What in the Ethereum application ecosystem excites me

2022 Dec 05 See all posts

Special thanks to Matt Huang, Santi Siri and Tina Zhen for feedback and review

Ten, five, or even two years ago, my opinions on what Ethereum and blockchains can do for the world were very abstract. "This is a general-purpose technology, like C++", I would say; of course, it has specific properties like decentralization, openness and censorship resistance, but beyond that it's just too early to say which specific applications are going to make the most sense.

Today's world is no longer that world. Today, enough time has passed that there are few ideas that are completely unexplored: if something succeeds, it will *probably* be some version of something that has already been discussed in blogs and forums and conferences on multiple occasions. We've also come closer to identifying fundamental limits of the space. Many DAOs have had a fair chance with an enthusiastic audience willing to participate in them despite the inconveniences and fees, and many have underperformed. Industrial supply-chain applications have not gone anywhere. Decentralized Amazon on the blockchain has not happened. But it's also a world where we have seen genuine and growing adoption of a few key applications that are meeting people's real needs - and those are the applications that we need to focus on.

Hence my change in perspective: my excitement about Ethereum is now no longer based in the potential for undiscovered unknowns, but rather in a few specific categories of applications that are proving themselves already, and are only getting stronger. What are these applications, and which applications am I no longer optimistic about? That is what this post will be about.

1. Money: the first and still most important app

When I first visited Argentina in December last year, one of the experiences I remember well was walking around on Christmas Day, when almost everything is closed, looking for a coffee shop. After passing by about five closed ones, we finally found one that was open. When we walked in, the owner recognized me, and immediately showed me that he has ETH and other crypto-assets on his Binance account. We ordered tea and snacks, and we asked if we could pay in ETH. The coffee shop owner obliged, and showed me the QR code for his Binance deposit address, to which I sent about $20 of ETH from my Status wallet on my phone.

This was far from the most meaningful use of cryptocurrency that is taking place in the country. Others are using it to save money, transfer money internationally, make payments for large and important transactions, and much more. But even still, the fact that I randomly found a coffee shop and it happened to accept cryptocurrency showed the sheer reach of adoption. Unlike wealthy countries like the United States, where financial transactions are easy to make and 8% inflation is considered extreme, in Argentina and many other countries around the world, links to global financial systems are more limited and extreme inflation is a reality every day. Cryptocurrency often steps in as a lifeline.

In addition to Binance, there is also an increasing number of local exchanges, and you can see advertisements for them everywhere including at airports.

The one issue with my coffee transaction is that it did not really make pragmatic sense. The fee was high, about a third of the value of the transaction. The transaction took several minutes to confirm: I believe that at the time, Status did not yet support sending proper EIP-1559 transactions that more reliably confirm quickly. If, like many other Argentinian crypto users, I had simply had a Binance wallet, the transfer would have been free and instant.

A year later, however, the calculus is different. As a side effect of the Merge, transactions get included significantly more quickly and the chain has become more stable, making it safer to accept transactions after fewer confirmations. Scaling technology such as optimistic and ZK rollups is proceeding quickly. Social recovery and multisig wallets are becoming more practical with account abstraction. These trends will take years to play out as the technology develops, but progress is already being made. At the same time, **there is an important "push factor" driving interest in transacting on-chain: the FTX collapse**, which has reminded everyone, Latin Americans included, that even the most trustworthy-seeming centralized services may not be trustworthy after all.

Cryptocurrency in wealthy countries

In wealthy countries, the more extreme use cases around surviving high inflation and doing basic financial activities at all usually do not apply. But cryptocurrency still has significant value. As someone who has used it to make donations (to quite normal organizations in many countries), I can personally confirm that it is *far* more convenient than traditional banking. It's also valuable for industries and activities at risk of being deplatformed by payment processors - a category which includes many industries that are perfectly legal under most countries' laws.

There is also the important broader philosophical case for cryptocurrency as private money: the transition to a "cashless society" is being taken advantage of by many governments as an opportunity to introduce levels of financial surveillance that would be unimaginable 100 years ago. **Cryptocurrency is the *only* thing currently being developed that can realistically combine the benefits of digitalization with cash-like respect for personal privacy**.

