast. When I started writing this past Sunday, my team thought I was nuts. “**120** theses for 2020? By Monday? Not possible. (Or smart.)”

We are indeed publishing this full report in full today, and plan to market six 20 section chunks for easier consumption over the last six business days before the holidays.

This is not just for our benefit, but for yours, as this year’s edition has a ton of third party links and must reads to comb through over the holidays. The goal is to give you a solid foundation in approaching the next year (and decade) of crypto.

Consider this Messari’s research foundation for 2020. We’ll build around these theses and our ongoing reports will help you build a solid crypto knowledge tree. This is too big for one sitting; it’s a mini-encyclopedia. Read it when you can, and when you want to learn something new.

I hope you enjoy reading it as much as I hated writing it.

-[TBI](#)

P.S. No one ever got fired for using Messari. If you like this post and our analysis generally, subscribe to our [PRO research](#), or contact us about [enterprise rates](#). You’ll get much more value out of our tools, then you’ll spend.

Disclaimer #1: Crypto Assets vs “Blockchain, Not Bitcoin.”

Let me save some of you in Corporate America^{^tm} some valuable time.

I believe in crypto, and our team does, too. A pre-condition to joining Messari is thoughtful conviction around crypto as a movement and paradigm shift, even if we’re often skeptical of many of the specific projects and announcements we sift through week to week.

This is **NOT** an objective analysis, but a collection of my / our strong convictions for the decade ahead. It’s based primarily on my nearly seven years studying this industry closely and working in it full time...with support from our excellent team of analysts. If you are looking for McKinsey-style neutrality, I’m sure there is a “blockchain for enterprise” presentation they can send you off-the-shelf for \$50,000-\$100,000.

I’m not a buyer of that sort of thing. But if you’re into crypto assets, this is for you.

Disclaimer #2: Asset First vs. Technology First

Keep in mind as you read this that one of my core mental models for crypto is that there are two distinct types of assets and communities.

On the one hand, there are asset-first, tech-enabled protocols like Bitcoin, stablecoins, and any other asset that aims to serve (and be valued) primarily as a monetary asset. The winners here usually require strong memes and a bit of collective, borderline religious, delusion on the part of their devotees. (Or a standing army in the case of central bank digital currencies.)

Then there are tech-first, asset-enabled protocols. Things like digital resource tokens (decentralized file storage and computation), “work” tokens (prediction market oracles), and governance tokens (voting rights on the management of a valuable underlying protocol).

In either case, you can’t separate the protocol from the asset.

If you are still in the asset-less enterprise blockchain mindset, perhaps you’ll still be interested in learning more about some of the potential hybrid public-private blockchain implementations that may anchor back to Ethereum, Polkadot, or Cosmos in the years ahead.

If you’re a crypto enthusiast or professional, or you’ve been tasked by your Fortune 1000 overlords to “get smart” on crypto assets, this report is definitely for you and can be your bible.

Without further adieu...

Top 10 People to Watch

If you're the average of your five best friends, then crypto is the average - and full spectrum - of these 10 people to watch in 2020. There will inevitably be a number of "who's who" lists that circulate around this time, but I've tried to capture unique "bell weather" personalities who fit part of a larger trend or narrative to keep tabs on in the decade ahead.

For reference, my [watch list](#) in 2019 was pretty good! CZ (Binance), Zooko (Zcash), and Rune (MakerDAO) return to this year's list given the tremendous pace at which their teams have continued to push the envelope in exchange innovations, stablecoin tech, and privacy.

Others from last year's list have dropped. Vitalik is still an obvious follow as the founder and spiritual center of Ethereum. But I believe Ethereum will thrive even when he inevitably takes a step back in the years ahead. Ditto Elizabeth Stark and the Lightning Labs team. Lightning is taking more time to develop than I'd originally thought, but I remain optimistic about its potential and there are now a number of capable teams building that infrastructure. Cosmos and Polkadot are the two top protocols that will vy for smart contract developers besides Ethereum. The former is now a top 20 crypto asset. The latter is due to launch in months. Others from last year's list had quieter years, although all remain influential within the broader ecosystem.

But enough about the old. Let's look at the new.



[Changpeng Zhao](#): Binance's founder & CEO, has become a legend in both western and eastern crypto circles, which may put him in a league of his own. His exchange captured the global lead in retail crypto trading less than two years after launching in mid-2017. The company's BNB token is now the seventh largest by market value, as well as one of the most useful and liquid. The Binance team has shipped new features at a relentless pace (IEO launchpad, margin trading, staking services, research arm, etc.), and CZ has built an army of missionaries, who are [willing to relocate at the drop of a hat](#) to complete the mission. He's the most interesting man in crypto right now because he's proven so adept at navigating the razor's edge of compliance and "damn the torpedoes" growth. Whether that edge remains sustainable, or fades in 2020+ depends on the company's successful regulatory engagement on a jurisdiction by jurisdiction basis. (More on Binance later.)



Jack Dorsey: The founder and CEO of Twitter and Square, sits squarely at the intersection of the crypto community and the mass retail markets. Crypto Twitter has taken the reigns from Reddit and BitcoinTalk before it, as the industry's dominant communication platform (at least in the West). At the same time, Jack has backed Lightning Labs and launched a crypto division of Square that's now funding bitcoin core development (among other things). Square's Cash App is now one of the primary retail onramps in the U.S. [accounting for \\$150 million of bitcoin purchases in Q3](#), or 8.6% of the total bitcoin mined during that time (and growing). If anyone is earnest about [bringing bitcoin to emerging markets](#) beyond an empty quote, it might be the enigmatic Jack: *"Africa will define the future (especially the bitcoin one!). Not sure where yet, but I'll be living here for 3-6 months mid-2020."* [Jack](#) was on my top 10 list before [this whopper of an announcement days ago](#) that Twitter would incubate "a small team of five open source architects, engineers, and designers to develop an open and decentralized standard for social media." The goal is for Twitter to ultimately be a client of the new "[Blue Sky](#)" standard. Wow.



Brian Klein: I've known Brian for about as long as I've been in the industry, though I'm rather happy we have never worked together. He's is a partner at Baker Marquart, where he was named one of the top 5 financial technology attorneys in the U.S. this year by industry publication Law360. A big part of that had to do with the who's who of clients he's represented over the years: Kraken's Jesse Powell, ShapeShift's Erik Voorhees, Charlie Shrem in his [dispute with the Winklevoss twins](#); the Breitmans as they warded off [multiple class action suits at Tezos](#); and most recently Block.One for whom Klein delivered what looks to have been a tremendous outcome, a mere [\\$24 million civil penalty](#) for the company's \$4 billion unregistered securities offering of EOS in 2017. He's now taken up the [controversial defense of Virgil Griffith](#), the Ethereum Foundation researcher the FBI has accused of aiding North Korea in circumventing U.S. sanctions. Everyone scoffs at the ruthless lawyer archetype...until they need one. Crypto will need Brian and others like him in their corner in the decade to come.



[Meltem DeMirors](#): I'm partial having worked with Meltem for three years at Digital Currency Group, and because she is a current investor in Messari. Regardless, you'd be hard-pressed to convince me there is anyone as well-connected / respected / productive across multiple communities and products as Meltem. As Chief Strategy Officer at \$500 millionn crypto investment manager CoinShares, she's everywhere. Podcast. ([What Grinds My Gears](#)) Weekly newsletter. ([Meltem's Musings](#)) Mary Meeker-esque state of the industry. ([CoinShares Crypto Trends](#)) But the 2019 highlight was her [Congressional testimony](#) this summer, where she got "shitcoin" added to the Congressional record.



[Congressman Brad Sherman](#): Speaking of Congress, Rep Sherman is crypto's most [formidable enemy](#) in Congress. The 20 year congressman ascended to Chair the House Financial Services Subcommittee that oversees the SEC and its self-regulatory bodies like FINRA in December. He's a clever and outspoken critic of crypto in Congress, in the "let's actually shut this thing down" kind of way. What makes him dangerous (and I've pointed this out for months), is that he understands the root threat of bitcoin and the "[Crypto Patriot](#)": creating a new seizure-resistant digital reserve asset. And he's shown a willingness to use the most damaging narratives ("crypto is for fraud, money laundering, and tax evasion") to rally colleagues to his cause. Coin Center has its hands full with him in 2020.



[Morgan Beller](#): I met Morgan for the first time in early 2018 as the Facebook team was first (quietly) coming together. She keeps a fairly low public profile ([to the extent that is possible](#) in her position), but her clout internally at Facebook/Libra is well known in the industry. She's listed as one of co-creators of Libra, alongside David Marcus (former PayPal CEO) and Kevin Weil (former head of product at Instagram and Twitter), and is now head of strategy for Calibra, Facebook's associated Libra wallet. If she were to leave Facebook or the Libra project at any time in the medium-term, it would be a canary in the coal mine: something is seriously wrong. Though I don't know many within the industry who are betting against Morgan and her team.



Rune Christensen: Rune is a less public facing personality compared to the others on the list, but his influence is obvious. As founder of MakerDAO, he wields influence over the entire DeFi landscape and the assemblage of businesses and protocols that depend on Maker's Dai stablecoin. A recent [attack vector](#) on Maker highlighted the existential threat for businesses leveraging Dai. A loss of the \$300+ million of collateral locked in the system or an unexpected inflation bug in a key Maker contract would likely lead to contract "bankruptcies" at protocols that leverage Dai, which would be a nuclear setback for the Open Finance movement. (More here: [Ensuring Ethereum isn't on the brink of a second bailout](#)). Rune is no mere figurehead, either. As the head of the Maker Foundation, which controls over 30% of MKR tokens, he has significant medium-term influence over the network, and has navigated several governance [challenges already](#). MakerDAO should transition to a decentralized autonomous organization at scale, and its Rune who'll lead them there. (More on [how Maker works](#).)



Zooko: The Zcash founder has been [pushing the privacy envelope for decades](#), and the entire crypto community (crypto meaning both cryptography and cryptocurrency) has benefited from his team's efforts. Many of the community's recent breakthroughs with "zk-snarks" are being incorporated into multiple open-source protocols outside of Zcash (e.g. Ethereum, Tezos), and Zooko's Electric Coin Company is at the bleeding edge of the regulatory battles that await truly anonymous digital cash. Some folks who know me will say Zooko is on Messari's list because I am an investor in ZEC ([woof](#)), but the reality is I'm invested because I believe in Zooko, not the other way around. He's an important leader for the future of the industry, and the Zcash community's continued near- and medium-term success hinges on his ability to navigate the network's upcoming 2020 halving and fork. This is one of four teams in crypto who I think have built a community of missionaries vs. mercenaries, largely off the back of a revered creator. The others are Bitcoin, Ethereum, and Binance. You can't build such a strong community with a token that's dropped to all time lows without strong leadership. Zooko has. (More on Zcash later.)



Justin Sun: You truly can fake it til you make it in crypto, and there is no better marketer in the industry than Tron founder Justin Sun. Despite allegations of plagiarism early on - in both the project's initial [white paper](#) and [code base](#) - Sun has memed and brute-force marketed his way into a global fanbase, as well as successful acquisitions of Bittorrent, crypto exchange Poloniex, and crypto content platform SteemIt. All in just eighteen months. That's to say nothing of his Warren Buffett lunch stunt, mysterious [last minute cancellation](#), and other associated (manufactured?) [controversies](#) this past year. Sun's inclusion is perfect evidence that I really have no idea how crypto or Asia work. (Note: You'll note this report is light on Asia coverage as I am not as familiar as I should be with that half of the market.) Tron remains a top 15 crypto asset, and one of the most liquid by volume on many of the major global exchanges. Sun has been so effective I'm starting to think I'm the crazy one for being skeptical. It's disorienting.



Peter McCormack: Crypto journalism had it's best year ever in 2019. *CoinDesk's* [Leigh Cuen](#) is the industry's best individual journo right now, though [The Block](#) has challenged (and probably surpassed) *CoinDesk* as an editorial brand overall. (*Decrypt's* not bad either.) But Bitcoin podcaster Peter McCormack is the one who really embodies everything amazing about the defiant crypto citizen journalist / pundit community in 2019. And I mean that genuinely, not in a left-handed compliment sort of way. The leveling up of crypto data, research, and information businesses has been one of the best parts of bear market build out. But it's the explosion of podcasts, led by McCormack (and of course, [Pomp](#)), that has really stood out in creating a new must-listen educational medium for new entrants to the crypto space.

Top 10 Narratives

1. **“Hyperbitcoinization vs. Digital Gold”** While you’ll see a great deal of chatter about the coming decade’s [hyperbitcoinization](#) if you read the [Bitcoin Standard](#) (which I recommend) and follow the hard core libertarian crypto crowd on twitter, it’s a mistake for everyone to keep hammering away at this currency narrative. It’s threatening and unnecessarily and prematurely hostile to the powers that be. It’s a harder narrative to grok for newcomers, and everyone that converts to crypto ends up hoarding bitcoin like digital gold, anyway. Practically speaking, we should go after the \$7 trillion gold market first, see how that goes, then move up the value chain to the next milestone if we get there. Bitcoin as everyday cash will also *always* suck in a world with stablecoins because of the tax consequences of spending, and the public audit trail those transactions leave.

2. **“Long Bitcoin, Short the Bankers”** In a world where every transaction has an associated cost basis and tax event, the real killer app for the industry is in collateralized lending. This is especially true in the U.S. with its crypto hostile tax regime. Rather than spend crypto and deal with accounting headaches, it’s becoming feasible to lend bitcoin in return for (tax free!) dollars out, at reasonably low interest rates! Of course, there is always liquidation risk in these products if your collateral declines in value, but borrowing against 10-20% of your holdings, for instance, is plenty of cushion for most people, especially if they’d be otherwise looking at 20-30 points of incremental capital gains tax liabilities in a sale. It’s nonsensical to take the tax hit on a big purchase (e.g. a down payment on a new house) if you can avoid selling. I’m waiting for one of the crypto tax software companies to collaborate with the lenders and create a calculator that runs through this logic for their customers. Borrow money from your own bank.

3. **“Stack Sats & Earn Crypto.”** I’m disappointed in what has become of Earn.com and Streamium. (You’d have to be OLD to remember [Streamium](#).) The potential to monetize your time via crypto is significant (an Airbnb or Uber for “spare time” is capital efficient), but it hasn’t hit yet. The potential for streaming metered payments is also there (telemedicine, international consulting, and of course, porn), but that hasn’t clicked either for some reason. I’m shocked we haven’t seen a BIG specialized payroll company that offers bitcoin payouts as a percentage of your paycheck (though [Coinbase may be working on it](#)). In the meantime, we put together an easy overview at Messari of [how to earn “free bitcoin”](#). Perhaps the easiest method today is Lolli, a browser extension that sends users bitcoin rewards for online shopping. Honey just sold to PayPal for [\\$4 billion](#). Lolli could be on a similar trajectory in the next bitcoin bull cycle.

4 “Unbank the Banked.” I love this quip. (I believe it originated with the [OmiseGo team in mid-2017](#).) It’s SPOT ON. There’s building tech for the disenfranchised, who often need financial services, but don’t make tremendously compelling early customers because of their low CLV (customer lifetime value). Then there’s building tech for those who are on the inside already, but feel like they may be on the way out: the misfits, the tinkerers, and the dissidents. We desperately need more success stories from Latin America, and the Middle East, and other emerging or unstable markets, particularly in regions where the rule of law is weaker and there are security risks associated with having a healthy bank account. Bitcoin took off in the U.S. in large part because Wences Casares, Silicon Valley’s “patient zero” was a successful entrepreneur from Argentina with a superhero backstory and a stunt that caught the attention of *the rich*. Bitcoin caught fire in the U.S. because he passed \$250k of bitcoin around a table of Silicon Valley power brokers at an exclusive 2013 dinner, not because someone at the party bought LSD on Silk Road (ok, ok, maybe it was both.)

5 “Missionaries vs. Mercenaries” The only crypto communities that will survive in the long-term will have strong memes. On the flipside, most attempts to bribe developers and users with airdrops and developer grants will fail (many already are), and most attempts to recruit insiders to a cause with pre-sale discounts and the (diminishing allure) of token flips will bring dysfunction and gridlock to projects that otherwise may have had a chance. We’re starting to see some teams come to terms with this reality. Stellar just burned [50% of its token supply](#) because they quite literally can’t give it away. The EOS “[cartel](#)” has likely led to [irreparable damage](#) in that protocol’s reputation in developer circles (why build on infrastructure that will get hijacked by ruthless investors). And I’m predicting another bloodbath for privately funded token networks that come to market in 2020. We’re also intentionally avoiding coverage of many new competitive Layer 1 blockchains in these theses for this same reason: the vast majority are simply not interesting from a narrative standpoint.

6. **“Bitcoin is a Platypus”** Blockchain Capital’s Spencer Bogart had one of the all-time classic analogies for Bitcoin in a 2017 post: [the platypus](#). He writes about the platypus’s history:

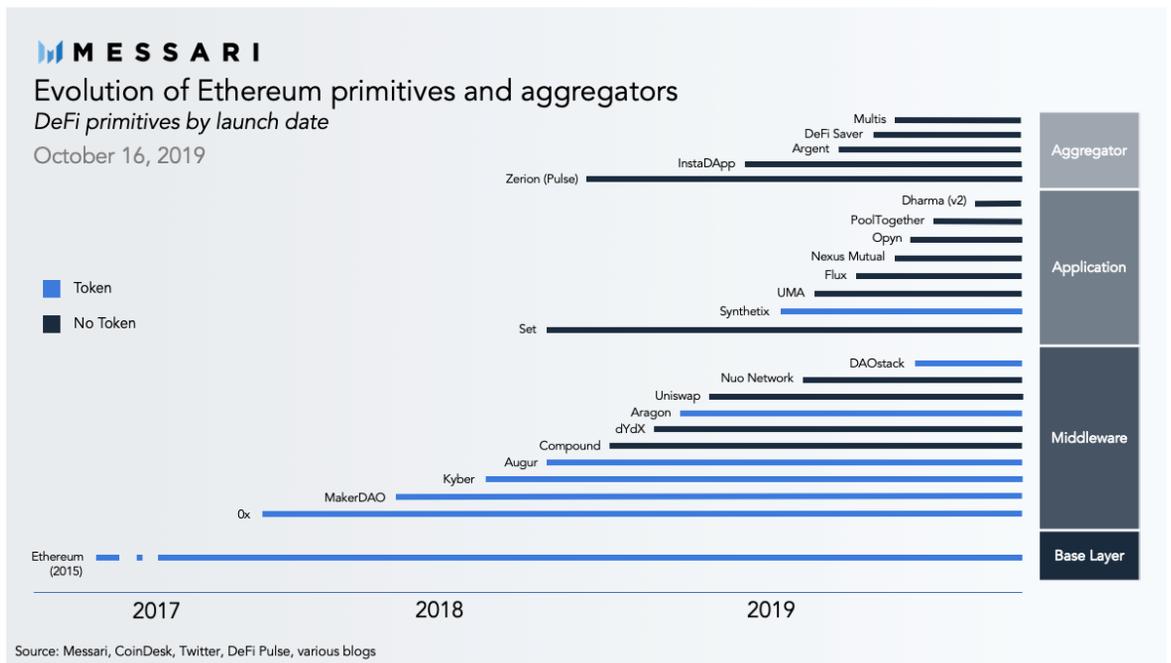
“The platypus is perhaps the most bizarre creature on the planet. It’s a venomous, egg-laying, duck-billed, beaver-tailed, otter-footed mammal. Those things simply aren’t supposed to go together. In fact, when leading scientists first read accounts of the platypus, they dismissed it as a joke—and for good reason: the platypus is a seemingly impossible animal that combines features from three different animal classes and four different animal orders....Even once the platypus was broadly accepted as a real and legitimate animal, classification provoked arguments: What type of animal is it? As it turns out, the platypus isn’t good at being a duck, it’s not good at being an otter, nor is it good at being a beaver or a reptile. The platypus is, however, great at being a platypus! In the end, the platypus was so distinct that scientists had to create a new animal category to accommodate its unique features. The platypus is a category creator.”

