The Rollup Multiverse

Originally posted to [Mirror.](#)

Thank you to [Patrick McCorry](#) and [Kobi Gurkan](#) for the invaluable feedback and review.

Introduction

I like rollups so I'm writing another thing, sorry.

I'm pretty sure it's helpful because I've gotten a ton of value out of these myself. Just writing it all down and talking to people like Patrick and Kelvin who have amazing mental models has been awesome. There might be a double-digit number of people crazy enough to even want this level of intuitive understanding of these systems, but if you're one of 'em hopefully this helps.

This time I'll more directly address why

the rollup ≠ bridge rambling is important, since I probably could've done a better job of explaining the practical and social implications more plainly in my [last post](#).

A few people got a tad upset at that one. Not my intention, but it wasn't the first time and won't be the last.

[Some of it](#) was a lack of understanding of how rollups work, but[others were more reasonable](#) - that the post was technically accurate, but it's not reflective of the current reality, and hair-splitting over definitions will create more confusion.

I can appreciate the latter sentiment, because [reducing](#)

[confusion](#) is my explicit intention here. The first obvious point is that[these aren't children's books](#).

That post was a technical look into the fundamental security and social consensus properties of rollups that takes over an hour to read if you go at it non-stop. [Though some already had pretty strong opinions ~20 minutes after posting it 😊](#)It's aimed at the reasonably technical audience responsible for building rollups and shaping the messaging around them.

First, to be clear:

- Rollups are dope - that's why I spend most of my waking hours on them.

- [Their "trust-minimized" bridges are also dope](#), and that's the biggest reason people use rollups like Optimism and Arbitrum today. [This can provide far superior security vs. bridging your assets to a sidechain](#)

I've always considered myself very Ethereum-centric. It's quite apparent from where I spend my time, and honestly most of my crypto bags are just ETH. This isn't a FUD rant. It's a short (for me) rant on the following:

- The current understanding of how rollups fundamentally work is inaccurate and misleading - it is itself the cause of much confusion today

- This framing is based on a microcosm of what we see in front of our eyes, and it will clearly change very soon

- A new framing can be incredibly helpful to fundamentally understand why these systems are so great

- The possibility of a rollup forking is a feature, not a bug

- Why we're stuck on it, and how to improve it

Our Current Framing is Harmful to Users

The focus of this whole framing:

They are. As much as people would like handwave this away by appealing to social consensus, the concrete properties of classic rollups are enforced by the bridge.

The bridge is an incredibly important piece of how rollups like Optimism and Arbitrum work, but it is not the rollup itself

. This may seem like semantics, so I'll be concrete.

It'd probably be fine if this description was stretching reality but it actually worked. However, in reality it's misleading:

For those unconvinced we need a better framing for rollups' security properties, and that anything nuanced & accurate will add more confusion

Whatever mental model we're using to communicate today isn't working so great if we're at ~50/50 here lol
https://t.co/IU46f1DqaI pic.twitter.com/TSLHxr2JxI

— Jon Charbonneau (@jon_charb) May 28, 2023

It should be obvious why this is. If we keep telling users that "the rollup is the bridge" and the "settlement layer L1" (Ethereum here) is this god that determines the truth, then users will naturally be led to believe that L1 + rollup bridge = safe. That's quite clearly the message.

Assets That Live Natively on Both Chains

Unfortunately, the reality is quite the opposite. Rollups can inherit their base layer's (e.g., Ethereum) security without the bridge. For assets that live natively on multiple chains, the native representation is always safer than their lock-and-mint bridged representation

.

The bridged asset is just an IOU from the bridge. That's why versions from different bridges aren't fungible As an example:

- If I hold native USDC minted on a rollup - I trust Circle

- If I hold bridged USDC minted on Ethereum → bridged to the rollup - I trust Circle and the rollup bridge

Circle is itself effectively a bridge from the real world (they bridge real-world USD into onchain USDC). CCTP will also allow for permissionless burning of native USDC on one chain and minting native USDC on another. As mentioned in my last post:

You could deploy an asset natively on multiple chains using a burn-and-mint bridge. However, note that this asset would then carry the security risk of the lowest common denominator of bridges deployed across all chains

In this case, Circle must attest to all mint-and-burns, so it happens to be the same trust model. In any case, holding a native asset that lives natively on multiple chains means you're always trusting:

- The backer (e.g., Circle) + mint-and-burn mechanism (e.g., CCTP)

Holding a lock-and-mint bridged representation of this asset means you're trusting:

- The backer (e.g., Circle) + mint-and-burn mechanism (e.g., CCTP) + the lock-and-mint bridge (e.g., rollup contract bridge)

You're inherently taking implementation risk here. For example, a smart contract bug could cause a bridge hack leaving the bridged rollup funds entirely unbacked. These contracts will harden over time, but we're definitely not all the way there yet. It's a risk.