But in either case, cryptocurrency is far from perfect. Even with all the technical, user experience and account safety problems solved, it remains a fact that cryptocurrency is volatile, and the volatility can make it difficult to use for savings and business. For that reason, we have...

Stablecoins

The value of stablecoins has been understood in the Ethereum community for a long time. Quoting a blog post from 2014:

> Over the past eleven months, Bitcoin holders have lost about 67% of their wealth and quite often the price moves up or down by as much as 25% in a single week. Seeing this concern, there is a growing interest in a simple question: can we get the best of both worlds? Can we have the full decentralization that a cryptographic payment network offers, but at the same time have a higher level of price stability, without such extreme upward and downward swings?

And indeed, stablecoins are very popular among precisely those users who are making pragmatic use of cryptocurrency today. That said, there is a reality that is not congenial to cypherpunk values today: the stablecoins that are most successful today are the centralized ones, mostly USDC, USDT and BUSD.

#	Coin	Price	1h	24h	7d	Mkt Cap
☆ 1	Bitcoin BTC	$16,906.10	1.0%	3.5%	4.7%	$324,950,635,810
☆ 2	Ethereum ETH	$1,280.66	1.2%	5.9%	12.8%	$154,281,907,530
☆ 3	Tether USDT	$1.01	0.7%	0.5%	0.7%	$65,891,847,384
☆ 4	BNB BNB	$299.04	1.3%	1.2%	12.3%	$48,841,350,953
☆ 5	USD Coin USDC	$1.00	0.4%	0.2%	0.4%	$43,475,130,147
☆ 6	Binance USD BUSD	$1.01	0.7%	0.4%	0.5%	$22,395,277,875

Top cryptocurrency market caps, data from CoinGecko, 2022-11-30. Three of the top six are centralized stablecoins.

Stablecoins issued on-chain have many convenient properties: they are open for use by anyone, they are resistant to the most large-scale and opaque forms of censorship (the issuer *can* blacklist and freeze addresses, but such blacklisting is transparent, and there are literal transaction fee costs associated with freezing each address), and they interact well with on-chain infrastructure (accounts, DEXes, etc). But it's not clear how long this state of affairs will last, and so there is a need to keep working on other alternatives.

I see the stablecoin design space as basically being split into three different categories: **centralized stablecoins**, **DAO-governed real-world-asset backed stablecoins** and **governance-minimized crypto-backed stablecoins**.

	Governance	Advantages	Disadvantages	Examples
Centralized stablecoins	Traditional legal entity	• Maximum efficiency • Easy to understand	Vulnerable to risks of a single issuer and a single jurisdiction	USDC, USDT, BUSD
DAO-governed RWA-backed stablecoins	DAO deciding on allowed collateral types and maximum per type	• Adds resilience by diversifying issuers and jurisdictions • Still somewhat capital efficient	Vulnerable to repeated issuer fraud or coordinated takedown	DAI
Governance-minimized crypto-backed stablecoin	Price oracle only	• Maximum resilience • No outside dependencies	• High collateral requirements • Limited scale • Sometimes needs negative interest rates	RAI, LUSD

From the user's perspective, the three types are arranged on a tradeoff spectrum between efficiency and resilience. USDC works today, and will almost certainly work tomorrow. But in the longer term, its ongoing stability depends on the macroeconomic and political stability of the United States, a continued US regulatory environment that supports making USDC available to everyone, and the trustworthiness of the issuing organization.

RAI, on the other hand, can survive all of these risks, but it has a negative interest rate: at the time of this writing, -6.7%. To make the system stable (so, not be vulnerable to collapse like LUNA), every holder of RAI must be matched by a holder of negative RAI (aka. a "borrower" or "CDP holder") who puts in ETH as collateral. This rate could be improved with more people engaging in arbitrage, holding negative RAI and balancing it out with positive USDC or even interest-bearing bank account deposits, but interest rates on RAI will always be lower than in a functioning banking system, and the possibility of negative rates, and the user experience headaches that they imply, will always be there.