Bitcoin can be used for payments, has provable scarcity like a commodity, can split like a stock, and serves as a foundational protocol for other types of value transfer. We’d do well to capitalize on the limited time bitcoin has left being considered a punch line. When someone in power says “This isn’t money, it sucks as money. No one accepts it!” You should say, “You’re right!” When they say, “This isn’t digital gold, it sucks as a store of value.” You should say, “You’re right!”

Please, please, please, let us hide in plain sight for one more bull run that gets us too big to fail.

7. **“The Revolution Needs Rules”** I wrote last year that I thought Gemini’s [controversial campaign](#) was brilliant. A year older, wiser, and more disgruntled has made me an even bigger fan of the messaging, though perhaps my punch line is different than the Winklevoss twins’. I believe *they* were trying to convey that Gemini is a regulated exchange that follows the law and sets the standard for what compliance should look like in crypto investment products. Good for them, but I take a less supplicant stance. When I think “The Revolution Needs Rules” I don’t think of placating U.S. regulators so much as I do of training a rag-tag militia. If we want to be better than the incumbents, then token teams: start disclosing insider sales; exchanges, clean up your wash trades; wallets, learn how to integrate with tax software systems and help your customers minimize their liabilities and pay only to Caesar that which is actually Caesar’s. The rules to the revolution shouldn’t all be defensive. Let’s play some fucking offense in the 2020s.

8. "ETH is money." Back in May [I spoke at Ethereum](#) and told the room full of "decentralized world computer" fanatics it was stupid for the Ethereum community to build non-financial applications. Being the reserve currency for DeFi / Open Finance was plenty good enough, and things like low value collectibles, gaming, and distributed applications were a complete distraction whose use cases they should forfeit to other blockchains. This was a good take, and a lot of other ETH fans are starting to fly that flag. Ethereum could power most major stablecoins, synthetic securities, and the vast majority of the programmatic crypto lending and derivatives market. C'mon, fam, FOCUS. Rebuilding *literally* the entire financial system would be a big enough win. Push the kitties to a separate blockchain.



9. "Dissident Tech" - Web 3 got real fast. I thought it would take years to get excited about "decentralized internet" applications, but perhaps it's sooner than we think, especially if it's getting the satirical treatment on [Silicon Valley](#). The continued exploitation of user data from tech behemoths (looking at you, Zuck) is making the concept of dissident tech — coined by [Maya Zehavi](#) — not only relevant, but cool. And new generations of users tend to gravitate towards "[cool tech](#)". The demand for privacy and freedom of expression sparked a proliferation of crypto solutions over the past year-plus, from decentralized hardware networks like [Helium](#) and [Orchid](#) to privacy-focused browsers like [Brave](#), which provide a glimpse of what's to come with the web3 data stack. I'm not too bullish on the projects sporting token-first models, but upstarts that apply token models to applications that *already work* are more interesting. What's also intriguing is the rate at which investors are defining their [investment theses](#) around dissident tech, emphasized by funds such as Cyberpunk Holdings and the mysterious [Unknown Fund](#). Demand for privacy and censor-resistant solutions will require a shift in user behavior, but "[the undercurrents are growing](#)" in the current environment. 12

10. **“ok, boomer.” but for crypto.** Crypto has some pretty good memes for insiders. But I’m not sure how effective our narratives will be during the political battles ahead. Are any of the nine narratives above capable of *winning elections*? Every time I look at that bald, conniving ape Sherman, I see someone who will lead and *win* the narrative battle against crypto with the most powerful people we cannot afford to lose. It strikes me there’s a generational divide we must recognize in that battle, a frustration we can capture and turn back against leaders like Sherman. An “ok boomer” that provides an effective counter to the damaging narrative that crypto is for “frauds, terrorists, and criminals.” I don’t know what it is, but I like these [500+ efforts to get it right](#). My favorite: “The rich got bailouts. The people got bitcoin.”

20 Bits of Investment Advice (This is Not)

1. My Top 20 coin hot takes (UPDATED): This is a refresh of my list from last year. Many of these haven't changed, but I've bolded the ones that have. Rankings based on OnChainFX.com. If you're not full-time in crypto, don't worry if you don't get the jokes, and skip to #2.

- BTC: Digital Gold
- ETH: **DeFi Reserve** (vs. ICO Reserve)
- XRP: Too-Big-To-Jail Coin
- USDT: **Surprise! They're more reserved than most Tier 1 banks.** (vs. Surprise! They're solvent.)
- BCH: Bitmain casino chips
- LTC: **BTC betanet 4->** (vs. Now useless)
- EOS: **Actually no, it is in fact broken and run by a cartel.** (vs. Wait, it's legit?)
- BSV: Faketoshi Coin
- XLM: **Burn the coins cuz no one wants them** (vs. Cool. Enigmatic.)
- BNB: exciting unregistered security
- LINK: **XRPArmy welcome**
- ADA: YOU STILL DON'T KNOW WHAT IT IS?
- XTZ: **Wow! Staking games will never backfire!**
- ALGO: **Top 20 if no one redeems, amirite?**
- TRON: **fake-it-til-you-make-it coin**
- XMR: Fluffy Pony Watch Fund
- LEO: **Quasi-security backing a quasi-Liberty Reserve**
- ATOM: **Most interesting ETH "complement"**
- NEO: "Chinese ETH"
- HT: Quasi-security that might have CCP blessing

Other quick notes: XRP has tremendous and surprising staying power. I didn't understand it when I realized [it isn't required to use Ripple's software](#). I really don't understand it in a future that includes institutional stablecoins and central bank digital currencies...The bitcoin forks are write-offs at this point, even if the IRS ends up walloping people during audit open season these next five years...A lot of the dogshit [washed away this year](#), or is on its way to predictable obsolescence, but Dogecoin will continue to rock because legends never die....Means of exchange tokens (why not use a more liquid crypto or stablecoin) and governance tokens (what valuable resource are you actually governing) are garbage and now trade as such.

2. Bitcoin will lead, or alts will bleed An interesting thing about crypto is that bitcoin has not actually led a supercycle rally since 2013. There's evidence to suggest that, back then, family office and accredited investor interest in the Bitcoin Investment Trust led the rally. In 2017, it was ETH and ICOs that led the rally. I remember being at the Enterprise Ethereum Alliance's inaugural event, and it was a who's who of "blockchain, not bitcoin" folks from the major corporates. I thought, "oh fuck, maybe I should buy some ETH just in case," then all hell broke loose with people raising \$30 million in 30 seconds with ETH. You made money in ETH / ICOs, then you "sold" into Bitcoin on Poloniex. That was the formula. It wasn't until later in the year that bitcoin became its own thing again following the resolution of the SegWit2x stalemate.

Why does this history matter? Because bitcoin *itself* hasn't sparked a proper rally in six years, and the much hyped "halving" narrative is bullshit because the magnitude of the decline in new issuance as a percentage of market cap is tiny. Instead, the 2013 and 2017 rallies were driven by new *types* of buyers. It just so happens bitcoin is the most likely asset to attract the next major new type of buyer again today: institutions. There won't necessarily be a sudden surge higher. Instead, it will be more like a snowball: one off announcements of adoption begin to increase in frequency before the price begins to tick slowly higher. I think bitcoin hits a new high before we go macro "risk off" again.

3. The "dumpening" will continue. I said during my inaugural 95 theses post that we'd see most tokens grind down 99%+ from their all time highs, mostly due to the incredible amount of selling pressure that would hit most token markets once teams and inside investors began liquidating positions. By this metric, XRP has a could-be-market-dumped liquid treasury of \$2-3 billion, XLM has a could-be-market-dumped liquid treasury of \$800 million, and Chainlink has a could-be-market-dumped liquid treasury of \$600 million. Those are some of the publicly traded assets. For token projects that raised gobs of money at nosebleed valuations in 2017, things could get very ugly, very quickly once they start trading. It's not even guaranteed Telegram, Filecoin, Dfinity, or Polkadot come to market in the new year, but if they do, I'd be surprised if they traded at anything close to their last priced rounds.

4 Yes, crypto is about the post-USD world. More than 95% of the value in crypto - outside of exchange tokens (which I'd argue are quasi-securities) is due to the *monetary premiums* of the top crypto-currencies. We've reached the point where the macro global currency narrative will make or break bitcoin in the next cycle. If huge piles of [negative yielding debt continue to build](#); if central banks continue to [flood their markets with cheap capital](#); if mistrust in most global governments continues to rise, then crypto will be a relatively strong asset to hold. If trade wars accelerate; if governments crack down on the regulated edges of the crypto economy; or if a major recession hits, it's going to be "risk off" and we'll be in for a long winter.

Modern Monetary Theory is the most [damaging economic voodoo bullshit](#) that has gone mainstream recently. “Rising debt isn’t a big deal because the dollar is a reserve” only makes sense if you ignore the reality that China is expanding its RMB reserve influence throughout Asia at an accelerating clip, and that [the central banks stockpiling gold](#) at record rates are also the same ones that happen to hate the U.S.: Russia, Turkey, and China. I’m surprised we didn’t see a top 50 central bank *announce* they were purchasing crypto as a speculative complement to their gold purchases. I’d be even more surprised if this weren’t happening in secret by now.

5. The gold-digital gold basket. If you’re a gold bug, I don’t know why you wouldn’t take 2% of your gold portfolio and buy bitcoin with it. Unless you were legally restricted from doing so for some reason. If you view these assets as perfect “store of value” complements, and you look at the demographics of who’s buying bitcoin (young people), you’d be a [fool](#) to not market cap weight your gold-digital gold basket. When I was in college, I told my grandfather that between freshman year and senior year, I watched the Mac user base go from 3% to 6% to 10% to 15% of my classmates over four years. Folks, this man doesn’t code on the weekends, but he did buy Apple stock between rounds of golf, then a new BMW a couple of years later when he sold some of the stock. That’s because sometimes the easiest investments decisions are the simplest ones, and I don’t know why any asset manager would stand in front of the freight train that is the generational rotation from boomer gold bugs to [millennial digital gold bugs](#).

6. Refresher on the crypto asset barbell. There’s nothing new under the sun. If bitcoin has converged on becoming a new form of digital gold, that still leaves plenty of other interesting and valuable monetary and non-monetary assets within crypto. The biggest bucket by far will be crypto-currencies (including stablecoins), followed by smart securities (which will take longer to develop), then a narrow band of digital tokens that span use cases like governance rights, digital resource allocation, work / affinity rewards, etc. BTC, ETH, ZEC, and XMR (the ‘ole [“consensus contrarian”](#) portfolio) are still the main cryptocurrencies, while exchange tokens are proving to be the first quasi-security tokens with Binance, Bitfinex, and Huobi tokens catapulting to the top 20 in the past year. (We should have known that the industry would dogfood its own companies as the first tokenized securities!) I cover this in pretty epic detail with Placeholder’s Chris Burniske in one of my favorite [interviews](#) of the year on the Messari podcast.

7. The insanity of inflationary staking rewards. Non-money and non-security tokens need some type of artificial velocity sink, otherwise their theoretical value should be capped at some discounted value of the future maximum network utility, divided by velocity. (I know that's a mouthful, bear with me.) Low velocity comes from the need to hold an asset in reserve or earn fees generated in the network (i.e. gas to run applications within the Ethereum virtual machine). Another way to create a velocity sink, though, is via inflationary staking rewards. Essentially taking money from one pocket and putting it in the other. Brilliant!

I don't want to mince words here: inflationary staking rewards are without qualification the dumbest thing this industry has deluded itself into believing since white paper investing caught fire in mid-2017. The logical end game is that custodial staking services centralize holdings, inflation rewards get split pro rata to 99% of the network that stakes, then those lucky recipients pay their staking services a fee AND get a cash tax liability for what is really more like a stock dividend. Then the custodial staking services report it all to the tax authorities. Madness.

8. I'm actually a medium-term bull on staking. Oh the irony! Solid governance infrastructure really needs to exist if proof-of-stake is going to work. I'd argue staking probably must be run (unfortunately) by a fluid oligopoly of providers for a while much like proof-of-work mining is run today. Counterintuitively, this means staking services probably *should* get bootstrapped around the inanity of "inflation rewards" vs. "network fees" because no one is using any of these networks today, but at least you can game participation in the games of stakes. Staking rewards (net of tax) should be value destructive, but we could see some major pops for a while as some teams "optimize for the monetary premium" - aka design token pump schemes.

We're seeing this already with Tezos as staking exchanges scramble to acquire XTZ on behalf of their customers. Some three quarters of Tezos is already staked, yet Coinbase, Kraken, and Binance need to buy more for their bonds if they want more users to stake. Not only that, but you can think of all this as practice marketing for the real staking bubble leading up to ETH staking early next year. All the staking services will be falling over each other marketing that.

9. Crypto-securities will continue to disappoint. As I predicted last year, nothing in the securities market has been very interesting yet. At least none of the tokenized real estate / private company shares / corporate bond projects have come to market. That's because their liquidity pools are elsewhere, and markets follow liquidity, not the other way around. What *has* been interesting is the proliferation of tokenized *quasi-securities*.

I'm bullish on exchange tokens with token burn models. I like synthetic DeFi protocols that mirror real world equities (buy the S&P as an Indian investor). I really like the design space that's opening up around DAOs, which is probably the logical end state for most "utility" network tokens that power protocols of any utility in the future. (Perhaps this is the path to value of the 0x token, e.g.) The trick is going to be winning the market without running afoul of SEC guidance - at least in the U.S. The great irony is that fear of the SEC may be preventing a number of teams from upgrading features of their tokens that would give the assets, ya know, *actual compelling fundamental value*.

Adding smart contract functionality to markets such as real estate, energy, insurance, and even human capital will happen eventually. Though issuing a token under Reg A+ as a security will have to be one of those areas that dies in a fire sooner rather than later in the 2020s. I can't wrap my head around how that makes any sense at scale. Crypto moves too fast to wait on the SEC to come up last year's learning curve.

10. Stablecoins will soon eclipse bitcoin in size. The stablecoin wars are heating up, and it's the best thing for the long-term viability of crypto. We have a whole top 10 section dedicated to them this year, but suffice it to say: interoperable global stablecoins could become bigger than bitcoin in short order if some of the major central bank digital currency projects take root. I'm not sure whether Facebook (via Libra) or Binance (via Venus) is well-positioned for success if more governments get serious about their own stablecoins, but Tether might be. More on all of these later. *(Note: Some may dispute that CBDCs are actually cryptocurrencies. Not arguing semantics, but we'll cover them at Messari.)*

11. I've come around on crypto funds. I can't believe I'm writing this, but I'm a net buyer of crypto fund managers generally. I still think most of them will be [alpha negative](#), but there's an accessibility element I underestimated when I first scoffed at 2 & 20 funds in 2017. That is, the unique tax, tech, and regulatory issues presented by crypto leads to a situation where it doesn't make economic sense to spin up infrastructure in-house as an asset manager unless you're *really* going all in. Institutional investors who want exposure will (and probably should) take LP interests in blue chip managers and *maybe* buy bitcoin directly. That's about it if you're managing a large portfolio. I don't expect this approach to frequently lead to alpha vs. the bitcoin benchmark, but it might lead to absolute outperformance as an LP if it's part of a broader investment portfolio. Watching pensions and [endowments](#) finally enter the fray has been wild. [The virus is spreading.](#)

12. I'm bullish on funds despite major coming markdowns. I'm a buyer of the crypto funds as a class despite (because?) so many of the OG funds have been sucking wind these past couple of years. Out of the crypto native funds, it seems Paradigm, Placeholder, and Polychain are in a class of their own reputationally. That said, there is some real toxic waste on some of these books that I've heard are *aggressively* marked. (The shadowy world of crypto valuation firms is probably fodder for one of our 2020 Pro research posts.) Fortunately, more of the top tier funds seem to have structured longer lock-ups and more credible LPs than may have been expected two years ago, so runaway liquidations seem unlikely. I'd be surprised if there were a high-profile (in terms of reputation, not AUM) fund blow-up next year, even if (when?) the "ETH killers" come to market and fizzle entirely. The worst has passed.

13. How about passive products? Everyone got a bit ahead of themselves in late 2017 regarding the tokenization of everything. This was back when bitcoin dominance fell to historic lows of 36%. (36%!!!) Back then I predicted *"most crypto funds (net of fees) would underperform vs. BTC and ETH as benchmarks...sooner rather than later, institutions will wise up to the reality they shouldn't be paying carry on funds denominated in BTC and ETH. When that happens, you'll see a massive influx of capital to passive index funds."* This was arguably right, but I overestimated the probability of crypto ETFs getting approved within two years, which is what continues to make crypto funds so attractive. As it turns out, the [regulators only want to approve](#) crypto products that depress the price, not add fuel to the fire.