And yet, this framing has left people with no clue. They're ~50/50 on what's safer. So not only only is our oversimplified mental model not reflective of the fundamental reality, it's also confusing and misleading

.

Rollup Bridged Asset vs. Asset That Only Lives Natively on the Rollup

The apples to oranges comparison would be a rollup-native asset (e.g., OP) vs. a bridged base layer-native asset (e.g., bridged ETH) on a rollup. So now the difference comes down to:

- Bridged ETH

- Additionally trust correct bridge implementation (including its onchcain governance potentially)

- Native OP

- Additionally trust Optimism social consensus (offchain governance)

As I noted in the last post, this points to the fundamental reason to own any asset vs. another:

However, you should notice why it's a perfectly ok assumption. You're obviously happy with the social consensus of Optimism if you hold OP because that's precisely why you hold it. It derives its value from that social consensus.

That's why these bridges are amazing - I don't have to trust another chain or

its social consensus. I can always force withdrawal back to Ethereum if that's the only social consensus I wanted to opt into.

If you don't trust the social consensus of a given chain not to take all your money, obviously you shouldn't hold that chain's native asset. Ethereum could hard fork tomorrow and just delete your ETH, but you probably feel pretty good about those odds if you hold ETH.

And that matters! What if Justin Sun was using bridged ETH (or some other asset custodied by an Ethereum rollup bridge) on a rollup instead of STEEM during the Steem-Hive Hard Fork? Well then they wouldn't have been able to fork out his funds. The social consensus can always hard fork a rollup, but they can't socially fork the collateral in the bridge

You may not want to opt into some external social consensus at times. You just wanna keep Ethereum's. Or, if the contract is upgradeable via an onchain governance mechanism you have faith in, you at least know the rules of the "due process" you're signing up for.

Rollups let you choose, and that's a superpower. However, if you want to use something like OP or ARB, then you are

opting into another social consensus. The chain and social consensus around it are fundamentally the driver of its value in the first place.

Our Current Framing is Not Future-Proof

And that's exactly why assets like USDC deployed natively (including on rollups) may very well grow in importance over the long-run. It's safer and fungible.

Native USDC is coming to Celestia rollups!   https://t.co/j1JguTgN2n

— Celestia (@CelestiaOrg) [May 30, 2023](May 30, 2023)

Today it's lock-and-mint bridged to rollups, but CCTP could make this mint-and-burn easy (and quite attractive, especially for optimistic rollups). We're also likely to see other real-world assets (RWAs) move onchain over time (e.g., Treasuries, etc.).

The implications of this would be clear - the relative importance shifts from the "official" rollup bridge → USDC and Circle (which is itself just a bridge for USD). The whole "practical" argument was that a rollup is defined by the bridge because it holds the majority of assets.

So what happens once we have a chain where native USDC (or some other RWA) TVL surpasses the "official" bridge TVL? This seems highly

likely given people have aspirations for consumer-oriented applications and payments, as simple examples. Now does Circle define the rollup? Or swap in any other RWA that may be used onchain. The mental model falls apart.

It's the same reason that people worry about stablecoin issuers' control over Ethereum in deciding a contentious fork

— Uma Roy (@pumatheuma) May 30, 2023

Does that mean Circle defines Ethereum? Of course not! The two ideas below are plainly incompatible:

- To realize that stablecoin issuers' power over Ethereum is a concern, but it does not define Ethereum

- Thinking the enshrined bridge will always define the rollup

It touches on the fundamentally important point though - social consensus always decides the chain, but whatever valuable state you have that someone has god mode control over (whether that's Circle or an Ethereum rollup bridge) has power in swaying social consensus to be the chain that "matters".

The bridges with the most economic bandwidth.

— Zaki ⚛ (@zmanian) May 24, 2023

To ignore the practical realities of what these systems will soon look like is short-sighted. Acting like the single "official" bridge is the final arbiter on everything in the rollup is inaccurate. We're communicating everything (incorrectly) based on two highly financialized general-purpose rollups with largely bridged assets for which this is a "good enough" description without looking any further.