The RAI model is ultimately ideal for the more pessimistic lunarpunk world: it avoids all connection to non-crypto financial systems, making it much more difficult to attack. Negative interest rates prevent it from being a convenient proxy for the dollar, but one way to adapt would be to embrace the disconnection: **a governance-minimized stablecoin could track some non-currency asset like a global average CPI index, and advertise itself as representing abstract "best-effort price stability"**. This would also have lower inherent regulatory risk, as such an asset would not be attempting to provide a "digital dollar" (or euro, or...).

DAO-governed RWA-backed stablecoins, if they can be made to work well, could be a happy medium. Such stablecoins could combine enough robustness, censorship resistance, scale and economic practicality to satisfy the needs of a large number of real-world crypto users. But making this work requires both real-world legal work to develop robust issuers, *and* a healthy dose of resilience-oriented DAO governance engineering.

In either case, *any* kind of stablecoin working well would be a boon for many kinds of currency and savings applications that are already concretely useful for millions of people today.

2. Defi: keep it simple

Decentralized finance is, in my view, a category that started off honorable but limited, turned into somewhat of an overcapitalized monster that relied on unsustainable forms of yield farming, and is now in the early stages of setting down into a stable medium, improving security and refocusing on a few applications that are particularly valuable. Decentralized stablecoins are, and probably forever will be, the most important defi product, but there are a few others that have an important niche:

- **Prediction markets**: these have been a niche but stable pillar of decentralized finance since the launch of Augur in 2015. Since then, they have quietly been growing in adoption. Prediction markets showed their value and their limitations in the 2020 US election, and this year in 2022, both crypto prediction markets like Polymarket and play-money markets like Metaculus are becoming more and more widely used. Prediction markets are valuable as an epistemic tool, and there is a genuine benefit from using cryptocurrency in making these markets more trustworthy and more globally accessible. I expect prediction markets to not make extreme multibillion-dollar splashes, but continue to steadily grow and become more useful over time.
- **Other synthetic assets**: the formula behind stablecoins can in principle be replicated to other real-world assets. Interesting natural candidates include major stock indices and real estate. The latter will take longer to get right due to the inherent heterogeneity and complexity of the space, but it could be valuable for precisely the same reasons. The main question is whether or not someone can create the right balance of decentralization and efficiency that gives users access to these assets at reasonable rates of return.
- **Glue layers for efficiently trading between other assets**: if there are assets on-chain that people want to use, including ETH, centralized or decentralized stablecoins, more advanced synthetic assets, or whatever else, there will be value in a layer that makes it easy for users to trade between them. Some users may want to hold USDC and pay transaction fees in USDC. Others may hold some assets, but want to be able to instantly convert to pay someone who wants to be paid in another asset. There is also space for using one asset as collateral to take out loans of another asset, though such projects are most likely to succeed and avoid leading to tears if they keep leverage *very* limited (eg. not more than 2x).

3. The identity ecosystem: ENS, SIWE, PoH, POAPs, SBTs

"Identity" is a complicated concept that can mean many things. Some examples include:

- **Basic authentication**: simply proving that action A (eg. sending a transaction or logging into a website) was authorized by some agent that has some identifier, such as an ETH address or a public key, without attempting to say anything else about who or what the agent is.
- **Attestations**: proving claims about an agent made by other agents ("Bob attests that he knows Alice", "the government of Canada attests that Charlie is a citizen")
- **Names**: establishing consensus that a particular human-readable name can be used to refer to a particular agent.
- **Proof of personhood**: proving that an agent is human, and guaranteeing that each human can only obtain one identity through the proof of personhood system (this is often done with attestations, so it's not an entirely separate category, but it's a hugely important special case)

For a long time, I have been bullish on *blockchain identity* but bearish on *blockchain identity platforms*. The use cases mentioned above are really important to many blockchain use cases, and blockchains are valuable for identity applications because of their institution-independent nature and the interoperability benefits that they provide. But what will not work is an attempt to create a centralized platform to achieve all of these tasks from scratch. What more likely will work is an organic approach, with many projects working on specific tasks that are individually valuable, and adding more and more interoperability over time.