14. Long Grayscale, short crypto. You'd expect passive crypto products to get ruthlessly competitive on fees, similar to the exchange market. But it's not the case. Digital Currency Group's Grayscale Investments sits in a unique regulatory position as an asset manager. They essentially have a strange temporarily monopoly on the U.S. crypto ETF market, where their ["sidedoor ETFs"](#) allow them to add AUM to the trust that essentially can never exit. I've written about the Grayscale trade, and how their products work in the past. But in brief, the odd structure allows institutional investors to create new shares in the trust, flip them after a year at a huge public market premium, then recycle the gains post-tax at a higher cost basis. In return for the clever structure, Grayscale gets all of the benefits of running an ETF business with [an insane regulatory moat](#) to defend the 2% management fee on their 4-5 public products for the foreseeable future.

And the plot thickens! DCG is also one of the best positioned U.S. crypto unicorns to access the public markets via an IPO, as their combined businesses throw off close to ~\$100 million in high margin revenue, and they have a vast digital currency and venture portfolio. (We also did a [sum-of-the-parts valuation](#) on DCG last quarter.) But the irony is that DCG likely needs to go public before a crypto ETF gets approved, which would likely lead to increased competition (and a fee slashing) for Grayscale’s products. Could a quasi-index fund go public if an ETF can’t?

Digital Currency Group Holding	Estimated Annual Revenue (\$ million)	Low End Multiple		High End Multiple	
		Multiple	Implied Valuation (\$ million)	Multiple	Implied Valuation (\$ million)
Grayscale	50.20	10.0x	501.77	15.0x	752.65
Genesis (Lending)	22.60	7.5x	169.50	10.0x	226.00
Genesis (Trading)	60.00	6.0x	360.00	9.0x	540.00
CoinDesk	14.40	3.0x	43.13	5.0x	71.88
Investments	--	--	506.00	--	506.00
Sum	147.2	--	1,580.39	--	2,096.52

Data compiled 08/21/2019.

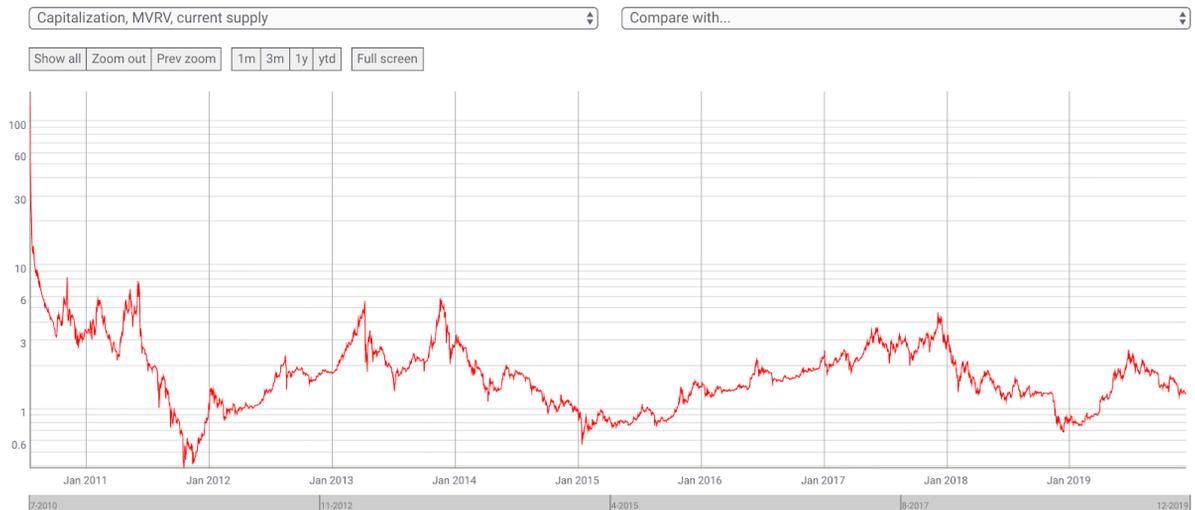
Source: Public disclosures, websites, and Messari analysis.

See report for full description of comparables and multiple ranges.

15. The Alchemy of Crypto. Meltem had a great post on the history of alchemy that explained crypto economics’ [current status as pseudoscience](#). *“Practitioners of alchemy had good intentions, and wanted to use knowledge as a tool to help humanity for the better...these pursuits played [a role] in the development of branches of philosophy, chemistry, biology, physics, geology, and more. What began as a pseudo-science, with its roots in mysticism, began to evolve into proto-science with practical applications and very real implications for the future of humanity.”*

This strikes me as sensible, and the best way to value crypto assets today may still be on a relative value basis or in baskets. Trade BTC/LTC , ETH/ETH Killers, XMR/ZEC when the relative values get too far out of whack vs. historical averages. Otherwise, when it comes to emerging fundamental metrics, there are three I like best:

1) Market Value / Realized Value ratio for proof-of-work coins. This measures the accumulated value of each newly mined coin based on the market price at the time of its original issuance, and then compares it to current market capitalization. The two times bitcoin's MVRV dropped below one historically were the cyclical bottoms for bitcoin in Jan 2015 and Nov 2018. LTC's MVRV has fallen by 50% since this summer, and ZEC is at just 0.32. This only works if you believe in the monetary fundamentals of a given asset, as you know it's human psychology for people to hold underwater positions in the hopes they will rebound. Here's the [chart to watch](#) to track MVRV from our friends at Coinmetrics.



2) Real 10 Liquidity Coverage ratio. Which I coined just now while writing this sentence. We use our "real" volumes from exchanges we believe omit wash trades from their public APIs, so we have a proxy for actual buy-side support. If you take that and divide it by the daily dollar-value of newly sold / mined crypto from a given network you could get a "Liquidity Coverage Ratio." This would give you a sense of whether there is enough exchange liquidity on a daily basis to handle new liquidations without completely tanking the price. Low Liquidity Coverage ratios typically lead to slow and steady grinds lower in individual markets. It's why I continue to hate XRP and love ZEC as a 2020 personal investment thesis. (NOT TRADING ADVICE, IDIOTS.)

3) [Network fees as a % of new issuance](#). As I mentioned in my blurb earlier on staking, I'm all in on network transaction fees as a driver of fundamental value for network tokens, and I hate inflationary rewards. Network fees mean people are actually using your platform, and that's a good thing! Even better if your fees ultimately overtake what you'd expect to earn from new block rewards. This will emerge over many years, not necessarily next year, but keep an eye on it as it will be a proxy for legitimate adoption.

16. The macro footrace. It might seem dramatic, but the next 12-24 months may decide whether crypto emerges as a serious asset class in the 2020s, or fades to a long, nuclear winter. It's a coin-flip right now. We probably need a 20x rally from here (which would put us on par with the dotcom bubble), before crypto feels too "big to fail" or difficult to regulate out of existence. This is a big number (about \$4 trillion), but it's not that big when you consider it might only take 10% of that market cap (\$400 billion) to move the market price that high. With institutions (and maybe central banks?) serving as the last money in, and trading, custody, and compliance solutions coming online, those sort of inflows are at least feasible. We're 20 years and a good deal of globalization beyond the dotcom bubble.

17. ICOs are dead, but ecosystem funds are alive. There doesn't seem to be much of a catalyst for growth in the 2020 ICO market, and private token liquidations will likely serve as the official death knell for ICOs for a while. The time to make money in ICOs was in 2015 and 2016 when they were contrarian. Going forward it will be interesting to watch how some of these foundations manage their enormous coffers. Ripple, Tron, Block.One, and Tezos have serious capital to deploy (more than almost all of the crypto funds) and have not been shy about their investing pace in complementary crypto and legacy businesses. The jury is still out on whether most of this capital will be squandered. Block.One [paying \\$30 million](#) for the voice.com domain certainly seems like something you'd do if you could set money on fire with no repercussions. Ripple and Tron seem to be more strategic so far. TBD on how disciplined the Tezos Foundation proves to be. Smart capital allocation is critical for the teams with mercenary vs. missionary communities: they'll need to be razor sharp at how they deploy capital to support their networks.

18. DAOs for LP Money. Investment stakes in decentralized autonomous organizations are the original security tokens, both as an experiment and [according to the SEC](#). We are just starting to see the emergence of DAO infrastructure, and it comes at a time when the SEC has conceded they [must do more to open private markets to retail investors](#) and re-think accredited investor statutes. For a full breakdown on my thinking of DAOs, you can read my [meatier post from October](#) as a reference guide. The gist is that the killer app of DAOs may not be in disrupting the VC managers directly, but rather liquifying the *limited partner* pool of capital that backs those managers. This could be a boon for specialists and legitimate value add investors with large networks, and it may be the most exciting segment of crypto in 2020+. If Messari folded up shop tomorrow (don't worry we won't, but you should still pay us money and go PRO), I'd work on a project in the DAO space.

19. Infrastructure M&A A couple of bitcoin miners and the major global exchanges make almost all of the money in crypto. To the extent other businesses also make money, it's selling tools and services to the exchanges. The result will be a continued (accelerating?) acquisition pace by top exchanges as they build out their suites of services. I predict BitMEX, Coinbase, Binance, Kraken, and Huobi will make nearly \$1 billion of acquisitions within the next 24 months. The number of deals will increase in a bear market. The size of deals will increase in a bull market. Either way, they're going to go shopping, particularly in the areas of compliance, trade execution, and custody/staking tools. Here are some of the largest deals to date, [courtesy of TokenData](#).

ACQUIRER	TARGET	YEAR	SIZE	SIGNIFICANCE
Circle	Poloniex	2018	\$400M	Largest acquisition to date, but Poloniex has since spun-out
BK Global Consortium	Bithumb	2018	\$350M	Buy-out of Korean exchange by a financial buyer consortium
Lightyear	Chain	2018	\$350M	Development team (Lightyear) of a public blockchain (Stellar) engaging in M&A
TRON	Bittorrent	2018	\$125M	Largest acquisition to date by an ICO-funded team (TRON)
Coinbase	EARN	2018	\$100M	Talent & technology
Coinbase	Venovate/Keystone	2018	\$10-25M	Regulatory driven M&A
Galaxy Digital	Bradmer Pharmaceutical	2018	N/A	Reverse merger
Kraken	Cryptofacilities	2019	\$100M	Acquisition of a regulated derivatives platform
Coinbase Custody	Xapo Custody	2019	\$55M	Horizontal merger of custody businesses
Facebook	Chainspace	2019	\$5-10M	Acqui-hire of blockchain development team to work on Libra project
Binance	JEX	2019	N/A	Acquisition of a derivatives platform
Coss	ARAX	2019	<\$5M	The industry's first token merger

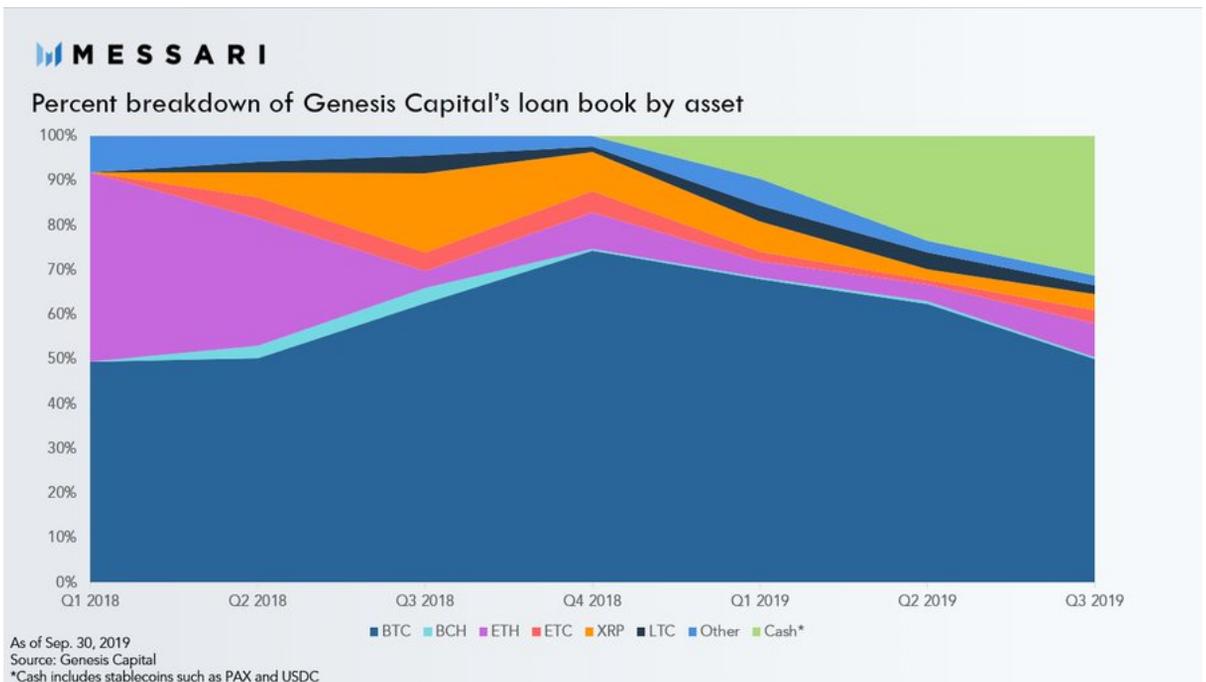
M&A 2018			M&A 2019		
Company	Industry	Deal Size	Company	Industry	Deal Size
1 Poloneix	Exchange	\$400 m	1 Kraken Futures	Exchange/Trading Services	\$100 m
2 Bitstamp	Exchange	400.0	2 Coins.ph	Payments	72.0
3 Earn.com	Crypto Finserv	120.0	3 Xapo	Custody	55.0
4 CryptoGlobal	Crypto Mining	80.7	4 CoinGeek Mining	Mining	34.8
5 Crypto 205	Crypto Mining	44.2	5 Freschette	Mining/Cloud	18.5
6 X2 Games	Blockchain Gaming	37.3	6 Neutrino	Blockchain analytics	13.5
7 Coincheck	Exchange	33.6	7 Blockchain Nordie	Investment Products	5.6
8 BitCity	Crypto Mining	31.9	8 Netcoins	Financial Software	2.3
9 Blockchain Dynamics	Security	23.2			
10 Blockseer	Data/Analytics	14.8			
Total:		\$1,186 m	Total:		\$302 m
			% Change Y/Y		
			-74.6%		

20. Protocol M&A. I was certain we'd see more protocol M&A by now, but a necessary pre-condition of chain mergers was likely tools that actually make chain migrations simpler. In the past year plus, we've seen ERC-20 tokens migrate to native blockchains, and non-ERC-20 tokens move to Ethereum (e.g. Tether). Cosmos launched as well as Polkadot's "parachain" testnet. With so many token teams sucking wind and watching their coffers diminish, this seems inevitable for teams that want to avoid the fate of becoming "zombie projects." TRON just announced its acquisition of content platform [SteemIt](#), and it's a matter of months before we see teams use treasury assets to buyout competing networks. This activity seems inevitable in proof-of-stake systems. We'll likely see some of those aforementioned ecosystem funds deployed (via token holder votes) to gobble up (51% attack?) smaller competitors.

Infrastructure Trends / Crypto Companies

1. Institutional Trading Tools, Custody, & Compliance It took a while for Bakkt to get out of the gates, but the ICE-backed crypto futures exchange has been steadily (if slowly) gaining market share vs. CME since its launch earlier this fall. Fidelity Digital Asset Services secured its New York State trust license. New institutional crypto custodians like Anchorage launched, while others merged (Coinbase-Xapo). Prime brokers like Tagomi launched to automate smart order routing and aggregate client trades on a “best execution” basis. Reference data experienced a major leveling up. In short, most of the critical pieces that were lacking in the last market cycle have been built and are capable of onboarding significantly larger customers. There might be some consolidation of these services if the market trades sideways for an extended period of time, but it’s tough to not get excited about the infrastructure that was built this year. <https://www.skew.com/dashboard/bitcoin-futures>

2. Lending Markets DeFi lending got a ton of hype in 2019 (more on that later), but it was the loan growth at centralized lenders that really went gangbusters. There was about [\\$650 million in loans originated](#) in all of DeFi. Meanwhile Celsius [lent out](#) over \$2 billion over the course of 90 days. Even upstart lending businesses like Blockchain.com, that began operations in late 2019 have been [lending over \\$100 million](#) per month. The majority of these loans are crypto denominated loans being used by investors to short assets, however, more recently we’ve seen cash loans collateralized by crypto taking up a growing portion of the loan market. Genesis Capital Q3 insights [provides insight](#) into the breakdown of their loan book.



Despite the growth, lending is still an immature and underpenetrated market. We expect loan growth to continue its torrid trajectory higher, and predict we'll see some spectacular lending desk blow-ups in the new year, as loan pricing gets more competitive and risk profiles rise.

3. Major Data / Research Upgrades. When we started Messari, CoinDesk and CoinMarketCap were basically the only data and information businesses with any degree of quality. Today, the Block, Decrypt, Delphi Digital, and a plethora of fund and exchange research groups offer a 10x improvement in the coverage and analytical rigor they bring to the market. Companies like CoinMetrics, Flipside Crypto and Kaiko (all Messari partners) provide exceptional and much more reliable metrics and data on the markets, blockchains, and off-chain trends affecting each protocol and its token. Still, there's a lot of wood to chop if we want to get a handle on anything that could be understood as "fundamentals" for a new asset class.

Case in point, I checked the 24 hour trading volume on OKEx according to five different top data providers, and got this as the result:

- \$523mm on CoinMarketCap
- \$67mm on the "Blockchain Transparency Institute"
- \$826mm on Nomics
- \$2.5billion on FTX's volume monitor (includes derivatives volumes)
- \$328mm per CryptoCompare

This is data for one of the largest crypto exchanges in the world. It's no wonder the SEC doesn't trust spot price data or have comfort with the internal compliance standards at even some of the most liquid global exchanges. Some of us, of course, will continue to drive data standards forward in the new decade, but the exchanges and projects have to meet us halfway with disclosures and some actual data standards.

4. Governance Tools: How do teams that start centralized decentralize over time? More specifically, how can projects launch and attract missionaries vs. mercenaries, now that it's clear the magic of bitcoin and ethereum's "fair" launches will not be repeatable. There are a limited, but growing number of precedents that give us a clue for what best practices might emerge as projects migrate from centralized company to foundation or fully entity-less DAO.

How might we identify the right sustainability models that attract long-term ecosystem players, or govern the foundations or tech councils that push commits to the protocol while minimizing the risk of self-dealing? How much governance should be enforced in code vs. legal entity levels, and how are the rules to the game updated over time? Zcash, MakerDAO, the Ethereum Foundation, Tezos, and many much smaller projects are learning on the fly, but I am sure that one of the biggest opportunities in crypto is in what could loosely be described as “governance services.” We’re reinventing how we organize people, so the staking services might be closest to the pulse regarding what tools are needed to optimally govern crypto protocols effectively. (It’s on my 2020 roadmap to firm up my political theory and history.)