The point is simple - we've developed inaccurate mental models of how these systems fundamentally work because we're influenced by what we see today

That's problematic considering not every rollup in the future is gonna look exactly like optimism and arbitrum

— Jon Charbonneau (@jon_charb) May 27, 2023

This applies equally to native assets which derive their value from a given chain's social consensus. If the majority of assets on a rollup are from native applications (i.e., bridged funds represent a smaller portion of value), then the rollup has significantly higher "practical" sovereignty.

What happens when the next big memecoin that moons is native to a rollup, and that comprises nearly all of its value? Assuming the memecoin is also primarily used on this rollup, then the community doesn't care as much about the bridge (because there's not much in it).

Take some rollup where the large majority of funds are from native assets, and there's a crazy bug on the rollup where someone prints a bajillion native tokens. Or maybe rollup governance token holders are getting greedy and extracting too much value. The L1 contract is immutable, or governance doesn't want to fork the contract, Ethereum obviously refuses to hard fork, etc. Well then social consensus obviously forks the rollup

.

They can't fork the bridge contract, but users can just force withdraw their ETH to the original contract. The rest of the chain doesn't even really care because it's not much of the value on the rollup anyway.

Hence my the framing I chose to use about "L1s" and "L2s" being relative terminology:

In essence, I use "L1" to refer to the portion of assets which derive their social consensus (and thus their value) from that chain. It is the ledger of record for these assets.

I then described a chain to be acting as an "L2" for its foreign state which does not add any security or social consensus assumption's beyond that state's "native" chain (or entity).

I consider "implementation risk" generally within the bounds of the native chain here. For example, if you put your money into a faulty smart contract (e.g., a rollup bridge), you're obviously taking a risk. You also need one honest party. This differs from an honest-majority bridge where now you trust another external consensus (or committee of people) to attest to offchain state, even if the contract implementation is perfect.

For example:

- Using bridged ETH on a rollup

- Even malicious rollup operators can't take my money. Ethereum can still save me (forced exit).

- Using native USDC on Ethereum

- Even if Ethereum is entirely malicious, they can't take my money. Circle can still save me (redeem for dollars).

Hence my somewhat crazy statement in the last post:

You could say that people like USDC for much the same reason they like rollups.

You're using some asset (ETH or dollars) bridged somewhere else without signing up for another set of rules, security, and social consensus.

As noted in the previous post, Ethereum can even be an "L2" to Optimism in this sense:

For example, let's say I bridge my OP token from Optimism to Ethereum. In both cases:

- My OP maintains the same social consensus assumptions of Optimism.

- My OP maintains the same security assumptions of Optimism.

Note that Optimism's security = Ethereum's security in this case, so it's indirect. In any case, the point remains - I'm adding no new assumptions external to Ethereum.

Whenever you use a chain as an L2, you have the same security and social consensus assumptions that you'd have on the home L1 + bridge risk (implementation risk)

. You'd be safer holding OP on Optimism vs. holding a bridged representation of it on Ethereum.

The "L1" for any chain by this framing is then the party that dictates the valuable state (purely financial or otherwise), and thus has significant power over determining that chain's future path:

- Rollup bridge contract

- Rollup onchain governance and Ethereum have power

- Real-world assets (RWAs)

- Issuer has power (e.g., Circle)

- Native state

- Rollup social consensus has power

This is a spectrum. To ignore this is to ignore the fundamental nature of how these systems work. We completely miss who actually has the power here.

The counterargument is the following:

[Obviously a smart contract rollup can be seen as a [sovereign] rollup for assets originating on it. The point is that's not why people use it. They use it for the bridged assets.](#)

[If you have an asset that's completely independent from everything else that happens on the rollup and Ethereum, you can of course choose to maintain your own fork. But who would use a smart contract rollup for that in the first place?](#)

Here I just fundamentally disagree. People don't use these rollups only for bridged assets. Using ETH on Optimism is clearly only one of many things you can do there. You could have a million other things on a rollup where bridged ETH plays a de minimis role.

In many situations, you'll likely have rollups that look much like today's. They'll have a bridge that holds a large portion of the rollup's underlying assets. This could effectively control the rollup, as it'll be impractical to fork away. Figuring out onchain governance will be especially important here.

So the current framing is good enough if you think the only long-run use case for rollups is roughly a bunch of based rollups without native tokens, and you just bridge up some ETH to leverage long ETH even more because it's too expensive on L1.

If you think it's anything else (I sincerely hope so), then we're completely missing the picture. What do NFT rollups look like? Native DeFi applications? Gaming? RWAs? Literally any of the things everyone keeps saying they're excited about?