And this is exactly what has happened since then. The Sign In With Ethereum (SIWE) standard allows users to log into (traditional) websites in much the same way that you can use Google or Facebook accounts to log into websites today. This is actually useful: it allows you to interact with a site without giving Google or Facebook access to your private information or the ability to take over or lock you out of your account. Techniques like social recovery could give users account recovery options in case they forget their password that are *much better* than what centralized corporations offer today. SIWE is supported by many applications today, including Blockscan chat, the end-to-end-encrypted email and notes service Skiff, and various blockchain-based alternative social media projects.

ENS lets users have usernames: I have `vitalik.eth`. Proof of Humanity and other proof-of-personhood systems let users prove that they are unique humans, which is useful in many applications including airdrops and governance. POAP (the "proof of attendance protocol", pronounced either "pope" or "poe-app" depending on whether you're a brave contrarian or a sheep) is a general-purpose protocol for issuing tokens that represent attestations: have you completed an educational course? Have you attended an event? Have you met a particular person? POAPs could be used both as an ingredient in a proof-of-personhood protocol and as a way to try to determine whether or not someone is a member of a particular community (valuable for governance or airdrops).

An NFC card that contains my ENS name, and allows you to receive a POAP verifying that you've met me. I'm not sure I **want** to create any further incentive for people to bug me really hard to get my POAP, but this seems fun and useful for other people.

Each of these applications are useful individually. But what makes them truly powerful is how well they compose with each other. When I log on to Blockscan chat, I sign in with Ethereum. This means that I am immediately visible as `vitalik.eth` (my ENS name) to anyone I chat with. In the future, to fight spam, Blockscan chat could "verify" accounts by looking at on-chain activity or POAPs. The lowest tier would simply be to verify that the account has sent or been the recipient in at least one on-chain transaction (as that requires paying fees). A higher level of verification could involve checking for balances of specific tokens, ownership of specific POAPs, a proof-of-personhood profile, or a meta-aggregator like Gitcoin Passport.

The network effects of these different services combine to create an ecosystem that provides some very powerful options for users and applications. An Ethereum-based Twitter alternative (eg. Farcaster) could use POAPs and other proofs of on-chain activity to create a "verification" feature that does not require conventional KYC, allowing anons to participate. Such platforms could create rooms that are gated to members of a particular community - or hybrid approaches where only community members can speak but anyone can listen. The equivalent of Twitter polls could be limited to particular communities.

Equally importantly, there are much more pedestrian applications that are relevant to simply helping people make a living: verification through attestations can make it easier for people to prove that they are trustworthy to get rent, employment or loans.

The big future challenge for this ecosystem is privacy. The status quo involves putting large amounts of information on-chain, which is something that is "fine until it's not", and eventually will become unpalatable if not outright risky to more and more people. There are ways to solve this problem by combining on-chain and off-chain information and making heavy use of ZK-SNARKs, but this is something that will actually need to be worked on; projects like Sismo and HeyAnon are an early start. Scaling is also a challenge, but scaling can be solved generically with rollups and perhaps validiums. Privacy cannot, and must be worked on intentionally for each application.

4. DAOs

"DAO" is a powerful term that captures many of the hopes and dreams that people have put into the crypto space to build more democratic, resilient and efficient forms of governance. It's also an incredibly broad term whose meaning has evolved a lot over the years. Most generally, a DAO is a smart contract that is meant to represent a structure of ownership or control over some asset or process. But this structure could be anything, from the lowly multisig to highly sophisticated multi-chamber governance mechanisms like those proposed for the Optimism Collective. Many of these structures work, and many others cannot, or at least are very mismatched to the goals that they are trying to achieve.

There are two questions to answer:

1. What kinds of governance structures make sense, and for what use cases?
2. Does it make sense to implement those structures as a DAO, or through regular incorporation and legal contracts?

A particular subtlety is that the word "decentralized" is sometimes used to refer to both: a *governance structure* is decentralized if its decisions depend on decisions taken from a large group of participants, and an *implementation* of a governance structure is decentralized if it is built on a decentralized structure like a blockchain and is not dependent on any single nation-state legal system.

Decentralization for robustness

One way to think about the distinction is: **decentralized governance structure protects against attackers on the inside, and a decentralized implementation protects against powerful attackers on the outside ("censorship resistance")**.