5. Exchanges as Open Finance have nearly all the money and power within crypto because they pool liquidity. Yet since it is such a ruthlessly competitive business and switching costs are relatively low, the pace of new product and service development is torrid by necessity. When users can move their assets fluidly across dozens of global exchanges, they expect their exchange to have A-grade security and service, seamless UX, and competitive fees as table stakes. But they also want margin trading, lending options, staking services, tax reporting tools, and whatever else becomes en vogue in the coming years.

I’d encourage you to take the time to read up on this mammoth report on exchange history from [Nomics](#), and the Multicoins thesis on [Exchanges as Open Finance](#), where Kyle Samani asks, “What if the exchanges haven’t peaked, but instead are only in the beginning stages of their ascent?” It’s one that I buy into: exchanges can buy centralized services that become attractive, fork interesting lower-liquidity projects and bring their own liquidity pool to the same protocols, and offer their users a piece of the action via their exchange tokens. Their power won’t subside anytime soon. It will increase.

6. Exchange Hackings Will Increase. It was another eventful year on the exchange hacking front, with seven global crypto exchanges experiencing hacks that collectively cost them over [\\$150 million in digital currency holdings](#). Binance, UpBit, and Bitthumb were among the victims in the top 20 global exchanges by volume. The targets may only get bigger in the years ahead as these teams swell in size (exposing them to greater risk of social engineering attacks), and exchanges roll out more of the services described above. AUM honeypots will grow, so attack frequency and sophistication will level up in lockstep. One nuclear-level threat for crypto will be the exploitation of a cold storage vulnerability on par with what we saw at Mt.Gox in 2014. If a similar scale attack happened to Coinbase, Binance, or a bigger institutional entrant like Fidelity, you should probably just sell your stake and join another industry for a few years while the radioactive matter decays.

7. The Crypto Cowboy Survives. Last year, our head of research predicted a large, offshore exchange would face serious legal action from a U.S. regulator (regardless of the exchange's U.S. user access restrictions). "It will set up an epic legal showdown, as \$10 billion companies usually don't roll over without a fight." Oh lawdy, what a year it was for exchange giant Bitfinex.

The Hong Kong-based exchange lost access to \$850 million following the New York Attorney General's office [arrest of two men accused of laundering money](#) through a shadowy payment processor called Crypto Capital that Bitfinex had leveraged for banking services. The AG then [sued Bitfinex parent iFinex](#) after alleging the company "engaged in a cover-up to hide the apparent loss of \$850 million of co-mingled client and corporate funds" by borrowing from Tether, its affiliated stablecoin operator, to make up for the shortfall. Bitfinex disputed the AG's claims, raised a [\\$1 billion in a token sale](#) in May to fully cover the "temporary" shortfall, and then won a stay in the case against the AG's office that limited the amount of information they were required to share with investigators in the Crypto Capital case.

The company is still aiming to "unfreeze" the Crypto Capital assets they believe are being held primarily by European authorities, while still fighting off what they claim are [overreaching inquiries](#) from the NYAG.

There's so much to unpack here as you think about the state of exchanges in 2020 and beyond.

- Early crypto exchanges aren't necessarily "shady" or running afoul of KYC or AML laws, but their banking intermediaries might be! It all stems from the painful reality that crypto banking is still alarmingly scarce.
- Tether appears to have been fully reserved before the Crypto Capital scandal, contrary to earlier speculation to the contrary. Circle Trade's former head OTC trader, Dan Matuszewski claimed on a recent podcast (an absolute must-listen by the way) that he "knew for a fact" that billions of dollars were sent to create USDT because he himself initiated at least that much in new transactions amidst the market euphoria of 2017.
- Despite all the drama, Bitfinex remains one of the top three most liquid crypto exchanges worldwide. The outstanding supply of tether has doubled since the beginning of the year. Professional crypto traders apparently embrace the exchange's anti-fragility and Wild West approach to building the business. At least, for now. Although it is difficult to imagine a scenario where this persists as institutional traders begin to enter the market.
- If you make enough money, and don't do things that are flagrantly illegal, you can hire the army of lawyers necessary to keep you in business. Cowboys.

For an excellent skeptic's take on the drama at Bitfinex and Tether and what it says about the state of the crypto economy, you simply must take the time to read [this full synopsis of the two entities' dual histories](#).

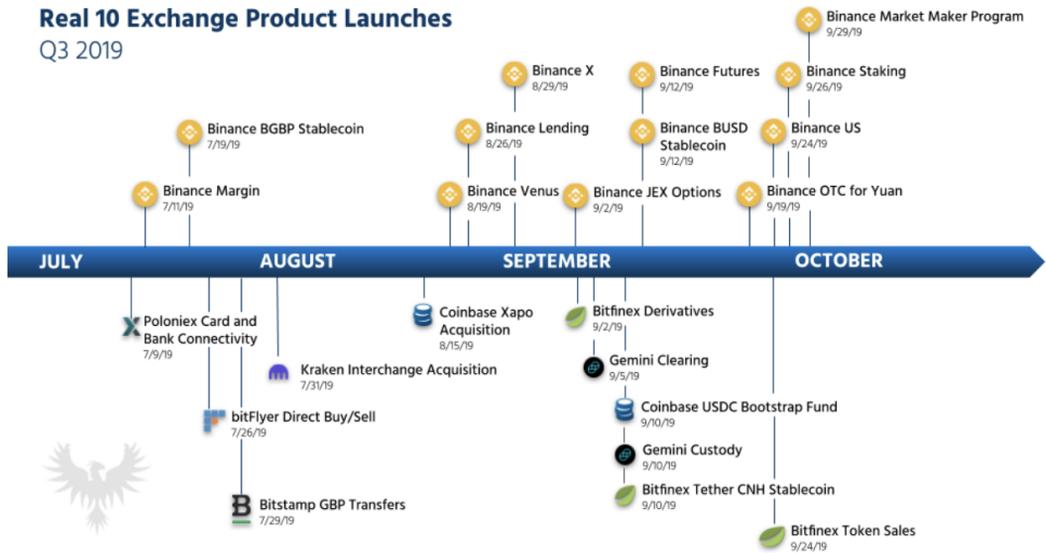
8 Coinbase vs. Binance There is no better illustration of the struggle for crypto supremacy than the ongoing competition between Coinbase and Binance. Coinbase remains in pole position to build the West's dominant crypto company and has redoubled its efforts to attract crypto retail users with a variety of new tools that promote "Open Finance", something it touts in its very mission statement. Coinbase will probably take a big chunk of the institutional market as well, given its unique position as the custodian of the world's largest fund, Grayscale's Bitcoin Investment Trust, and its recent acquisition of [Xapo's custody business](#). The acquisition of New York-based institutional prime broker Tagomi [was denied](#), but it makes a ton of sense; I hope it pans out in 2020.

Keep in mind, that Coinbase has maintained this lead *despite* a tumultuous year that led to remarkable ([and very public](#)) turnover of the senior leadership, including CTO, COO, Head of Institutions, VP of Engineering, and three *other* engineering directors. The resilience is astounding and speaks to the depth of Coinbase's ranks, as well as its competitive moat. Coinbase is still synonymous with "place to buy crypto" for millions of consumers, they have a Top 5 war chest to tap for M&A, and the company's engagement with regulators puts it head and shoulders ahead of its counterparts from a compliance and "trustworthiness" standpoint. Circle is no longer a competitor as it heads towards a winddown or sale (perhaps to Coinbase), Kraken does not offer nearly the same breadth of services, and new institutional entrants at Fidelity and Bakkt cater to different customers at (predictably) a much slower clip.

Coinbase's only real threat is geo-political, something with which its top competitor can certainly empathize. The pace of growth at Binance is legendary. It has been one of the fastest growing companies - in any market - of all time, hitting a billion dollars in revenue within its first 18 months.* And the company [shows no signs of slowing down](#).

What makes Binance work?

As Multicoin Capital has [quipped](#), Binance continues to blitzscale.



Sources: Kraken blog, Coinbase blog, Bitfinex Blog, Gemini blog, Bittrex News and Announcements, Poloniex blog, itBit blog, Binance blog, Bitstamp News and updates, bitFlyer USA blog, CoinDesk, The Block

*Technically, EOS creator Block.One is the fastest growing company in history, as its one year \$4 billion crowdsale was likely treated as revenue. But that's fodder for another time.

9. All other Liquidity Sources We could do a whole other report on crypto's broader market micro-structure (and likely will next year), but suffice it to say Bitfinex, Coinbase and Binance might not even be the largest or most important exchanges in the market today. So much crypto trading and liquidity takes place at the mega-OTC desks (where the majority of original order flow originates today), on "unregulated" futures markets like BitMEX (which is arguably THE source of price discovery in crypto today), and behind the great firewall at mega-exchanges Huobi and OKEx. That also doesn't even include the largest Japanese and Korean exchanges which may be nearly as large as Coinbase Pro. I've gotten more comfortable with Bitfinex over the years. But BitMEX still scares the shit out of me, and seems like a ticking time bomb from a regulatory standpoint. Fortunately, running the world's largest crypto casino means you can also afford great lawyers.

10. Security tokens Outside of exchange tokens, which are quasi-securities, and synthetic instruments, which we've covered in our DeFi section, security tokens are so irrelevant right now that I nearly forgot to include them in this report (let that sink in!) Arjun had the thesis right in his post last year, when he wrote one of his standing rules was that "No investment vehicle should promise greater liquidity than is afforded by its underlying assets." I agree, and this is especially true with assets that come with more regulatory restrictions than everything else that currently trades on crypto's infrastructure.

Here are the most interesting things that happened in the securities token market this year: Harbor [scrapped its \\$20 million dorm token sale](#), and the company's CTO left. SeedInvest may be the only business [Circle can't find a way to sell](#). tZero claimed it would raise \$400 million then \$100 million, [then nothing](#)? I thought maybe they raised a couple million after all that drama, but I don't care enough to look it up because the only thing I remember about the company is that Overstock CEO (and tZero booster) Patrick Byrne seemed to have used it to screw over his company's short sellers for a hot minute before resigning, fire-selling his shares, and moving to South America after "exposing the deep state." (Matt Levine's posts on this subject were pure art.)

Security tokens seem to be one of those solutions without a known problem, and are quickly taking the place of the "blockchain not bitcoin" as the most over-hyped and nonsensical meme in the market. If anything, companies seem sooner to decentralize their business models with token-powered networks than to tokenize (and destroy liquidity for) their equity and debt. Full scale crypto lending and derivatives markets need to materialize before security tokens get interesting in 5-10 years, so maybe we'll include them more prominently in our 2030 report.

Bitcoin Trends

1. For most people, it's still "bitcoin", not "crypto." If you're in the weeds, you forget that almost no one outside of the industry cares about anything but bitcoin. The reason is that you can explain it to a five year old. I don't care what the ethereum crowd rants about (and I love ETH!), there will be no "flipping" this decade because after a crash like 2018, people will only want to invest in money that they view is safe, secure, and simple. Bitcoin's got the lowest attack surface (because it's feature-poor), the longest track record, and the easiest-to-understand analog competitor (gold). There just isn't a strong anti-government counter-culture with Ethereum like there is in bitcoin ([in fact the ETH community skews left, while BTC skews right](#)), so it stretches credulity to think the strongest crypto narrative -- around government mismanagement of debts -- will attract people to ETH before BTC.

2. The halving only matters as a self-fulfilling prophecy. The halving narrative makes sense for high inflation assets because I think people don't really understand the impact that persistent daily selling pressure has on a given asset. Some analysts say halvings are all priced in because the information is known up front, but that assumes the crypto markets are rational, which they are, umm, not. The truth is probably somewhere in between. In the early stages of a fixed emission network, perhaps people get too trigger happy to accumulate, and underestimate how few people will follow them in line as the mining machines whir. Later on, the stakes are lower. Intuitively, it makes sense that (other things equal), [watching bitcoin inflation drop from 3.7% to 1.8% in six months](#) will be less of a supply shock than Zcash going from 32% today to 12.5% next November. Either way, sample sizes of two are not very scientific, and bitcoin needs bigger macro catalysts than a marginal 2% point reduction in inflation rates.

On the other hand, the halving does throw into stark relief just how limited bitcoin's supply really is. So the buzz around THAT could very well spark new demand. It's powerful to know that just two U.S. companies that report on their ongoing crypto purchases, Grayscale and Square, will, on average, purchase the majority of new network issuance every single day come Q3 2020.

3. There's only one bitcoin. I think we can call the fight when it comes to taking Bitcoin Cash any more seriously than another alt-coin like Litecoin. The reality is even bleaker for those hailing Bitcoin SV and some of the other garbage further down the fork list. The odds are low we ever see another meaningful hard fork of bitcoin unless 1) it becomes *obvious* that the security of the network is under stress from too-low block rewards, or 2) developers soft-fork in a "too good" privacy upgrade that forces supporting exchanges to fork away for compliance purposes. At current prices and sub-2% inflation, the mining industry shrinks to ~\$2 billion annualized in May, while securing ~\$700 billion in annual economic transfers, about in line with what the credit card companies do on a fee basis. I think about this as more of a 2022 or 2023 issue to keep an eye on if transaction fees don't begin to take a more meaningful percentage of the block rewards or the BTC price stays stagnant (or drops further).

4. Lightning It's tough not to be disappointed with the Lightning Network's [lack of growth](#) this year. Granted, it was a big milestone to have [Bitfinex come online](#) as the first major exchange to support LN. And granted, I'm aware that there could be some fully private channels and bitcoin locked in lightning that is under-counted there. And yes, fine, granted active nodes have at least grown 5x ([nice work, Casa](#)). Still, \$6 million in channel capacity? In comparison to [DeFi apps on Ethereum](#), that would only be good for #8 in terms of adoption, between Nuo and Bancor. Woof.

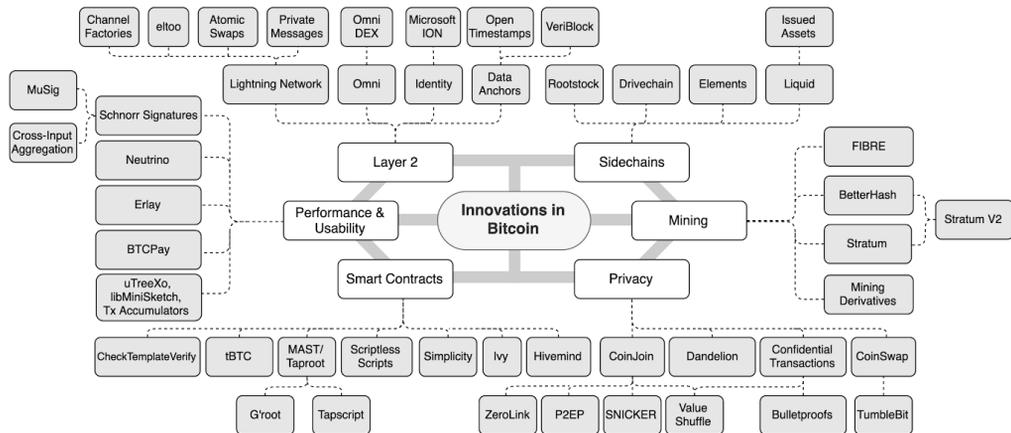
All that said, I'll double down on my prediction from January, that Lightning Network will have it's irrational exuberance moment, and blow up 50x YoY in USD growth to \$100mm in channel capacity (but 2020 vs. 2019). It's hard for me to believe Cash App won't release some features that spark that given Jack's 2018 investment in Lightning Labs, the addition of bitcoin core developer [Matt Corallo](#) to the bitcoin team in April, and the [expansion of the group](#) this fall.

There will likely be an inverse correlation between the number of assets a wallet / exchange supports and its likelihood of adding Lightning Support in the near-term. So begins the separation of the "bitcoin exchanges" from the "shitcoin exchanges"?

By the way, BitMEX research had an epic four part series on LN that you should read up on over the holidays if you haven't already, but want to learn more about the Lightning Network and are intrigued by some of the new payment applications it could power. ([1](#) [2](#) [3](#) [4](#) [5](#))

5. Layer 1 Privacy My co-founder Dan nailed this prediction last year regarding bitcoin privacy: *“Lightning could start to be used as a privacy layer for BTC transactions. There will be a lot more talk of privacy solutions for layer-1 on bitcoin, but no progress that impacts end users.”* I spent an hour looking around for the bitcoin roadmap to see if there were any target dates proposed by the community for when [privacy features](#) like Dandelion (obfuscates the IP address of the first node that broadcasts a transaction), Schnorr signatures (among other things obfuscates multi-signature transactions, which combined with “CoinJoin” could turn a pool of bitcoin transactions into a Monero-like jumble), and [Taproot](#), which could bring more scalable private smart contracts to bitcoin. I suppose it’s unknowable exactly when some of these will be soft-forked into the protocol, but I’d expect a soft-fork that enables Schnorr signatures by Q3, and almost certainly by year end as that upgrade is the linchpin of most of the exciting feature additions bitcoin developers are studying.

6. It’s maddening to keep up with bitcoin and ethereum roadmaps. Bitcoin’s doesn’t really exist, and Ethereum’s never gets hit on time. Thank you to Lucas Nuzzi of Digital Asset Research for this brilliant graphic that at least helps to organize the [state of innovation and the long-term roadmap within bitcoin](#).



He saved me from ripping out what remains of my hair, and I at least can feel good knowing that I have a categorized cheat sheet to reference for when our team pieces together timelines from John Newberry’s excellent [Bitcoin OpTech](#) newsletter and pairs them with the plain English explainers of Bitcoin Magazine’s [Aaron van Wirdum](#). Outside of Lightning and the major privacy upgrades, I’m most excited about some of the boring-but-important work that’s being done on the mining pool software front. Keep bitcoin (as) decentralized (as possible).

7 Bitmain will not go public in 2020. Bitmain may be battling back after a rough patch, but the company is still a shadow of its former self. Although, they've now [filed a confidential registration document](#) with the SEC to go public in the U.S., I'd be surprised if they actually pulled the trigger in 2020. Their valuation will be dramatically lower than the \$12 billion they had hoped to target in 2018. Their top comp, Canaan Creative, [dove 45% in its first two weeks of trading post-IPO](#) last month. The timing couldn't be worse for Bitmain financially going into the May halving during a sideways crypto market [amidst stiffer competition than ever before](#). You may have also heard they recently had [some founder drama](#) that might need settling in court.