ETH will certainly play a huge role, but this isn't a black-and-white all-or-none thing here. Maybe I'm too optimistic, but my strong guess is that rollups will actually have some interesting and valuable state beyond bridged ETH trading.

TLDR

- Use whatever definitions for "L1" and "L2" you want, I know people get scared by new things. But this alternative framing of L1 and L2 actually captures both critical points:

- Assets are safer on their native chain (or entity)

- The chain (or entity) which acts as the L1 for given assets is the ledger of record. It has effective control over them when chains are used as L1s and L2s here, so the real L1 has meaningful implicit economic influence over the social consensus of the L2 which is reliant on this collateral

The current framing captures neither. It's mostly just a loose description of the security relationship, but this doesn't seem helpful since "base layer/DA layer" and "rollup" already cover this. That's where the rollup's security comes from.

Also, the current "L2" definition generally includes validiums, which makes little sense to me. These validium bridged assets don't get Ethereum security anymore - they get the security of their DA layer.

(Note that a validium DA failure wouldn't let you force an invalid state transition and steal user funds. However, you could force a valid

state transition and withhold the data. Then, nobody else can recreate the state, and you demand ransom with the chain halted.)

Onchain vs. Offchain Governance

My previous post fit my typical style of focusing more on the technical and economic implications of my arguments. This time, I'll philosophize a bit on the more squishy social stuff.

As a refresher, I mentioned last time:

Upgrading a rollup's enshrined bridge requires upgrading its smart contract. This upgrade path is often undesirable:

- Today

- Contract upgrade keys are often held by a multisig of core team members. They may have the ability to make instant and arbitrary upgrades to the contract.

- Future

- Hopefully, upgrade keys will move over to rollup governance (or become immutable). In any case, this must take the form of onchain governance (e.g., token voting, or using some other form of onchain identity to vote). Ideally, the upgrade window would be set comfortably longer than the withdrawal period. If you don't like the upgrade, you can withdraw your funds.

Just because the bridge contract requires onchain governance (or is immutable) does not mean the rollup itself requires onchain governance (or is immutable).

Offchain governance can always fork the rollup, but onchain governance is needed to fork the bridge. Bridge ≠ rollup.

And users can still withdraw their collateral from the bridge to the original fork. They may or may not choose to bridge it back into the new fork. The new rollup would simply lose the ties to the collateral behind the bridge.

Whether it's "practical" to fork socially is a spectrum based on how important the bridge is, but it is not a fundamental limitation. If all the users decide that the forked rollup is the new "canonical" rollup and they all use that one, then that's what matters.

This doesn't invalidate that the bridge is real (wrt/ Ethereum) but makes the point that the thing object we actually care about and attach the OP Mainnet Name is not inextricably tied to the bridge

— smartcontracts.eth (✩°   _   ✩°) (@kelvinfichter) [May 27, 2023](#)

There's a reason that Ethereum has offchain governance - onchain governance kinda sucks so far

. If there's one thing that crypto certainly hasn't figured out yet, it's how to implement functioning and non-plutocratic token-holder governance. This understandably hasn't been a priority for most rollups at the moment, so I applaud those who are focusing on it.

Arguing that the bridge defines the rollup then implies that if onchain governance (generally token holders) say something, that's what goes. This seems patently unacceptable to me considering these are inherently social systems. The implication here is that every Ethereum rollup is fully subject to onchain governance (if any), and rollup social consensus is absolutely powerless.

Take another simple example - we have some social media application that has its own rollup. Users have a little bit of bridged ETH on there to pay for gas fees. But this application starts to get really popular, so the governance token holders get greedy. They start jacking up prices on users.

But most of the valuable state here is just user data, not the bridged funds

. [Patrick](#) had [an amazing way of framing this more broadly](#).

The fundamental issue is that people talk about blockchains in the form of products. That creates lots of confusion as there is no native way to compare it.

It's better to get back to basics and say: "I want to build a database that anyone can read/write too."

Then talk about posting data onchain as that allows anyone to post a transaction / read all transactions to compute the db.

"Ok now anyone can get access to the database, how can I send messages from a blockchain network to this database and vice versa"

Then you start thinking about bridging protocols and of course the validating bridge. So there are really two tasks:

- how to build an open database
- how to communicate to/from the open database

The reason people link the validating bridge to the rollup is mostly because:

- it is hard as shit to build
- it currently holds >90% of bridged assets
- it is currently being leveraged to define access to the DA layer
- multiple validating bridges == fragmentation of assets, not really desirable for DeFi

So theoretically they are two different problems, but practically the bridge has been overloaded to perform more than just custodying assets. Whether that is good or bad I don't know, but it's still early days in the land of bridges and cross-chain protocols.