First, some examples:

	Higher need for protection from inside	Lower need for protection from inside
Higher need for protection from outside	Stablecoins	The Pirate Bay, Sci-Hub
Lower need for protection from outside	Regulated financial institutions	Regular businesses

The Pirate Bay and Sci-Hub are important case studies of something that is censorship-resistant, but does not need decentralization. Sci-Hub is largely run by one person, and if some part of Sci-Hub infrastructure gets taken down, she can simply move it somewhere else. The Sci-Hub URL has changed many times over the years. The Pirate Bay is a hybrid: it relies on BitTorrent, which *is* decentralized, but the Pirate Bay itself is a centralized convenience layer on top.

The difference between these two examples and blockchain projects is that they do not attempt to protect their users against the platform itself. If Sci-Hub or The Pirate Bay wanted to harm their users, the worst they could do is either serve bad results or shut down - either of which would only cause minor inconvenience until their users switch to other alternatives that would inevitably pop up in their absence. They could also publish user IP addresses, but even if they did that the total harm to users would still be much lower than, say, stealing all the users' funds.

Stablecoins are *not* like this. Stablecoins are trying to create stable credibly neutral global commercial infrastructure, and this demands both lack of dependence on a single centralized actor on the outside *and* protection against attackers from the inside. If a stablecoin's governance is poorly designed, an attack on the governance could steal billions of dollars from users.

At the time of this writing, MakerDAO has $7.8 billion in collateral, over 17x the market cap of the profit-taking token, MKR. Hence, if governance was up to MKR holders with no safeguards, someone could buy up half the MKR, use that to manipulate the price oracles, and steal a large portion of the collateral for themselves. In fact, this actually happened with a smaller stablecoin! It hasn't happened to MKR yet largely because the MKR holdings are still fairly concentrated, with the majority of the MKR held by a fairly small group that would not be willing to sell because they believe in the project. This is a fine model to get a stablecoin started, but not a good one for the long term. Hence, making decentralized stablecoins work long term requires innovating in decentralized governance that does not have these kinds of flaws.

Two possible directions include:

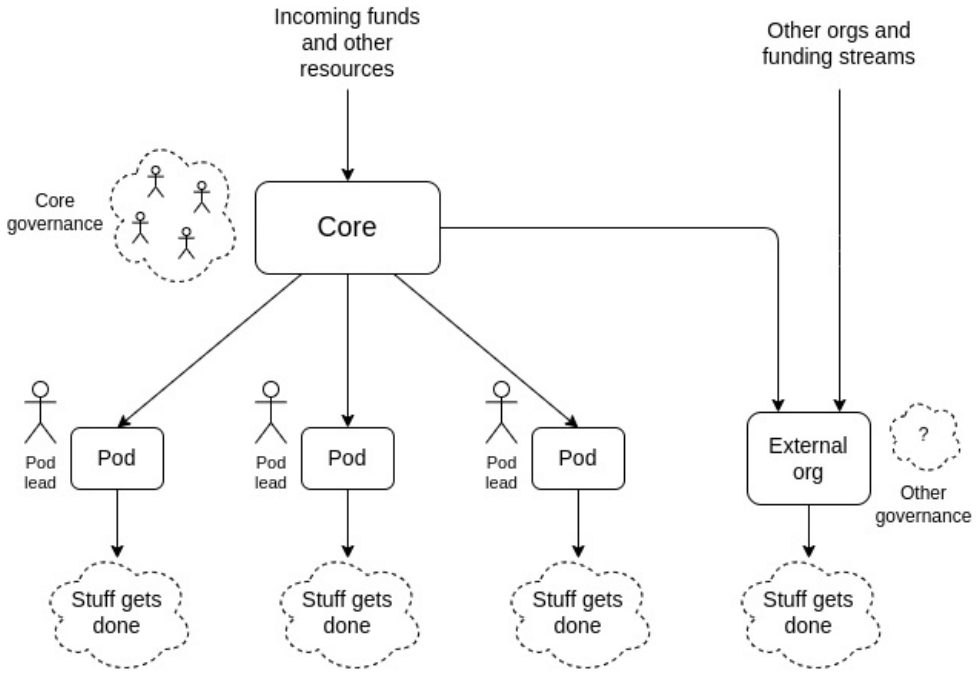
- Some kind of non-financialized governance, or perhaps a bicameral hybrid where decisions need to be passed not just by token holders but also by some other class of user (eg. the Optimism Citizens' House or stETH holders as in the Lido two-chamber proposal)
- Intentional friction, making it so that certain kinds of decisions can only take effect after a delay long enough that users can see that something is going wrong and escape the system.