8 Mining is back, baby! Denver-based miner Crusoe Energy Systems is opening a fourth bitcoin mining facility in the Rockies having recently [closed \\$70 million](#) in new funding for its new locations. The company is part of a cohort of firms who have set up shop in the U.S. to take advantage of the recent shale boom, including [Bitmain](#) and [DCG-backed Layer1](#). What's interesting is that these data centers merely use excess natural gas supply that would otherwise be lost to "gas flaring", when the energy companies literally burn capacity because they have too much inventory that might be more expensive to store or ship.

How about that? Energy-efficient miners!

It's a welcome development from a network risk standpoint to have more diversified mining capacity by country. And if Bitmain's IPO *does* pan out, I'd expect it to spark even more facilities development in the U.S. in 2020, even despite the upcoming halving. CoinShares published its [latest report on Bitcoin mining](#) last week, which found that one Sichuan province, Sichuan, accounts for 54% of global mining. Risky geopolitically, but also a net positive for the environment today as the 90% of that capacity is powered by renewables.

Table 9: Breakdown of Global Renewables Penetration in Bitcoin Mining

Region	Global Mining Share	Renewables Penetration	Share of Renewables for Mining	Share of Fossil/Nuclear for Mining
Sichuan	54%	90%	48%	5%
Relevant Remaining China	11%	44%	5%	6%
Relevant Non-Chinese Regions	31%	62%	19%	12%
Rest of World	4%	18%	1%	4%
Global Total	100%		73%	27%

Sources: Morgan Stanley Research (Oct 2018), EIA (Nov 2018), Natural Resources Canada (Sep 2018), R2E2 (Jul 2017), SATBA (Feb 2017), CoinShares Research (May 2019)

9. Sidechains, Finally? Similar to Lightning, Bitcoin sidechains haven't yet gained much traction since Blockstream's much hyped [whitepaper](#) in 2014. We still seem far off from having a realized vision of trust-minimized sidechains, but "federated" (i.e. consortium-managed) sidechains like [Liquid](#) and [RSK](#) are starting to see some pick-up.

BTSE, one of the 23 initial launch partners for the Liquid network, is [planning](#) to raise \$50 million in one of the first and highest profile token offerings on the Liquid network. The token would function similarly to existing exchange tokens with BTSE using 30% of all revenue to buy back and burn tokens. There was much gnashing of teeth from critics on [crypto twitter](#) calling out the hypocrisy of the Bitcoin community who had otherwise spent years criticizing ICOs and token projects. While my bias is that exchange tokens - as quasi-securities with actual company revenues to support them - are much more interesting products than your run-of-the-mill 2017 "utility" token. But I agree with the skepticism around [BTSE \(pitch deck\)](#). No way they raise the \$50 million they're looking for. It's a year late and an ERC-20 short.

Money on Chain, a DeFi startup, recently revealed it was [launching](#) a DeFi platform on RSK. The platform would offer a Bitcoin collateralized loan system similar to MakerDao on the RSK sidechain. The bull case is that DeFi on Bitcoin could leverage Bitcoin's liquidity and stability to offer a compelling alternative to DeFi based on Ethereum. The bear case is that it will be difficult to bootstrap a DeFi ecosystem on Bitcoin from scratch using federated sidechains. Not only may builders be skeptical of relying on a federated "trust" model, but they may also be anxious about forgoing the composability of Ethereum's burgeoning DeFi ecosystem.

Still, if Bitcoin sidechains are just a lesser version of Ethereum's fundraising and lending infrastructure, it's hard to get too excited. (*ducks for cover*)

10. BTC Privacy Canaries. There's a larger societal war on privacy taking place, and when it comes to crypto, Monero and Zcash are on the front lines. Monero should, in theory, be the most difficult asset for exchanges to support from a compliance standpoint because all transactions are anonymized by default via the protocol's ring signature scheme. But it's Zcash that will ultimately be the asset to watch as a privacy canary in the regulatory coal mine. Zcash offers unshielded t-address wallets along with its spookier z-address assets (fully anonymous). Because exchanges can default to supporting the t-addresses and verify the sender (in theory), Zcash should be at less risk of delisting by most of the major global exchanges. If it struggles with exchange support, it's a sign that bitcoin privacy upgrades will also present massive compliance risk.

The Multicoin team gave an [excellent primer](#) on privacy that I recommend reading in its entirety to get a better sense of the important trends to watch out for in 2020, especially. Multicoin draws a different conclusion than I do (that privacy chains are worthless themselves, as privacy is a forkable feature into any network), but the team sells short the power of the privacy-by-default meme, and their write off of ZEC because its performance has been horrible ignores the impact high inflation rates has had (temporarily) on Zcash’s attractiveness as an asset.

	BTC	ETH	ZEC (Transparent)	BTC + CoinJoin	ETH + Mixers	ETH + Aztec	XMR	ZEC (Sapling)
Sender	Public	Public	Public	Obscured	Obscured	Obscured	Obscured	Private
Receiver	Public	Public	Public	Obscured	Obscured	Obscured	Obscured	Private
Amount	Public	Public	Public	Obscured	Obscured	Private	Private	Private
IP Address	Public	Public	Public	(+ Dandelion)	(+ Kovri)	(+ Kovri)	(+ Kovri)	(+ Dandelion)

Legend
Public
Obscured
Private

Table 1: Privacy spectrum for cryptocurrency transactions.

From a technical standpoint, even Multicoin seems to concede that Zcash is best in class. Their argument instead is that bitcoin’s privacy by obscurity is “good enough.” We’ll see. If your life depended on doing a series of crypto transactions privately, wouldn’t you want to transact in the green zone there? If your answer involves a coin other than bitcoin, there's an investment case for that set of coins.

Other privacy coins that rely on proof-of-work face an uphill battle. If you look at the pressure Zcash has faced in the first three years leading up to its first halving in Q4'2020, it's impossible to get excited about [Grin](#), where it will take twice as long for its inflation to drop to ZECs level. That's too much sell-side pressure for too long. Disqualifying from a pragmatic standpoint, and it's got an inorganic mercenary community of VC-miners to boot.

Ethereum Trends

1. ETH 2.0 Research/Governance/Roadmap at a glance If history is any guide, we're not going to see ETH 2.0 until 2022 at the earliest, even if the earliest phases of "Serenity" begin getting pushed in mid-2020. ETH 2.0's rollout breaks down into seven (7!!!) phases and brings with it the promise of staking, sharding, a new virtual machine, and I'm sure more [dancing badgers](#).

(One of our analysts, [Wilson Withiam](#), put together an excellent overview of both the ETH 2.0 and ETH 1.x roadmaps for this report. They are critical to track and understand at a high-level given how much Ethereum's performance will affect other competitive projects and most of the DeFi and Web 3 infrastructure. So these next two sections are longer and more technical.)

Here's [what you need to know](#) about the current gameplan for crypto's largest platform.

[Phase 0](#) marks the launch of the "beacon chain", which will serve as the backbone for a new blockchain. The beacon chain will manage network validators (large early stakers like ConsenSys) and ultimately assign validators to individual shards (slicing the new blockchain into smaller chunks is a key, difficult, controversial scaling decision that's been made). The new chain will support Ethereum's new proof-of-stake consensus mechanism, and offer inflation rewards with new ETH2 for those that pony up and lock 32 ETH1 tokens into an irreversible contract. That [one way](#) bridge into the new system is also contentious, but it means ETH1 supply will start getting ["effectively burned"](#) once token holder begin claiming beacon chain validator slots. Initial reports claimed Jan. 3 as a realistic launch date (lol). It will be amazing to see this launched by end of June.

[Phase 1](#) will introduce 64 individual shard chains ([reduced](#) from 1,024!!!) to the network, with the option to increase the total down the road as the design gets tested. The Ethereum elite see sharding as the "key to future scalability" as shards can parallelize transaction processing, something that could improve network performance and reduce individual validator's costs (good for decentralization). It comes with big risk: this is still theoretical. No network the size of Ethereum has successfully sharded its blockchain. In Phase 1, shard chains will only contain simple data sets (no smart contracts or transaction executions) to test the system's structure. As with Phase 0, the beacon chain will continue to run in parallel with ETH 1.x throughout the phase. Don't expect Phase 1 anytime before 2021.

[Phase 2](#) marks the full launch of the ETH2 chain, allowing for on-chain contract execution and introducing the new eWASM virtual machine (dubbed EVM 2.0). At this point, existing dApps can start migrating their contracts from ETH 1.x to a specific shard (one shard per contract) in the new network. Storage rent, charging contract owners for storing data on the network (more on this below), is in the cards as well, which would require mass contract rewrites. Even though Phase 2 intends to replace the original Ethereum blockchain entirely, ETH 1.x may still live on as a shard within ETH2. (How confused are you by now? See why bitcoin will still dominate the macro narrative for a while?) A late 2021 release for Phase 2 is optimistic. Before the end of 2022 would be a win.

The final four phases are less defined, and without an attached timeline:

[Phase 3](#) implements state-minimized clients (because stateless clients are just too much). [Phase 4](#) allows for cross-shard transactions. [Phase 5](#) improves network security and the availability of data proofs. [Phase 6](#) introduces meta-shards, as in “shards within shards within shards,” for near-infinite scaling. If you’re scratching your head and are sadistic enough to read more, the [Sharding Wiki page](#) does note, “this may be difficult.”

Scaling and compilation efficiencies aside, the most notable change in Ethereum’s metamorphosis is the transition from proof-of-work to proof-of-stake. PoW is the more battle tested security model for blockchain networks, while PoS may prove to be more efficient but with new and less obvious attack vectors. For the more technical, we recommend reading Bison Trails’ Viktor Bunin on the subject of [PoS security threats](#).

Past research has also shown PoS requires an extra layer of “trust” vs. PoW, to help nodes sync to the network. Most models share specific characteristics to address this trust issue, such as allowing for a dynamic set of validators (rotate your security), promoting token holder [participation in consensus](#), and assessing steep penalties (slashing) for any network participant that violates the protocol guidelines. ETH 2.0 will function similarly, but may be able to learn from other PoS networks (and their R&D) as well as those come live and see real world issues. As Vitalik points out, recent research in PoS resulted in [“great theoretical progress.”](#) But...

Listen, we're talking about practice. Not a game. Not a game. Not a game. We're talking about practice. Not a game....Practice? We're talking about practice, man? We're talking about practice. We're talking about practice. We ain't talking about the game. We're talking about practice, man.

Vitalik was eight when this happened, so the [clip might help and prove metaphorical](#).

2. ETH 1.x Research/Governance/Roadmap at a glance. Ok, one more. Bear with us. Let's reiterate, ETH 2.0 is a **brand new** blockchain. It's going to be a chaotic and high-risk transition. In the meantime, the existing network needs to run existing applications (particularly financial settlements for DeFi transactions). More critical upgrades are needed in the current system.

To that end, ETH 1.x devs have three goals to boost performance and reduce blockchain bloat: (1) introduce client optimizations that increase transaction capacity; (2) cap disk space requirements and prune old, memory-sucking data (so running a node is less expensive and more decentralized); and (3) upgrade the EVM to eWASM, a newer open standard for code compilers that simplifies debugging, and is also used by all the newer smart contract platforms.

ETH 1.x developers have decided to split the major tasks amongst four working groups:

- [State Rent](#): Developers today incur a single payment for deploying contracts and storing data on the network. Thanks to the immutable nature of blockchains, this data occupies the disk space of node operators [permanently](#). As the network's state grows, so do operating costs, which is where "state rent" comes in. It makes sense to charge for ongoing storage needs since the node operators are on the hook in perpetuity. This is a big change as it could break a bunch of contracts, but also limits state growth and creates economic incentives to run a node. What happens to data that users don't want to pay for? Boot delinquent user data off the network but keep a stub (a hash) of information on hand in case the user wants to later reinstate it.
- [Pruning](#): Similar goal. Pruning removes old data that is longer useful, but does so in a way that allows clients to prove past transactions. There are a couple of ways developers think this is possible (e.g. maintain a proof of deleted chain segments, which is similar to a "light client" in bitcoin that makes it possible to run a wallet on your phone), but all current strategies would cap annual "state growth" to prevent spikes in storage costs, at the expense of some new complications (e.g., dApps might be unable to access some data, and nodes might be unable to tell if data was deleted or whether it never existed in the first place).
- [eWASM](#): Like ETH 2.0, devs plan to implement eWASM on the flagship Ethereum chain. The eWASM virtual machine, a subset of the well-established WebAssembly compiler, offers improved flexibility for the introduction of "high-performance" smart contracts.
- [Simulation and Emulation](#): This group develops tools to help support and evaluate the other groups because, well, someone has to test everything.

Core developers intend to introduce most of these implementations through a series of hard forks, the latest of which activated just over a week ago (Istanbul, Dec. 7). However, Istanbul's second phase, tentatively scheduled for Q2 next year, has Ethers at each other's throats. The controversy boils down to the fork's inclusion of [ProgPoW](#), an ASIC-resistant hashing algorithm designed to replace Ethereum's current algo. ProgPoW aims to even the playing field for GPU miners and ward off the entrance of potential ASIC competitors. The miners like that. But many miners and investors see ProgPoW as a threat to their investments. For miners, the change would shift the power dynamic away from mining farms and render expensive, specialized mining hardware useless. Ethereum (and ERC-20) investors intent on securing their assets might balk because ASIC miners typically prop up hash rates (overall chain security) and [their costs](#) "naturally create a price-floor for ASK prices of miners' sell-orders."

This saga is far from over. The infighting will likely continue leading up to ProgPoW's activation date mid-next year, and presents the strongest potential for a network split since "The DAO" fork that spawned Ethereum Classic. The looming transition to ETH 2.0 (and proof-of-stake) will likely deter investor pushback, because it's a short-term battle in a war the miners are ultimately going to lose, anyway.

Unless the roadmap changes *back* to supporting a hybrid PoW/PoS system, of course, but...

Oh my god, I'm just kidding this section is mercifully over.

3. ETH Killers Ethereum will face legitimate smart contract platform competition during its transition, and the most credible early favorites to attract defectors are likely Cosmos and Polkadot. Forgive me, but I'm skeptical of almost all the others.

As I wrote earlier, EOS is a disaster, and the worst fears surrounding its [cartel](#) seem to [be materializing](#). Stellar had to burn airdrop reserves because they literally [could not give this shit away](#). Most of the other ETH killers haven't launched yet either, and their communities are *tiny*. It's hard to imagine a glut of expensive VC-backed protocol tokens hitting a sideways market at the same time Ethereum soft launches staking (and those associated rewards) on its beacon chain, and that being bullish for the newcomers. I'm bullish on ETH, short the basket of everything else with that in mind, and that matters because you can't kill ETH without that sweet sweet monetary premium.

The knives are going to come out, though, for sure. Ethereum-now-Polkadot co-founder Gav Wood has acknowledged the new competitive dynamics, even if others are tempted to continue to extend the “we’re all in this together” platitudes. I read [Gavin’s piece on CoinDesk](#) earlier this week, and couldn’t have written the punch lines any better myself:

1: *“Monopolies make great returns for their backers. Duopolies are okay too. But an active market saturated with great teams doing awesome things is just not worth the bother. Large and vaguely strategic investors act as catalysts, unfairly popularising their own bets, sometimes against better alternatives. In other words, it’s winner-take-all. This makes the industry-wide “open-source” collaboration and technology sharing, which has characterized blockchain innovation so far, much less likely to continue.”*

2. *“Consider that Silicon Valley startups are not well known for giving away the engineering secrets to their core products. Sure, Apple “open-sourced” Darwin, but it kept the real jewels of OSX for itself. Ditto Facebook. Ditto Google. Companies share what makes strategic sense to share, but that rarely means sharing the really cool stuff. The game becomes increasingly zero-sum. This is already happening to some degree in our space with numerous well-funded and research-heavy startups like StarkWare and Dfinity refusing to open up the important bits of their technology. Some are even considering patents.”*

3. *As the payout from the winning ticket increases and the total winners are fewer, then in a zero-sum game the participants necessarily begin to start looking at each other not as comrades or a valuable resource but as obstacles to victory, to be removed. This doesn’t paint a pretty picture of the future.”*

According to Gavin, there’s no regulation or law that seems to protect crypto protocols from black-hat attacks, and no existential consequences for networks that benefit from competitors’ exploited vulnerabilities. This is unique to crypto and will likely exacerbate the problem, but also make the systems more anti-fragile. In other words, it gets (much) worse before it gets better.

“As smart systems operating under their own brutal rules backed by dizzying sums of money wake up and gain a form of self-awareness, existential desire will put those resources to work. Over time, governance-backed, economically-incentivized positive action will turn into outwardly-directed negative action against competitors. Initially, it will be the dumb networks that are eliminated.”

I agree. If you’re a public figure in crypto in 2020+, invest in a helmet.

4. Compatibility/Composability. “Developers don’t want to build on a moving target, and backwards compatibility should be taken seriously...Ethereum is not a toy anymore, it’s a platform with a sizable investment and a big reach, and as such changes like this need to be professionally measured before being taken.” So said Aragon One CTO Jorge Izquierdo once it became clear that last week’s Istanbul upgrade would break some 680 contracts on his team’s governance platform.

Indeed, in last week’s “Istanbul” hard fork, some Ethereum operations were repriced due to small changes, and [it broke thousands of dApps](#). Some argue a lack of backwards compatibility is itself a form of censorship (one reason the bitcoin community has balked on principle on non-essential hard forks), but then again Ethereum arguably has the luxury of this sort of fast-and-loose approach given the enormity of the bigger change that lies ahead with 2.0. It’s caveat emptor when building on ETH 1.x today, and teams should know that now. The question is how much bigger can DeFi get before these structural issues are definitively resolved.

The bigger fear may be around *composability*, though, which impacts the ability of developers to modularize app development across multiple interoperable smart contracts. The question is how old contracts will migrate, and how they will remain interoperable in an environment where these things might exist on parallel “shards” of the new network. It’s wonky stuff, but this was a big enough concern that CoinDesk’s Leigh Cuen wrote a [controversial article](#) about it during DevCon that inspired a near immediate response from [Vitalik](#). Proposals for smart contract migrations to ETH 2.0 that protect Ethereum’s composability are the most important area of development we’ll monitor in 2020-2021 as the community gears up for the ETH 2.0 launch.

If Ethereum handles its composability and backwards compatibility challenges, we’re unlikely to see mass defections to other competitors. (The devil you know.) But that’s a big if, and it’s a narrative competitors will hammer away on during the aforementioned blockchain wars.