We want to build systems with open databases. Anyone can read it, interact with it, and verify it at any given time. For this

database to interact with external state, we need a method of communication (bridges). Rollup bridges are great for this - they can reduce trust in external parties.

The DA layer is just a public bulletin board to this end which provides global consistency. If people wanted, they could decide to interpret the data differently, or even pick a different bulletin board.

With this in mind - the users hold the power here

. So what they do? They socially fork the chain

. This property is absolutely critical. It's a huge part of what makes blockchains what they are. No lock-in, social consensus, users decide. That's literally the whole reason that people want to do a bunch of social media stuff onchain. This extends to the protocol itself just as much as it applies to someone making a front-end application for it.

To ignore this social consensus property appears completely antithetical to everything we're supposedly building.

It makes little sense to use this messaging that the bridge = the rollup, leaving users entirely subject to onchain governance. Yes, the bridge's onchain governance has power, but this is not an absolute.

Obviously these contentious forks are not everyday circumstances. People don't like thinking about them. It's abnormal for large and economically important contingents (e.g., onchain bridge governance vs. offchain rollup social consensus) to diverge, but these are precisely the defining moments and qualities that make these systems what they are

. It can be easy to forget that sometimes.

The fact that social consensus has power is great! It's a feature, not a bug!

Why Are We Stuck to Our Current Mental Model?

For most of the people I've argued with here, I obviously love them. We just love debating about crypto, and mostly get caught up on some finer points of semantics on occasion. I tend to debate the most with the people I like a lot in case you haven't noticed by now.

Outside that, I think there's a few broad reasons why some others have had a tough time seeing eye-to-eye here:

- They already get it

- A handful of people already intuitively understand what I'm saying. But the current rough terminology we're using seem "good enough," and this new stuff is just too confusing. As described above, our mental models aren't translating very well outside of this small group. Most people don't get it. It also makes little sense in the future (not even that far out).

- They don't get it

- See above. This is no fault of their own - I think we just haven't been doing a great job of explaining how these systems work to most people. We're all learning as we go along.

- It's uncomfortable

- It's the opposite of how most people describe this stuff, and it doesn't apply to the two largest rollups today. It doesn't fit what we see right in front of our eyes. This is naturally jarring, but I think we need to open up here. Rollups are gonna be much bigger than what we see today.

There are also some more personal factors:

- "Settlement Layer"

- The whole "Ethereum world settlement layer" thing sounds cool and valuable. A lot of people like that, and I reframed what this notion actually means. While the social implications I'm making are positive, a lot of people seem more focused on what they view as the economic implications based on their preconceived notions of where value will come from.

- ZKR vs. ORU

- Some ZK teams in particular have dedicated an immense amount of work into building amazing proving systems and associated bridges. It's a tremendous achievement which can't be understated. The rollup ≠ bridge thing can seem as if it's giving a "free pass" to rollup teams who've focused less on the bridge/proof aspect of the rollup.

- "Sovereign Rollups"

- The implication that the bridge grants security to the rollup[makes it sound like "traditional" sovereign rollups (i.e., those without an enshrined L1 bridge) are completely insecure](). It amazes me how prevalent this notion is, even amongst "experts" I speak to. This was a big point I wanted to clarify in that post.The cynic in me realizes that some of this is likely intentional. This is probably seen as beneficial because they aren't generally viewed as an "Ethereum idea." They're seen as more of a Celestia or Bitcoin thing now. This of course makes little sense, as you could easily deploy "sovereign" rollups like this on Ethereum.

But that.. isn't true. I can make a "sovereign" rollup on Ethereum that has a single sequencer that can't steal anything.

— smartcontracts.eth (✧ _ ✧) (@kelvinfichter) [May 27, 2023]()

I get it, we all want our thing to be special:

- My ZKR is super fast, and your ORU isn't.

- My ORU actually works, and your ZKR is on "announcement of an announcement" #12 for being the first zkEVM.

- My sovereign rollup is super sovereign, and your smart contract rollup isn't.

- My smart contract rollup is super secure, and your sovereign rollup isn't.

Sometimes they're a lot closer than we actually think though.

But we're missing what makes our things actually

special, and it's often the social consensus behind them. Blockchains are social coordination tools. We are building inherently social and political systems. That's the whole point.