There are many subtleties in making governance that effectively optimizes for robustness. If the system's robustness depends on pathways that are only activated in extreme edge cases, the system may even want to intentionally test those pathways once in a while to make sure that they work - much like the once-every-20-years rebuilding of Ise Jingu. This aspect of decentralization for robustness continues to require more careful thought and development.

Decentralization for efficiency

Decentralization for efficiency is a different school of thought: **decentralized governance structure is valuable because it can incorporate opinions from more diverse voices at different scales, and decentralized implementation is valuable because it can sometimes be more efficient and lower cost than traditional legal-system-based approaches**.

This implies a different *style* of decentralization. Governance decentralized for robustness emphasizes having a large number of decision-makers to ensure *alignment* with a pre-set goal, and *intentionally makes pivoting more difficult*. Governance decentralized for efficiency preserves the ability to act rapidly and pivot if needed, but tries to move decisions away from the top to avoid the organization becoming a sclerotic bureaucracy.



Pod-based governance in Ukraine DAO. This style of governance improves efficiency by maximizing autonomy.

Decentralized implementations designed for robustness and decentralized implementations designed for efficiency are in one way similar: they both just involve putting assets into smart contracts. But decentralized implementations designed for efficiency are going to be much simpler: just a basic multisig will generally suffice.

It's worth noting that "decentralizing for efficiency" is a weak argument for large-scale projects in the same wealthy country. But it's a stronger argument for very-small-scale projects, highly internationalized projects, and projects located in countries with inefficient institutions and weak rule of law. Many applications of "decentralizing for efficiency" probably *could* also be done on a central-bank-run chain run by a stable large country; I suspect that both decentralized approaches and centralized approaches are good enough, and it's the path-dependent question of which one becomes viable first that will determine which approach dominates.

Decentralization for interoperability

This is a fairly boring class of reasons to decentralize, but it's still important: **it's easier and more secure for on-chain things to interact with other on-chain things, than with off-chain systems that would inevitably require an (attackable) bridge layer**.

If a large organization running on direct democracy holds 10,000 ETH in its reserves, that would be a decentralized governance decision, but it would not be a decentralized implementation: in practice, that country would have a few people managing the keys and that storage system could get attacked.

There is also a governance angle to this: if a system provides services to *other* DAOs that are not capable of rapid change, it is better for that system to itself be incapable of rapid change, to avoid "rigidity mismatch" where a system's dependencies break and that system's rigidity renders it unable to adapt to the break.

These three "theories of decentralization" can be put into a chart as follows:

	Why decentralize governance structure	**Why decentralize implementation**
Decentralization for robustness	Defense against inside threats (eg. SBF)	Defense against outside threats, and censorship resistance
Decentralization for efficiency	Greater efficiency from accepting input from more voices and giving room for	Smart contracts often more convenient than legal systems

	autonomy	
Decentralization for interoperability	To be rigid enough to be safe to use by other rigid systems	To more easily interact with other decentralized things

Decentralization and fancy new governance mechanisms

Over the last few decades, we've seen the development of a number of fancy new governance mechanisms:

- Quadratic voting
- Futarchy
- Liquid democracy
- Decentralized *conversation* tools like Pol.is

These ideas are an important part of the DAO story, and they can be valuable for both robustness *and* efficiency. The case for quadratic voting relies on a mathematical argument that it makes the exactly correct tradeoff between giving space for stronger preferences to outcompete weaker but more popular preferences and not weighting stronger preferences (or wealthy actors) *too much*. But people who have used it have found that it can improve robustness too. Newer ideas, like pairwise matching, *intentionally* sacrifice mathematically provable optimality for robustness in situations where the mathematical model's assumptions break.

These ideas, in addition to more "traditional" centuries-old ideas around multicameral architectures and intentional indirection and delays, are going to be an important part of the story in making DAOs more effective, though they will also find value in improving the efficiency of traditional organizations.