I think Dan got it right in our prediction piece last year, “platforms will run aggressive marketing campaigns, but stall as ETH’s culture, grassroots mindshare, and developer network-effect lead prove too strong to overcome.” This is still Ethereum’s race to lose, even if its governance processes leave some professionalization to be desired.

5. ETH is money (for DeFi). I can't imagine a scenario where high-throughput applications run - *or should run* - on Ethereum vs. another purpose-built blockchain for a given non-financial Web 3 application. The "world computer" narrative was marketable, but in practice, Ethereum is limited in terms of ["throughput, latency, and cost constraints."](#) Its current network design cannot support the requirements for every potential use case. The CryptoKitties crisis was just one example -- an event that snowballed to the developer team at dApper Labs opting to build a high-throughput alternative. This is the ["unbundling of Ethereum"](#) among non-financial verticals.

The glaring exception to this trend is DeFi for two notable reasons. First, an open financial ecosystem requires a robust aggregate economy and sufficient liquidity to function, which no other smart contract platforms can support at the moment. Second, Ethereum's latency and gas requirements do not undermine the user experience for financial asset settlement. Fees are the norm in finance, less so for in-game actions.

6 Privacy on Ethereum Privacy guarantees for certain types of Ethereum contracts should improve markedly following the recent "Istanbul" fork. The upgrade reduced gas costs necessary to power bandwidth-heavy contracts that incorporate zero-knowledge privacy technologies, and protocols like [Aztec](#) have developed a series of contracts that help build out Ethereum's privacy pool. AZTEC is not the first effort to bring zk-snarks to Ethereum: JPMorgan revealed they were adding zk-snark technology to their private ethereum fork, Quorum, and EY introduced a similar implementation called [Nightfall](#) earlier this year. This in addition to a growing number of wallets (e.g. Argent) that include "mixers" as part of their core product. These privacy tools get more robust, on a compounding basis, as additional assets and contracts that leverage them grow the overall privacy pool and create a larger "crowd" in which to obfuscate transactions. I'm especially excited to see how the [partnership between Carbon and Aztec plays out](#), as a stablecoin that incorporates zk-snarks seems like a killer app.

7 Developer Tools It's helpful that Ethereum has been live for just four years. Critical developer infrastructure is still missing, which is one reason we haven't seen more instances of product-market fit in the "dApps" space. By any measure, 2019 was a banner year for some of the pre-requisite building blocks (i.e., wallets, node and data services, code auditing tools, etc.)

Node infrastructure in particular has improved. A multitude of new managed node providers launched or expanded operations to offer a simpler alternative to Geth and Parity nodes and a more robust service than ConsenSys's Infura. Initiatives range from the developer-focused, such as Bison Trails, Alchemy, Blockdaemon, and Quiknode, to end-user focused, such as dAppNode and Vipnode. Infura for its part, is aiming to shift towards a more decentralized, less-AWS reliant model. When it comes to critical core infrastructure, the more the better.

Data querying abilities also reached a new level of simplicity thanks to the remarkable rise of The Graph. In the 11 months following a [\\$2.5 million raise](#) in Jan., The Graph added support over [400 smart contract subgraphs](#) for Ethereum-based projects and now sees request volumes in the millions per day. It's one of our top companies and projects to watch in 2020.

8. ConsenSys resurgent? There are few companies you could argue are existentially important to Ethereum, but Joe Lubin's "venture production studio" is one of them. They had a brutal end to 2018 with hundreds of layoffs and project spinouts as the price of ETH plummeted. But I said last year that "rumors of ConsenSys's death have been greatly exaggerated," and that seems to be directionally correct, even though ETH is flat on the year. The company's infrastructure companies are all well-funded, even as the side bets and fat have been cut. No one has ever increased their risk by focusing, and ConsenSys is no different. A cursory look at [their home page](#) highlights the new logical orientation of the business. I expect a big 2020 from them, and wouldn't be surprised to see a nine figure investment from a strategic partner like Microsoft.

9. Proof-of-stake risks: I have never really wrapped my head around proof-of-stake. We talked about it a bit above, but it seems too easy to centralize and create a "rentier" class of oligopolists that control these networks. That could expose the "validators" to censorship or worse. What we're seeing unfold with staking services is basically leading these risks to compound at hyper-speed: intermediation drives most staked assets to exchanges, and then lending markets ("[super-fluid collateral](#)" as my friend Dan Elitzer put it) encourage the centralized services to offer risky synthetics on top of those locked deposits. That's bad enough (think: mortgage-backed securities, but backed by memecoins vs. homes), but [Digital Asset Research's Lucas Nuzzi](#) highlights another problem that's potentially much bigger / existential. Because the ease of exchange has reduced exchange AND network switching costs:

"A "synthetic staker" in one network is an exchange rate away from staking in another network. Whales now can just chase yield and engage in "staking arbitrage" across PoS networks. Like bonds, the staked asset is paying a fixed yield in its own denomination, but price of what's staked (bond price) fluctuates based on opportunity cost (real yield). At expiration, intermediaries simply adjust the collateral. After all, they make money in trading fees now. The security budget (or the cost-to-attack) in PoS networks becomes highly sensitive and volatile, like the price of the staked asset as a result. And lower price leads to lower (more volatile) security, which further depresses price: a true death spiral.

Perhaps there are solutions (i.e. hybrid PoW / PoS systems like Decred), but this theoretical problem likely applies to most proof-of-stake networks not named ETH, and ironically gets worse as the markets get bigger and more liquid. The further down the pecking order you get, the bigger the risks.

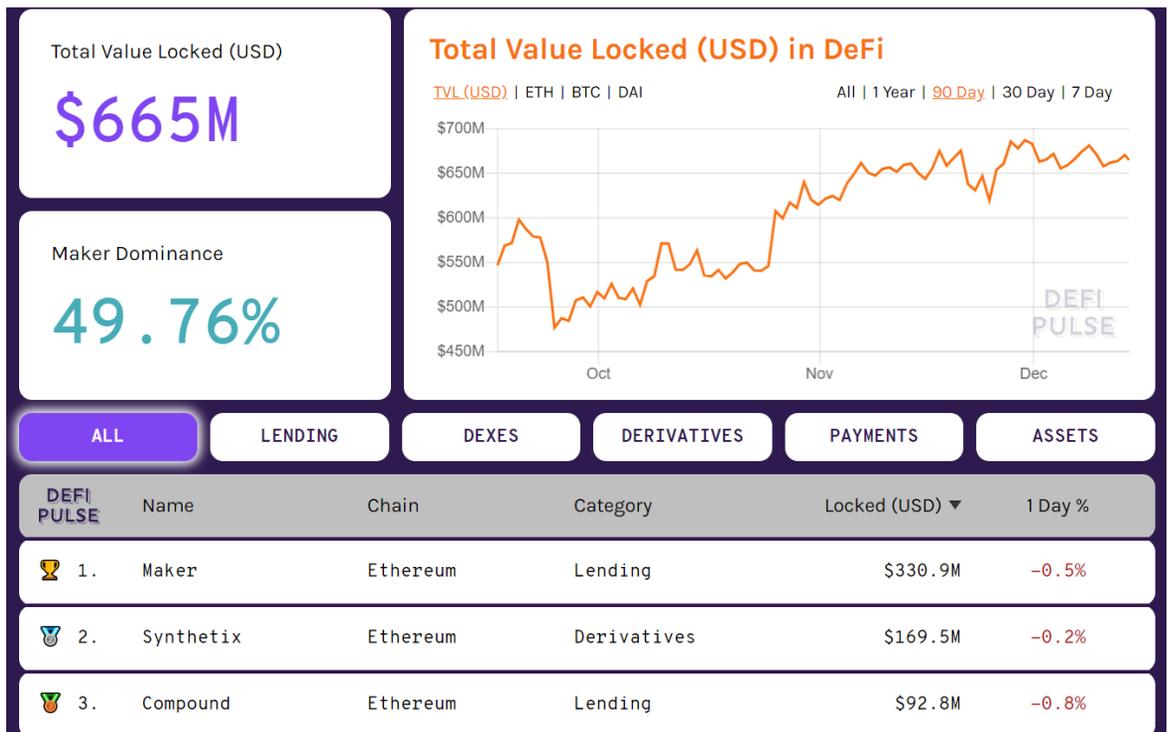
10. Other assets not covered. I don't have a number 10 for Ethereum this year (because some of the above sections were huge and the ETH sectors of "DeFi" and "Web3" exist as standalone sections), but this is the optimal place to remind you I know there are many "exciting" assets in crypto beyond BTC and ETH and those elsewhere referenced.

If your favorite isn't mentioned herein, it's either because a) I don't take it seriously, and I'm following the old Grammy rule of "don't say anything at all," (most likely) b) our customers don't and likely won't give a shit about it in 2020 (strong overlap with 'a'), or c) that particular asset has some work to do before it's coverable (marketing, exchange listing, actual adoption, etc. which has a strong overlap with 'b'.)

Also, if I say "I like token #347 on CoinMarketCap" (because we don't even cover it on Messari yet), then Toby from our team is going to flip his shit on me for making implicit investor recommendations on a penny stock. Toby protects me, and still lets me tweet from my own account. He also knows that I've already spent too much time on this 60 page beast to opine on much more than I already have.

DeFi Trends

1. Maker: No longer the end-all be all for DeFi. The incredible progress of DeFi in 2019 can largely be traced back to MakerDAO, the industry’s most systemically important protocol. Maker’s Dai underpins the majority of the DeFi ecosystem and remains the largest and most battle-tested collateralized stablecoin solution. However, it’s no longer the *only* important DeFi protocol, and will likely face steep new competition on the lending and stablecoin fronts. MakerDAO led much of the [growth](#) in value locked in DeFi through the first half of the year, doubling from ~\$250 million in January to ~\$500 million in July. That’s when the rise of new DeFi protocols began in earnest. Maker now [locks](#) ~\$330 million of ETH in DeFi, while protocols like Synthetix and Compound have locked \$260 million combined. Maker “dominance” dropped from 90% in the beginning of the year to just below 50% today according to [DeFi Pulse](#).



Maker realized its long time vision of launching [Multi-Collateral Dai](#) last month, which introduced support for new collateral types besides ETH and added the critical new Dai savings rate (DSR), a “risk-free rate” on Dai that will help ensure Maker stability fees are kept in check, as Maker holders now have an alternative lever to pull to increase Dai demand (like anonymized central bankers). These feature additions should attract a new collateral base in 2020 that sparks growth and adds new stability mechanisms for Dai.

2. Synthetix Soars. Synthetix, a protocol for issuing synthetic assets, has seen its volumes grow from under \$1m in August to nearly \$10 million in December (based on 30-day moving average), and introduced a new stablecoin, Synthetix USD (SUSD) that could rival Dai. While SUSD's market cap of ~\$10 million is still an order of magnitude lower than Dai's, Synthetix as a platform is [growing fast](#), and is bound to attract attention now that its token soared 3300% in 2019. We don't think this project is a flash in the pan, though there is some concern about the reflexivity of the Synthetix token (the value locked in Synthetix while minting new types of synthetic tokens is the SNX token *itself*, which screams "systemic risk").

We wrote last year, "dollar-backed stablecoins would catapult "open finance" into mainstream adoption. The idea of dollar backed stablecoins will be generalized to other asset classes, i.e. a token that tracks S&P 500. New crypto indices that mirror traditional asset performance (synthetic crypto securities) are a massive untapped (but technically illegal) market that could pick up steam in 2019." How can you mimic returns in the S&P for an investor in Indonesia that can't buy the index directly? Synthetix is on the bleeding edge of answering that question, though again we've already [seen the risks](#) that stem from their reliance on immature oracles to power these contracts. (More on oracles below.)

3. Not-so-DeFi. DeFi protocols tout themselves as open, permissionless, censorship resistant etc. but it's a bit early to trust those sweeping, aspirational claims. Earlier this year, an [audit found](#) Compound had administrative privileges that allowed the team to change various parameters and censor transactions. The team quickly [upgraded](#) the protocol, but the message should have been clear: don't trust the "De" in DeFi during these beta stages. If anything, it's a good thing some of these early stage networks have strong community leads at the helm. Consider the contrast between the speed at which the Maker Foundation addressed a [recent vulnerability](#) with that of Augur, whose community struggled for months to reel in the malicious behavior of a [single anonymous prankster](#) as he created a number of sham prediction markets throughout 2019.

4. Superfluid collateral (aka "how can I destroy the system?") and on-chain derivatives. To date, DeFi participants have mostly behaved benevolently towards their peers. This may be due to the fact that most early adopters are ideologically aligned early token holders. That will change as DeFi's growth continues to explode, and investors figure out how to put on effective short positions. Critics have pointed out security [holes](#) in these DeFi systems before, and some may begin attempting to break contracts and [seize](#) collateral soon. Risks compound as protocols continue to build atop one another. Much like the mortgage-backed security crisis, it will be tough to unwind collateralized DeFi positions in the event of a system-wide "black swan" event. In fact, I'm convinced the Defi space must have a major exploit a la "The DAO", where investors get completely wiped out, before resetting and rebuilding with a bit more rigor.

Given the risks of systemic DeFi failures, most practitioners will require better hedging tools before they put any real capital at risk. [Ohmydai](#), based on the [Convexity protocol](#) white paper is an early example of ways users might be able to buy put options on Dai (sell Dai for 1 USDC at any point in the future). It's like a credit default swap on a protocol that already mimics credit default swaps (I love crypto), but it makes sense! If you're making a good net interest margin on your Dai lending book, you might happily pay a point of spread for this sort of insurance. If 2019 was the year of DeFi lending, 2020 will be the year of DeFi derivatives. Long hedging, short risk.

5. Departments of DAOs While the original DAO had a grandiose vision of something akin to a leaderless Softbank Vision Fund for the people, we saw a resurgence of much smaller and careful experiments in DAO design. Examples include [MolochDAO](#) (allocation of ETH 2.0 funding grants), [MetaCartel](#) (Web 3.0 dApp development grants), and the [MarketingDAO](#) (a community governed marketing fund for Ethereum). So far, these have worked because they have managed public goods and expense accounts, not investor capital. But the 2019 successes showed how DAOs could effectively coordinate human financial actions. That's big. In 2020, the first "for-profit" DAOs won't be very far behind.

6. Centralized exchanges experiment with Open Finance This past year we watched every exchange do what they do best - follow Binance. Most of the non-US exchanges have already followed Binance's lead in selling their own exchange tokens. After the release of the [Binance Launchpad](#), nearly every single major global exchange followed suit with an IEO platform. When Binance launched its own blockchain, others followed. Exchange tokens represent a new breed of affinity tokens - part loyalty coin, part lottery ticket, part equity share. And as some exchanges migrate tokens to their own native blockchains and decentralized exchanges (vs. Ethereum), the line between company and network begins to blur. It could make sense for a large exchange chain (like BNB) to fork a DeFi protocol like Compound that already has demand, but negligible relative liquidity. If exchange tokens (and their corresponding liquidity pools) can entice DeFi users to switch networks, then Ethereum's DeFi protocols could be relegated to testbeds.

7. Decentralized exchanges experiment with centralized finance. In the world of exchange, liquidity is king. That's true in both the centralized and decentralized world, and that was further validated by P2C (peer-to-contract) models like Uniswap, an [automated market maker](#) that enables anyone to get paid in return for depositing capital into a shared liquidity pool. The P2C model is particularly effective because it removes the need for a counterparty along with the associated complexity of providing liquidity to a decentralized order book. That's why Uniswap is thrived at a time when P2P models were sucking wind.

Total Value Locked (USD) in Uniswap



Now it looks like Uniswap could be the solution to making illiquid security token markets as well. With some legal engineering, it may be possible to create a whitelisted security token for a defined type of (KYC'd) traders and facilitate trading on a P2C market. RealT just [sold](#) a property in Detroit to investors across the world with a Uniswap-supported security token that represents fractional ownership and rental income rights for holders. Centralized securities token exchanges may take years to build sufficient liquidity and secure regulatory licenses before they become interesting or available to end issuers. Uniswap could be faster to market because the stakes are smaller (for now).

Uniswap is the lone bright spot amidst a [disappointing year for DEX](#) projects and their trading volumes (down with the rest of the market). These protocols may be essential for cross-chain application interoperability (contract to contract or machine to machine payments), and could still win out over centralized exchanges when it comes to trading less liquid or difficult to support tokens (privacy focused or quasi-securities), but spreads will remain high, and centralized exchanges and OTC desks will still account for 99% of volumes for the foreseeable future.

8. Lending Markets Lending has emerged as a growth market in general, but it's especially huge in DeFi. Over the course of 2019 DeFi protocols originated [\\$650 million](#) in loans, with [\\$450 million](#) currently locked up as collateral and [~\\$75 million](#) in loans outstanding according to [LoanScan](#). Compound (which does not have a token), is now second in value locked behind Maker amongst lending protocols and has drawn the attention and [investment](#) of top crypto investors. (Is there a long-term business model, though, if billion-dollar exchanges fork your code without repercussions?)

Loans Originated

YTD VOLUME

\$653,432,393

YTD TRANSACTIONS COUNT

284,291



BY ASSETS			BY PROTOCOLS		
PROTOCOL	SHARE	AMOUNT	PROTOCOL	SHARE	AMOUNT
Maker SCD	42%	\$276,119,232	dYdX	36%	\$234,166,967
Compound v2	22%	\$143,146,486			

Collateralized lending is a start, but a new financial system won't be built on collateral-based lending alone. We're still waiting for better decentralized identity and credit scoring apps to fill the void in today's DeFi lending equation. Until we get there, lending will be limited by the value of all crypto held as collateral. That's probably a good thing for this experimental stage, as the real risks are around smart contract security, governance, and collateral auditability. The potential for a DeFi bank run is under discussed, but Alethio explained the mechanics well in an excellent post [here](#).

9. DeFi Wallets Monthly originations in DeFi lending increased by 5x to over \$100 million per month this year. As crypto-collateralized lending began to find product-market fit, attention shifted (naturally) to capturing the user relationship. New DeFi interfaces are aggressively competing to become the one-stop-shop where users can hold, transact, exchange and lend all in the same place. The most successful interfaces will be the exchanges (existing audiences) and the tools that best abstract away the complexity. Betterment-LendingClub- Robinhood hybrids like [InstadApp](#) and [Zerion](#) raised money from prominent investors like Pantera Capital and Placeholder. I'm expecting these teams and others ([Linen](#), [Argent](#)) to raise more money in 2020 to compete as the gateways to crypto for "self-sovereign" crypto users.

10. What's changed from last year? I thought prediction markets, token curated registries, and "continuous organizations" were exciting earlier this year. I suppose I still do, but prediction markets have taken a serious step backwards. Augur has just 13 active markets with under \$3mm in locked value today, and its most promising startup [shut down in July](#) after just six months of operations. The 1.0 incarnation of TCRs are static dogshit. No one has innovated in that area since 2017, and the curation market design we initially proposed for Messari's own token registry will end up looking more like a DAO / work token when it eventually goes to market. ICOs/IEOs are on their last legs, but will be put down like the lame horses they are soon enough. (We just need to get through this spring's round of disastrous private SAFT liquidations.) I'm still excited about the concept of "Continuous Organizations", which seem like they could be like this year's "Uniswap" of ICOs. (Keep an eye on projects like [Fairmint](#).)

Web3 Trends

If you want to “re-decentralize” the internet, there are some critical pieces of infrastructure you need to ensure are in place first. Decentralized hardware, computation, domain registry, identity and governance systems are just a few. Let’s dive into the infrastructure that’s been built so far, and peak around the corner at what’s next in the non-financial Web 3 stack.

1 Decentralized Hardware. It’s unclear whether there’s real demand for many non-financial “uncensorable” applications today given their sky-high costs relative to centralized alternatives. Most new hardware projects and marketplaces will face significant challenges in bootstrapping their networks to the point that economies of scale kick in. That said, two projects we’re excited about are [Helium](#), which has created a protocol to incentivize the buildout of a wireless IoT device network, and [Orchid](#), a decentralized VPN protocol. Orchid is especially interesting as part of the crypto commerce stack, as its protocol helps node operators earn tokens by providing bandwidth to users in a tor-like routing network and decentralized marketplace.

2 Compute/Storage Along with the “utility token” narrative, demand for decentralized storage, computing, etc. seemed dead this year. We still believe in the thesis, though I think we properly set expectations last year: *“this is a five year vs. 2019 trend; these tokens will be critical to fueling Web 3.0’s future growth.”* I’ve gotten more bullish on digital resource tokens recently. As government surveillance ramp up, the “Airbnb” model for excess file storage / compute / data gets compelling much sooner than I thought it would. Filecoin released its [public testnet](#) last week with an anticipated mainnet launch sometime around the start of Q2. (At this point, I’ll be liquid on my FIL tokens by 2023 or 2024.) Storj is in a final beta phase leading up to its production launch, scheduled for [early 2020](#). Sia is expanding into video streaming storage thanks to a mid-summer [\\$3.5 million](#) raise, and has some valuable regulatory clarity in the form of its settlement with the SEC for the 2014 Sianote offering.

So these projects are real now, but it’s unclear to what degree Filecoin’s mainnet launch and token distribution will ultimately be hindered by its initial reliance on the controversial SAFT fundraising instrument, and how that will impact their eventual token distributions. If the team can resolve outstanding issues with the SEC (I think they will), then the Web 3 storage market is Filecoin’s to lose. Its remaining ICO warchest gives it plenty of runway to outmarket and outlast competitors. Areweave may be the other platform to watch, as they launched late last year and recently raked in [\\$5 million in funding](#) from a good group of [investors](#).

3. Replacing ICANN. It's clear the current DNS/Certificate Authority needs an upgrade. Nothing spoke to that recently quite like a private equity firm [buying the entire .org domain name space](#) for \$1 billion. Token Daily's Imran Khan published a terrific post last year on how exactly the current system is [centralized and inefficient](#). Handshake remains the favorite to solve the issue, especially among the developer crowd. (At least in this market cycle...we remember Namecoin!) Handshake still hasn't emerged from development, but community sentiment indicates it could be barreling toward a mainnet launch (and [massive token airdrop](#)) within the next few months. If true (I think it is), it will be interesting to see which sites seek a Handshake-powered solution. Disgruntled .orgs working in tech / libertarian markets would be a good starting point.

Handshake isn't alone in the race to replace the old registry infrastructure. Draper-backed Unstoppable Domains [expanded its domain markets](#) to include Ethereum addresses (using crypto) in October after launching auction markets for Zilliqa domains earlier in the year. Its top rival, the Ethereum Name Service (ENS), completed a major upgrade back in May, which allowed it to start issuing Ethereum-based [domains as NFTs](#). Most Unstoppable Domains and ENS customers are purchasing domains as a replacement for convoluted public key addresses or as possible investments. But neither startup offers a more complete solution than what Handshake is promising.

4. Blockstack. We're going to see fairly quickly whether its tenable for a crypto token to survive the SEC registration process, and promote a fully functioning network and community. By going the Reg A route Blockstack allowed non-accredited U.S. investors to purchase STX tokens while simultaneously making it all but impossible for those investors to sell the tokens on any exchange based in the country. So what's the plan? Down the road Blockstack believes the project could be "[sufficiently decentralized](#)", which would allow them to deregister the tokens.

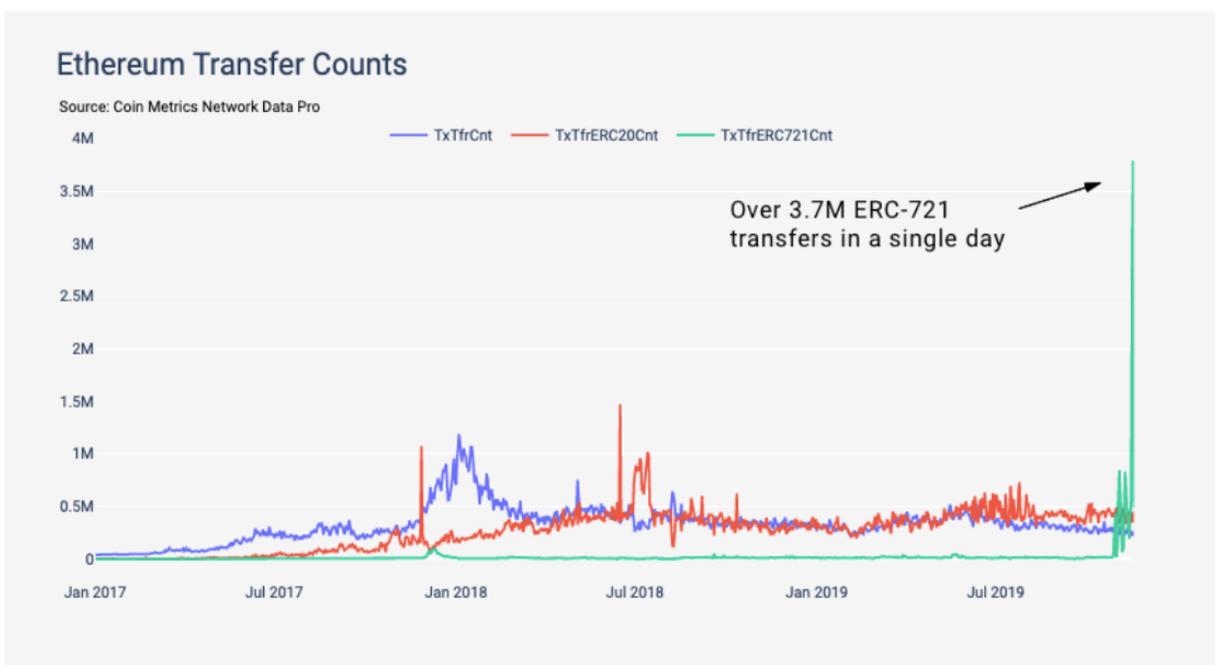
Outside of the novel token issuance, Blockstack is tackling something that actually matters (a rarity in crypto these days) and building a new tech stack that aims to give users total control over their application data. Blockstack was more than just the inspiration for the new Silicon Valley plotline. Their [marketing](#) is pretty good too.

5. Oracles I'm baffled by Chainlink. Is it the solution to the evasive [Oracle Problem](#)? Or is it an overhyped project that seems to have inherited the #XRPArmy as followers? Tech giants [Oracle](#) and [Google](#) recently announced plans to use Chainlink's network for data sharing purposes, and multiple large Ethereum-based projects, such as [Synthetix](#) and [Streamr](#), have turned to Chainlink for reliable data feeds. But I still don't understand the economics of the token itself? And I definitely don't understand them at \$1.3 billion in network value.

Outside of Chainlink, various DeFi protocols - [MakerDAO](#), [Compound](#), and [UMA](#) among them - also introduced new oracle designs in 2019 to remove the layer of trust associated with their price feeds. Financial protocols and applications like derivatives need ultra-reliable data (obviously), but there's diminishing returns with all these new oracle releases. I anticipate the rate of new releases will decline, and the variety of solutions will ultimately contract as projects merge their designs and converge on a unified oracle contract standard. There's no reason why MakerDAO wouldn't adopt some of UMA's Data Verification Mechanism elements, for instance.

6. The Web 3 Browser Brave has been the quintessential example of how an app's adoption mustn't necessarily correspond with value accrual to token holders. The Brave browser and ecosystem are growing [fast](#), with Brave now claiming over 10 million monthly active users. So far, that's had little impact on the BAT price, though Brave will be an interesting project to watch as the company has already done the hardest part in creating a quality product that people actually want to use at scale. With their rate of adoption, BAT is a prime candidate for experimentation with new token economic models that could bring unique value to Brave's users ([rewards](#), [tipping overlay](#), etc.)

7. Gaming as in NFTs Demand for crypto-collectibles dried up almost as quickly as it caught on with CryptoKitties. The free-fall in user interest was not surprising as "card" games that leveraged non-fungible tokens seemed like a niche market that offered little value compared to larger franchises with in-game virtual goods. Then "Gods Unchained" happened. Demand for the (at-the-time) mildly popular NFT trading game exploded after gaming giant Blizzard opted to blackball a professional gamer on its platform for publicly backing the Hong Kong protestors. The Gods Unchained team [called out](#) Blizzard for the move, and this happened:



Source: [CoinMetrics](#)

I'm not sure I'd call this show of moral support an NFT resurgence per se, but the [rise of NFT marketplaces](#) and Microsoft's interest in [offering crypto collectible rewards](#) to Azure customers are two additional promising data points. In the meantime, the de-platforming trend is getting more real and economically dangerous, which makes me more bullish we'll see some willingness for gaming companies to allow goods to trade freely across ecosystems. The good news is the NFT space has time to identify more suitable, high-throughput environments to build on. Most of those platforms are still in the early stages of development and likely won't be ready to support such games for 1-2 more years anyway.

8. Gaming as in Gambling. It's understandable users have gravitated towards blockchain gambling apps. Online gambling operations remain banned in the [US and most of Asia](#), two of the largest crypto user bases, and permissionless platforms offer a refuge for the risk-seekers in these countries. dApp.com's latest [dApp Market Report](#) shows that gambling applications represent more than twice the market share as any other gaming sector in terms of active users, transactions, and volume.



It's also interesting which chain(s) these apps call home. Most online casinos have opted to build on low-to-zero fee, high-throughput platforms like EOS and Tron (for now), as they were happy to trade off censorship resistance for increased performance and higher profit margins (should apps look to subsidize users by eating transaction fees for the sake of adoption).



Or so they thought. A [report from Coinbase](#) and a [30-day notice](#) posted by EOS-based dApp EarnBet suggest things are not all fun and games on EOS at the moment. An early November spike in on-chain user actions threw the network into “congestion mode,” making it excessively expensive to execute any transaction. Could this EOS implosion actually spell good news for (dare I say) Tron? Maybe, but we’d actually see layer two solutions like Loom Network being the ultimate beneficiaries of EOS’s congestion. In the long run, expect to see the online casinos build on their own Polkadot parachain or Cosmos zones.

9. New social platforms Decentralized social media projects are early; but the potential is there. I don’t really buy the near term potential that users will go for the explicit financialization of their previously intangible social capital. (Remember the rags-to-riches reddit gold stories? Me neither.) The real challenge with “decentralizing” social media is not the incentive models, but in the user acquisition away from the large incumbents, who are so entrenched that you might argue the real decentralizing innovations may *have* to come from them (or regulatory actions). In the face of continued challenges to free speech across the media landscape, expect to see more calls for [protocols, not platforms](#).

The longer we go without seeing Telegram’s TON, [Kakao’s Klay token](#), or Signal’s Mobilecoin, though, the more skeptical I get about their potential, and the more they begin to look like overt 2017-2018 cash grabs. I do believe in Jack and Twitter, though. As I noted in the “people to watch” section, [Jack](#) recently revealed a plan to decentralize Twitter’s back-end with a small independent initiative called [Bluesky](#) that will be led by Twitter’s CTO. It makes sense, too. Even if Twitter ultimately become a client of that open standard, some would argue the value of the platform would come from the parent client’s curation vs. the raw firehouse of unfiltered data.

If Facebook’s Libra announcement was a seminal moment in the history of cryptocurrencies, the Bluesky announcement may be of similar magnitude for the [Web 3](#) thesis. A protocol-dominated social media world would permit competing implementations of each protocol, allowing new non-exploitive business models to be tested, switching costs to be slashed, and free speech and privacy to flourish. But you have to believe in the messenger.

In that case, I don’t trust Zuck. I do trust Jack. (If I had to choose one.)

10. Everything else. The layers to the Web 3 stack itself are still evolving, and we haven't even had time to touch on two of the more interesting applications in Web 3, video transcoding (Livepeer) and geospatial mapping (FOAM). Livepeer built the [first video transcoding product](#) on top of its network (via Livepeer, Inc.) and also launched a public testnet for a new, scalable protocol called [Streamflow](#), after raising [\\$8 million](#) in June. FOAM launched a [beta version](#) of its token-curated registry (TCR) to verify user geolocation submissions, which as of April boasted [~140 monthly participants](#), and began testing a [purpose-built scaling solution](#) themselves for accelerating location updates. As projects powered by "work" tokens, FOAM and LPT depend on adoption, but their addressable markets seem small and maybe too early. Who will be the most likely early adopters?

They highlight the thrust of the Web 3 question in general. Are we still five years too early?

Stablecoin Trends

1. Tether (USDT) Let's start in order of historical importance. Tether was one of crypto's early killer apps because it emerged as the reserve currency of crypto to crypto trading and inter-exchange global liquidity. It rose to prominence in an era when most exchanges struggled to maintain banking relationships and process deposits and withdrawals in local currencies. Tether fits my mental model of technically illegal, but not necessarily unethical innovations, and its management has been an exercise in survival via obfuscation.

In spite of the banking issues at partner Bitfinex (recounted earlier), allegations of fraud and inappropriate account commingling with the exchange, and an ongoing cat-and-mouse game securing banking relationships via shell corporations, Tether's market cap *doubled* in the past year, even as more "trustworthy" competitors emerged. It remains the most liquid, stable, and censor-resistant stablecoin in crypto, with a coterie of powerful supporters (the exchanges) whose success today still largely depends on Tether.

It is an order of magnitude larger than its next closest fully-reserved competitor USD Coin (managed by Coinbase and Circle), and 40x larger than MakerDao's crypto-collateralized stablecoin, Dai.

🇺🇸 USD ▼

Stablecoins

all currencies platforms stablecoins exchange tokens dapps

Name	Price	24hr	7 Day Trend	Market cap ▼	Vol 24hr	More
4 Tether	\$1.00	+0.07%		\$4.1B*	\$386M	go pro
25 USD Coin	\$1.00	+0.05%		\$476M*	\$20.1M	go pro
33 Paxos Standar...	\$1.00	+0.07%		\$234M*	\$2.43M	go pro
39 TrueUSD	\$1.00	+0.16%		\$160M*	\$3.23M	go pro
77 Dai	\$0.9975	-0.41%		\$51.6M*	\$29,785	go pro

(Note: "Dai" here refers to single-collateral Dai vs. multi-collateral Dai. More on that below.)
 Source: Messari

Given the rumors that have swirled around Tether's solvency, and the fact the company *had admitted* USDT banking balances were (at least temporarily) under-reserved and secured by non-USD assets at Bitfinex, you'd expect Tether to trade at a discount, as it [did when rumors of insolvency](#) hit their peak in late 2018 and earlier this year.

Alas, it does not currently, and has not usually traded at a discount, but a premium. Magical.



Source: Messari

2. USDC, Paxos, et al. [USD Coin](#) and [Paxos](#) are basically the professional, fully-banked and regulated versions of Tether. Like Tether, USDC and PAX are fully-reserved with U.S. dollars. Unlike Tether they are issued by regulated financial institutions (Circle, Coinbase, and Paxos, primarily) whose deposits are audited monthly by real accounting firms. USDC and PAX are the top current competitors vying to overtake Tether as the dominant liquid reserve for inter-exchange trade settlement. It's unclear that these assets are fungible, given they rely on tight banking relationships, and it would be likely the issuers would attempt to blacklist any assets involved in suspicious or illegal transactions. USDT's weakness may be its lack of reliable banking partners, but its strength is the same: the hydra has proven hard to kill. My bet is that early regulated USD stablecoins exist primarily as medium-term fixes that boost exchange liquidity. They'll end up competing long-term with central bank digital currencies, and look less like "crypto," and more like business as usual with an updated transaction ledger.

3. DAI We covered Dai at length in our DeFi section on MakerDAO, but the asset has truly been a bright spot from the bear market. For those worried about the seizability of USDC, or uncertain reserves in USDT, Dai presents a compelling alternative. Dai survived a major market test in 2018, answering the question, “Can Dai survive a market crash?” when ETH drew down 94%. It hit another major milestone last month when it moved from its single-collateral model (beholden solely to ETH) to a multi-collateral model that could one day open the door to support for thousands of collateral assets. Although competition is fierce and growing in the stablecoin market, I bet both ETH locked in Maker CDPs (currently 2.7mm ETH) as well as circulating Dai (currently just north of \$100mm) doubles in 2020. Has the issuance of ETH collateralized stablecoins destroyed the “ether is money” narrative? The long-term bull thesis for ETH is now “digital collateral for Defi”.

4. Emerging Market Dai. I predict Dai (though don’t write off USDT!) will ultimately be the dominant stablecoin of choice in emerging markets like Latin America, where no one actually wants to hold the local currency. Maker’s Mariano Conti gave an inspiring keynote at DevCon “[How I Survive Argentina’s 50% inflation](#)” that is worth a watch if you want to understand how important a decentralized USD-stablecoin is for emerging market users. (Yes, I know he’s talking his book as a Maker Foundation employee. Just watch the presentation.)