Case study: Gitcoin Grants

We can analyze the different styles of decentralization through an interesting edge-case: Gitcoin Grants. Should Gitcoin Grants be an on-chain DAO, or should it just be a centralized org?

Here are some possible arguments for Gitcoin Grants to be a DAO:

- It holds and deals with cryptocurrency, because most of its users and funders are Ethereum users
- Secure quadratic funding is best done on-chain (see next section on blockchain voting, and implementation of on-chain QF here), so you reduce security risks if the result of the vote feeds into the system directly
- It deals with communities all around the world, and so benefits from being credibly neutral and not centered around a single country.
- It benefits from being able to give its users confidence that it will still be around in five years, so that public goods funders can start projects now and hope to be rewarded later.

These arguments lean toward decentralization for robustness and decentralization for interoperability of the superstructure, though the individual quadratic funding rounds are more in the "decentralization for efficiency" school of thought (the theory behind Gitcoin Grants is that quadratic funding is a more efficient way to fund public goods).

If the robustness and interoperability arguments did *not* apply, then it probably would have been better to simply run Gitcoin Grants as a regular company. But they do apply, and so Gitcoin Grants being a DAO makes sense.

There are plenty of other examples of this kind of argument applying, both for DAOs that people increasingly rely on for their day-to-day lives, and for "meta-DAOs" that provide services to *other* DAOs:

- Proof of humanity
- Kleros
- Chainlink
- Stablecoins
- Blockchain layer 2 protocol governance

I don't know enough about all of these systems to testify that they all *do* optimize for decentralization-for-robustness enough to satisfy my standards, but hopefully it should be obvious by

now that they *should*.

The main thing that *does not* work well are DAOs that require pivoting ability that is in conflict with robustness, and that do not have a sufficient case to "decentralize for efficiency". Large-scale companies that mainly interface with US users would be one example. When making a DAO, the first thing is to determine whether or not it is worth it to structure the project as a DAO, and the second thing is to determine whether it's targeting robustness or efficiency: if the former, deep thought into governance *design* is also required, and if the latter, then either it's innovating on governance via mechanisms like quadratic funding, or it should just be a multisig.

5. Hybrid applications

There are many applications that are not entirely on-chain, but that take advantage of both blockchains and other systems to improve their trust models.

Voting is an excellent example. High assurances of censorship resistance, auditability and privacy are all required, and systems like MACI effectively combine blockchains, ZK-SNARKs and a limited centralized (or M-of-N) layer for scalability and coercion resistance to achieve all of these guarantees. Votes are published to the blockchain, so users have a way independent of the voting system to ensure that their votes get included. But votes are encrypted, preserving privacy, and a ZK-SNARK-based solution is used to ensure that the final result is the correct computation of the votes.