5. Algorithmic Stablecoins We covered fiat-backed stablecoins and collateralized stablecoins above, but there’s a third, under-explored option: algorithmic stablecoins, where the original creator (at least at first) incubates and then gradually decentralizes an algorithmically managed central bank. One mega-hyped algorithmic stablecoin project, Basis, shut down and [returned investor capital last December](#), amidst concerns their dual token structure would run afoul of U.S. regulators. I’m much more bullish on one of their counterparts, Reserve, which is [backed by investors](#) like Peter Thiel, Coinbase, and DCG, and appears to be delivering against its roadmap in anticipation of a full 2020 launch targeting several emerging market economies. (It is already in [beta in Venezuela](#).) Reserve is one of my top projects to watch in 2020.

6. Libra It’s odd to bury the year’s biggest story in the middle of the stablecoin section towards the back of this report, but frankly, that’s where this belongs. The Facebook / Calibra team severely underestimated how unpopular their announcement would be, and their plans to decentralize the project in any real way out of the gates are more or less DOA. All of their meaningful payments partners (Visa, Mastercard, Stripe, PayPal) were scared off by the [strong-arm tactics of Congress](#), and the group that’s left would do well to pare back the initial ambitions of the project.

The Libra team’s opening salvo to run a basket-weighted international reserve is definitively not going to happen in the next several years. Instead, it’s more likely the team starts developing single currency stablecoins for the markets in which it operates. Who knows, perhaps it even gets co-opted by the US government to develop Fedcoin in the event they get spooked by the pace of development of China’s stablecoin (we’ll get to that). That type of coup would be some 4D chess, indeed, but I think Congress hates Zuck enough that that will not happen. I’d trust the Libra team to manage the economic complexity of a new global reserve currency, but not the political complexity of getting it from 0 to 1. Odds are, they’ll end up with a strategy similar to that of Binance.

7. Venus Less than two months after Facebook’s initial announcement around Libra, Binance announced its [Venus initiative](#) to develop *localized* stablecoins and fiat-pegged assets worldwide. (You have to love the troll, too, as Venus is the ruling planet of Libra in astrology.) The individualized approach makes sense for Binance to run in parallel to their more general regulatory conversations, as they seek banking relationships and government blessings across a wide range of jurisdictions. My bet is that we need to see stablecoins pegged to most major world currencies before we see a basket-weighted version successfully come to market. At that point, the basket-weighted alternative could just as easily be a new synthetic instrument built atop the fiat-pegged tokens.

8. Stablecoin Economics Fiat-reserved stablecoins are a funny thing in that if you know you can make a bunch of interest on the deposits, then you may be willing to sometimes sell a dollar for \$0.99...particularly during your bootstrapping period. This is exactly what [Gemini tried last year](#) as they tried to win back some of their plummeting market share from USDC and Paxos. The Gemini dollar looked like it would be competitive for a while, hitting \$95mm in supply in January vs. Paxos’ \$135mm, TrueUSD at \$210mm and USDC’s \$335mm. Their gambit didn’t work, as the trading rebates Gemini offered OTC desks were quickly arbitrated away, and the exchange ultimately couldn’t get over its lack of listing on (and liquidity from) Binance. GUSD is now just a \$4mm stablecoin. It’s functionally dead.



In general, you might expect stablecoins to be priced at a slight discount that reflects catastrophic default risk or uncertain holding periods (in the event of account seizures). The present value of the future implied default risk should end up providing basis points (or full points) or discount, but we haven't seen that yet.

9. DCEP (China) *"As global macro fears return, talk of central bank digital currencies — and their Orwellian surveillance and control — will excite Big Brothers globally. BTC will remain an antidote to financial totalitarianism. CBDCs "replacing bitcoin" will become this cycle's "blockchain not bitcoin" stupid establishment meme."* We wrote this a year ago and it's more relevant than ever, but maybe not entirely correct in light of the pace at which China seems hellbent on building out its "DCEP" (Digital Currency / Electronic Payment).

On October 25th, China made the most important cryptocurrency related [announcement](#) of the year as President Xi Jinping touted blockchain as a revolutionary industry China would invest in heavily. Bitcoin rallied [nearly 40%](#) until everyone realized Xi's comments had nothing to do with crypto currencies, so much as they did with challenging the US Dollar's monetary hegemony, and expanding the country's sphere of regional influence at hyperspeed.

It's been [reported](#) that the PBoC is "expected" to launch the tests of DCEP in Shenzhen and Suzhou with China's "Big Four" commercial banks in early 2020. It's one thing for western nations to ignore *announcements* of China's coming central bank digital currency; it's an entirely different thing for them to ignore the actual *launch*. DCEP could give China the generational opportunity to seize greater control over its monetary system, while still offering neighbors a 10x improvement over the USD in terms of transparency and utility. That vision alone should be scary enough to shake Western leaders out of their anti-crypto stupor and get in the game.

10. Fed / EU Efforts Of course western nations will not stand by and watch this all play out without responding, right? Although there have been no proposals to date for a FED or ECB-backed digital currency, both organizations are [ramping up their research](#) on the possibilities. Fed Chairman Jerome Powell appears lukewarm to the idea, questioning whether a CBDC would offer the same benefits to the US as it would to other nations. (Are we caught in an national monetary innovator's dilemma?) European Bank President Christine Lagarde, on the other hand, appears warmer to the idea, and some [pilot programs are already being planned in France](#). It may be off to the CBDC races everywhere except the U.S.

Policy trends

1. As China/Congress goes, so goes the crypto price. It's wild (though maybe not entirely surprising to me that the "China narrative" still seems to drive so much sentiment within the global crypto markets. Expect more chatter around "bitcoin bans" in China and the U.S. in the years to come, particularly as China rolls out its state-issued digital currency, and the U.S. Congress lumps crypto projects together with its most despised initiative, Libra. States aren't going to cede one of their primary sources of power to these leaderless networks, and they don't necessarily have to "ban" them to severely hinder their progress.

In China, the major miners and exchanges continue to operate at the pleasure and under the watchful eye of the CCP, and there remains serious "stroke of the pen" risk that the party could ban non-state sanctioned currencies outright. In the U.S., it's unlikely that Congress would get its act together any time soon to pass legislation that cripples the industry, but then again they don't need to. The mere Congressional threat of enhanced oversight, led seven major payments partners in the Libra initiative to exit at the 11th hour.

2. Crypto's Single Point of Failure: Banking. The path to crippling crypto's growth in the U.S. without banning it is manifold. Crypto banking is facilitated - more or less - by three small banks: Silvergate, Metropolitan, and Signature, and major regulatory actions against any of those banks would border on an existential threat to the industry. Silvergate, which recently went public on the NYSE, may be the primary bank to watch as they make regular filings with the SEC, serve 750+ crypto firms, and currently custody over \$1.3 billion in crypto customer deposits, roughly 60% of their total deposits. The only other bank that reports on that metric specifically is Metropolitan, who handles less than 20% Silvergate's deposits. Silvergate truly is a crypto-first bank, and the stakes are enormous for them and their customers.

3. Tax Reporting Nightmares Continue It keeps me up at night thinking about the havoc that the IRS could wreak on so many people in the industry personally...not through willful non-compliance with the tax code, but because it's likely the major exchanges are reporting data to the IRS that makes it all but impossible for the agency to reconcile a taxpayers' cost basis and portfolio details with those of the multiple services the taxpayer may have used.

If you were early in the industry, you knew better than to keep all your assets on one exchange or wallet. But if the IRS sees an outflow from Coinbase and doesn't realize that transaction was a like-kind transfer to Poloniex, and the auditors assume instead it was actually a sale vs. a transfer, it's going to be a nightmarish process to comb through all the old records. Many people are going to get audited and penalized unfairly because of how early they were and because of the immaturity of the tax reporting infrastructure.

Beyond that, the IRS's most recent guidance on forks and airdrops is insane, and it will severely hurt users depending on how and whether the major custodial wallets and exchanges share that information in the first place. It must be nice to live in [Germany](#), where there are no capital gains taxes for crypto held longer than one year, or [France](#), where crypto-crypto transactions are not taxed at all. While poor tax law could prove to be a weapon for countries that wish to strangle crypto, I'd expect favorable environments to continue to attract more capital in the years ahead.

4. IRS Auditing Nightmare Begins If reporting is a nuisance, then audits and fraud nightmares are just about to begin. It will likely start with those who failed to comply with the IRS's strictest warning letters this past summer regarding potential penalties for non-compliance, and I am 90% confident we'll see at least one high-profile tax evasion case of a high-profile early adopter in 2020. The IRS will go with the lowest hanging fruit (true fraud), then work their way to more advanced cases as they begin to rack up legal wins and important precedents.

The first batch of targets will date back to the subpoena of Coinbase [and the 13,000 customer records they turned over in 2018](#). But you can rest assured that records of anyone and everyone who has traded on Coinbase, Poloniex, Kraken, Gemini, and Bittrex in the U.S. since then are now in the hands of the IRS. The next shoes to drop in 2021+ will be in cases where customers failed to report crypto-crypto trades, inappropriately flagged them as "like kind", or failed to account for [forks and airdrops](#). Short of a safe harbor provision for crypto investors who transacted before a certain date (or an act of Congress), these cases will linger for many, many years. And it gets worse!

The truly scary new development lies in what we know the IRS is already pursuing, and the fact that the IRS has three years after a return's due date to assess a deficiency, but *six years if income is understated by more than 25%*. That means you can expect enforcement against beneficiaries of the 2013 Coinbase bubble by October of this year, and enforcements against 2017 Poloniex/Bittrex token flippers and shitcoin traders as late as 2023.

Like I said, just getting started.

5. The war on privacy. Oh, wait you thought that last section was bad? No no no. It gets worse still, if you think about this in the context of privacy, and "un-confiscatable" wealth. The IRS for one has added this loaded question to its tax questionnaire for 2019: "At any time during 2019, did you receive, sell, send, exchange, or otherwise acquire any financial interest in any virtual currency?" The only folks who can answer "no" here are those with zero crypto exposure or holders with zero transactions.

That's one step closer to putting crypto - the "Swiss bank account in your pocket" - in FBAR territory, Report of Foreign Bank and Financial Accounts. That is, the tax authorities will at some point in the future demand that even holders disclose their wallet addresses if they contain more than \$10k in aggregate value held in a financial account "located outside of the U.S." Outside the U.S. doesn't really apply to crypto, though. It's fuzzy, and I'm certain that by 2025 (if not sooner), barring successful legal victories that invoke the 4th and 5th amendments, the FBAR reporting requirements will expand to include crypto. A dangerous and Orwellian path indeed that would put bitcoin and crypto-currencies functionally equivalent to state-issued digital currencies.

The good news is that this isn't just crypto's fight anymore. Big tech companies are also pushing back against unreasonable requirements that the authorities provision "[backdoor access](#)" to systems that could then be similarly exploited by criminals, hackers and repressive regimes. Security holes don't discriminate between who is a good guy vs. a bad guy, and crypto vulnerabilities in particular could cause literal life and death security threats in the coming years. I'd put the IRS request for information on crypto purchases as one of those security "back doors", though it only really becomes an issue if and when the government ever puts crypto addresses in their FBAR bucket.

6 SEC Enforcements Who's afraid of the big bad wolf? Just hire some expensive lawyers! Here's what I expect to take place in 2020 as the SEC continues to grapple with the glut of 2017 token sales they believe look like unregistered securities offerings.

- The SEC may be drawing a clear line between their pre- and post- DAO report enforcement actions. If you expect leniency for teams that completed token sales prior to July 25, 2017, then Cosmos, Basic Attention Token, and Tezos are in relatively good negotiating position when it comes to top 30 projects with U.S. teams.
- If the SEC was willing to settle for a mere \$24 million with Block.One over their year long \$4 billion EOS crowdsale, then I don't think we should expect to see a case against Ripple, whose advisory ranks are best in the industry (ex-regulators Mary Jo White (SEC), Ben Lawsky (NYDFS), Gene Sperling (White House) are advisors or directors).
- If we expect the SEC to take a "do no harm" approach to public, liquid tokens that have performed well despite the bear market beatings, then Chainlink and Maker should really be in the clear as well.
- Most of the other enforcement actions I'd expect are with egregious violations of the securities law or outright fraud. If the SEC is going to give people a hard time, it's likely going to be with those who completed SAFT mega-rounds in the 6-9 months following the DAO report, but who have yet to come to market. (Telegram, Filecoin, PolkaDot?)

7. ETF Proposals It seems as though pretty much every country aside from the U.S. will have a Bitcoin ETF/ETP by the end of 2020. The most important developments of the year on the ETP front have happened in the past month. First with Canadian asset manager 3iQ's approval from the Ontario Securities Commission to [offer an exchange-traded Bitcoin fund on the TSX](#), a move that could nudge the SEC in the direction of approving a U.S. ETF. Then with WisdomTree's sponsorship of a European Bitcoin ETP in Switzerland [on their SIX exchange](#).

New York Digital Investment Group (NYDIG) recently received [approval by the SEC to offer a closed-end mutual fund](#) that trades cash-settled Bitcoin futures, and Galaxy recently joined the mix of asset managers offering competitive [investment vehicles for accredited investors](#).

Still, the SEC doesn't look like it's budging in the election year, at least if you take Blockchain Association ED Kristin Smith at her word. She says Jay Clayton [has to go](#) before there is any movement on the bitcoin ETF. I still don't understand how the SEC can allow Grayscale's products to trade (with their ~30% premiums), and not go ahead and bless the damn ETF. It's embarrassing. Bitcoin's markets are at least as transparent as the commodities markets, with much tighter spreads, and arguably less price manipulation.

8. Stablecoins as Securities? If this section in particular feels very U.S. centric, it's because a) we live and work in New York, and b) there's a lot to unpack with respect to how ass-backwards U.S. crypto policy is. Take a recent stablecoin bill that was introduced in Congress, ostensibly aimed at directly impeding Libra's progress, which aims to classify as a security any stablecoin with "an issuer who plays an active managerial role in adjusting the composition of assets that back the coin and guarantee its stability." The bill is expected to be reintroduced during the new session of Congress. Coin Center has already [highlighted concerns](#) the overly broad language could lead to USD-pegged stablecoins being classified as a security. If you want to cripple the industry, you don't need to ban it, you just need to make abusive tax and securities laws that are impossible to comply with.

9. Regulatory Competition The world's largest crypto exchange is currently domiciled in Malta after operating without a real headquarters for stretches of time in 2017 and 2018. Most of the world's largest crypto businesses are based in Asia, but non technically Asia. Many New York crypto businesses are technically in New Jersey. Many of the wealthiest U.S. crypto investors live in Puerto Rico, but don't really live in Puerto Rico. It's all part of the ongoing game of regulatory arbitrage that may only get more prevalent depending on who gets elected in your next regional or national elections.

Let's hope more countries in Europe take France and Switzerland's relatively friendly stance towards crypto, and let's hope more U.S. state regulators follow [Wyoming's lead](#), which has laid the groundwork for a crypto-friendly state regime, and whose model is starting to gain pick up in neighboring states like Colorado.

(Note: Now that I am writing this last section, just minutes away from publishing, I'm kicking myself for excluding Caitlin Long, the real driving force behind the Wyoming legislation, from our top 10 people to watch list. You should [follow her](#).)

10. Common Sense If you couldn't tell from the above, I'm not an uber-bull on our regulators and government leaders. But I do believe in crypto, and common sense, and maintaining the moral high ground and acting beyond reproach when it comes to building the infrastructure for a more open and efficient financial system. We'll continue pushing for common sense disclosures norms for projects, standardized data from exchanges, and ethical design of these new protocols. If you'd like to support us, drop us a line at research@messari.io.

Top 10 Re-Readings To Get You Fired Up for the Decade Ahead

- 1. Defiance Podcast:** [Andreas Antonopoulos](#) <> Peter McCormack Even though we've bounced off the bear market lows of late 2018, this year has felt like a slog at times. So I recommend this chat with Andreas Antonopoulos on the Defiance podcast, as he continues to be the clearest and most inspiring teacher in crypto. "Money is the language by which society not only coordinates but also expresses value."
- 2. Nic Carter:** [A Most Peaceful Revolution](#) A rallying cry for the battles ahead as bitcoin crosses the chasm to mainstream relevance, and we grapple with some hard questions as an industry, including "are we all activists?"
- 3. CZ:** [ICO's Not Just Good to Have, But Necessary](#) If you want to have the bull case for ICOs, then here it is. There's tremendous clarity of thought here, and I'd argue CZ was one of the few entrepreneurs who had a clear vision for how a token for his company would accrue value. Binance may be to tokens what Amazon was to e-commerce. CZ found his "online book store" wedge in offering a token that eliminated trading fees for early users, and built from there.
- 4. Naval:** ["Blockchains will replace networks with markets."](#) "The 20th century created a new kind of network - market networks. Open AND meritocratic....Blockchains are a new invention that allows meritorious participants in an open network to govern without a ruler and without money." Just go read the full thread.
- 5. a16z:** [Crypto Cannon](#) This is the deepest curated collection of insights I've come across. It's information overload, perhaps, but if you were going to start a crypto curriculum, you'd likely want to build off of this skeleton.
- 6. r/bitcoin:** ["I'm a time traveler from the future, here to beg you to stop."](#) God, this keeps getting better and scarier every year that goes by. We're laughing about the dystopian future we're approaching so that we don't cry.
- 7. Charlie Munger's** [Mental Models for "Human Misjudgment"](#) I wrote up a dozen or so of the best "Mungerisms" from this interview in my original 95 theses. They are gold, and it's worth reading the insights from one of the best investors of all time, as you think about tackling the wild world of crypto.
- 8. Paul Graham:** [Lessons](#) There may be a recency bias here, but this struck a chord with a lot of people, me included this month. Graham writes about unlearning the lesson "get good grades in school" as a precursor to unlearning how to optimize for winning other silly and nonsensical games in the real world. This gets to the root cause of many of society's structural problems.

9. Tim Urban: [Your Life in Weeks](#) & [The Tail End](#) Tim is in my pantheon of writers I admire most, along with Stephen King, and Matt Levine. (It's good to have eclectic tastes.) These posts are on my annual holiday reading list as I mentally prepare for the year ahead. Life is short. Work on meaningful things with good people you like spending time with. Or get a new job.

10. Satoshi Nakamoto: [Bitcoin: A Peer-to-Peer Electronic Cash System](#) Show some respect, dammit. I re-read this regularly when I need a reminder that I can - if I try to - write about this highly complex industry in clear and non-jargony language. And I always pick up something new, like the fact that the "blockchain" was really just referenced as a "timestamp server", which is fascinating in and of itself.

That's it. I'm never writing again. (Until 2020.) Thanks for reading, and Happy Holidays!

-TBI & the Messari team