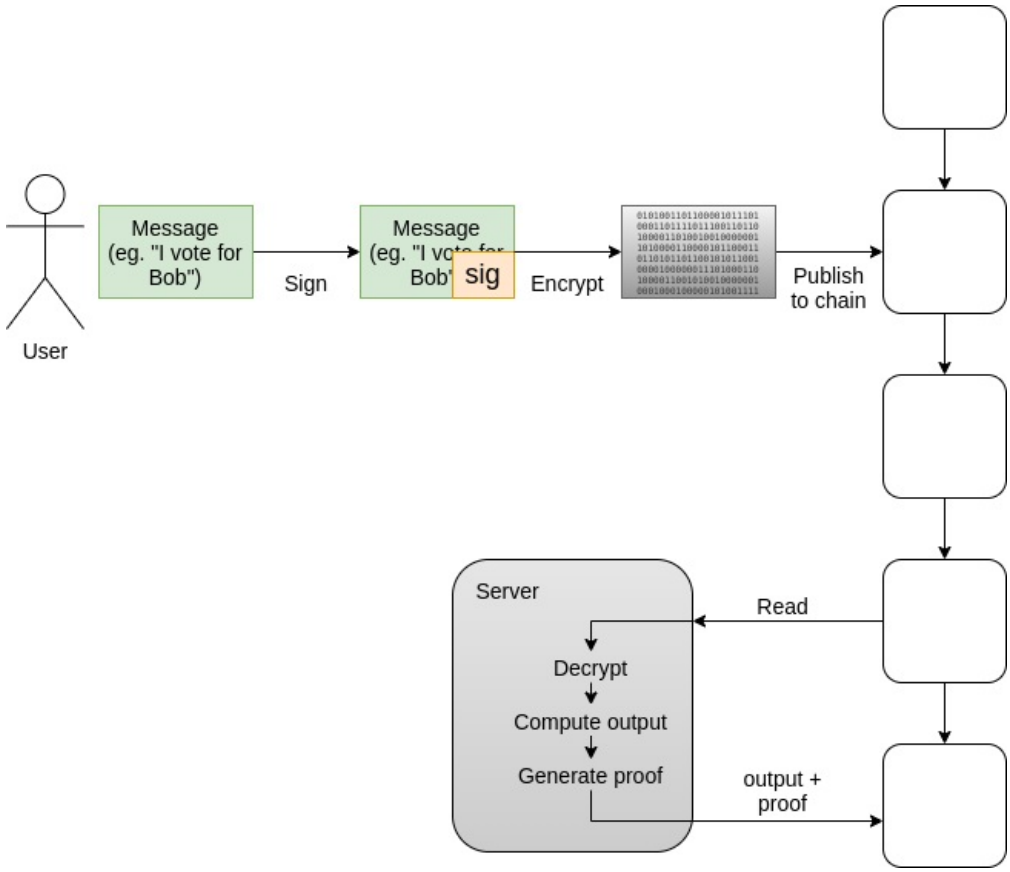


Diagram of how MACI works, combining together blockchains for censorship resistance, encryption for privacy, and ZK-SNARKs to ensure the result is correct without compromising on the other goals.

Voting in existing national elections is already a high-assurance process, and it will take a long time before countries and citizens are comfortable with the security assurances of any electronic ways to vote, blockchain or otherwise. But technology like this *can* be valuable very soon in two other places:

1. Increasing the assurance of voting processes that already happen electronically today (eg. social media votes, polls, petitions)

2. Creating new forms of voting that allow citizens or members of groups to give rapid feedback, and baking high assurance into those from the start

Going beyond voting, there is an entire field of potential "auditable centralized services" that could be well-served by some form of hybrid off-chain validium architecture. The easiest example of this is proof of solvency for exchanges, but there are plenty of other possible examples:

- Government registries
- Corporate accounting
- Games (see Dark Forest for an example)
- Supply chain applications
- Tracking access authorization
- ...

As we go further down the list, we get to use cases that are lower and lower value, but it is important to remember that these use cases are also quite low cost. Validiums do not require publishing everything on-chain. Rather, they can be simple wrappers around existing pieces of software that maintain a Merkle root (or other commitment) of the database and occasionally publish the root on-chain along with a SNARK proving that it was updated correctly. This is a strict improvement over existing systems, because it opens the door for cross-institutional proofs and public auditing.

So how do we get there?

Many of these applications are being built today, though many of these applications are seeing only limited usage because of the limitations of present-day technology. Blockchains are not scalable, transactions until recently took a fairly long time to reliably get included on the chain, and present-day wallets give users an uncomfortable choice between low convenience and low security. In the longer term, many of these applications will need to overcome the specter of privacy issues.

These are all problems that can be solved, and there is a strong drive to solve them. The FTX collapse has shown many people the importance of truly decentralized solutions to holding funds, and the rise of ERC-4337 and account abstraction wallets gives us an opportunity to create such alternatives. Rollup technology is rapidly progressing to solve scalability, and transactions already get included much more quickly on-chain than they did three years ago.

But what is also important is to be intentional about the application ecosystem itself. Many of the more stable and boring applications do not get built because there is less excitement and less short-term profit to be earned around them: the LUNA market cap got to over $30 billion, while stablecoins striving for robustness and simplicity often get largely ignored for years. Non-financial applications often have no hope of earning $30 billion because they do not have a token at all. But it is these applications that will be most valuable for the ecosystem in the long term, and that will bring the most lasting value to both their users and those who build and support them.