Hopefully we can broaden our views going forward without going totally crazy (maybe a bit optimistic, but worth a shot). I just don't want to start going the Bitcoin maxi route because then Eric and Udi will start trolling us more, and we'll have to give Eric more tungsten cubes.

It's not good business to get anyone upset, but I'm gonna call stuff out if I think it's incorrect and misleading. Maybe I could tone down the post titles since some people don't really read past them, but then again this is crypto. We've gotta have some fun while we're here.

The Rollup Multiverse - The Bridge Defines One Rollup

Before we wrap up, I'll briefly explain what I think is the more "technical" reason we're stuck on.

I send Ethereum assets (e.g., ETH) into the contract and get the bridged version on the rollup. Assuming correct implementation, I can always get my ETH back on Ethereum

.

That's great. This contrasts with traditional honest majority bridges where I now trust the receiving chain's consensus not to screw me. The rollup operator could be malicious, rollup social consensus could socially fork, etc. It doesn't matter. The bridge will just observe the rollup chain that this holder cares about. They can always come back home.

The bridge often does other important stuff as well. For an "enshrined" bridge, the rollup's state often depends on the contract in some way today. For example, [even if the Arbitrum sequencer never includes your transactions, you can post it to the delayed inbox contract and "force include" it after some delay period (currently ~24 hours on Arbitrum One)]().

This bridge enforcement could be seen as one distinction vs. an "unofficial" rollup bridge (which still fully validates the rollup) where the rollup's state doesn't depend on it in any way. As I mentioned last time, [Sovereign Labs will implement the fork-]()

[choice rule baked directly into the ZK proof, which includes scanning the DA layer for any eligible transactions to force inclusion of](). Clients just run the rules offchain and enforce it using the proof. Clients also receive the proof via p2p rather than looking to the contract as their "source of truth."

They can then have validating bridges to the base layer which aren't "enshrined" in the sense that the bridge doesn't directly impact the rollup's state in any special way. [Different bridges can have different upgrade paths]()

Back to the Arbitrum inbox though:

- This enforces censorship resistance, allowing users to force include transactions into the "canonical" chain from the bridge's point of view

. It doesn't care if the rollup socially forks. It won't observe it (unless the contract is upgraded to do so).This bridge has a total radar lock on one rollup from its perspective, implying its existence. It does "define" this one

rollup in this sense, regardless of whether anyone cares about it.

- However, it provides no guarantees of being included in the "canonical" chain from anyone else's point of view

. The contract saying "please force include my ARB transfer" isn't very meaningful if the rollup were to socially fork, and this new fork is the only one where ARB has any value. Everyone else moved onto another fork which doesn't listen to the contract anymore.

And that's the point - the "canonical" chain is relative. As a user who has assets bridged from Ethereum, I place no assumptions on the rollup. I can go back home to Ethereum because that's the ledger of record for my asset. It can't help me if the thing I want to do is inherently tied to the social consensus' view of what is the "canonical" rollup.

We live in the multiverse of rollups. It's messy when the timelines fork, but it can happen.

TLDR

- Rollup = bridge, but also rollup ≠ bridge. You get to choose though, and that's why they're great.

Simple Takeaways

Here are the key points:

- Rollups can inherit their base layer's security regardless of whether they have a bridge.

- Rollups are basically just some data output that we all agree is interesting, based on some data input that we posted onchain (like on Ethereum).

- The bridge doesn't define the "canonical" rollup because there is no globally absolute "canonical" rollup. It does cool stuff like control the collateral for bridged funds though, and that's super important when applicable.

- Assets which some offchain actor (e.g., a rollup's L1 bridge contract, or RWA issuers) has total control over can't be forked without their permission. The entities that control these assets are economically super important. They can sway social consensus.

- Social consensus = communities can always socially fork the native state that derives its value from that chain and the social consensus around it.

- Natively minted assets are safer than their lock-and-mint bridged representations.

- If you're gonna bridge, rollup bridges are dope. Sidechain bridges = you've gotta trust the other chain's consensus too. Rollup bridges = the home chain can save you.

That's about it. Call these things rollups, L1s, L43s, cotton candy, whatever - I don't really care. Just remember those.

Rollups are *actually* just fruit flavored candy

Words Aren't Real

I'd pay a lot for a canonical crypto dictionary, but alas, here we are. The teams building "zkEVM L2s" don't even agree on what's a "zkEVM" or an "L2." It's kinda funny if we're being honest.

If you use the big buzz words, then just clearly define what you mean. But the whole "my thing is X and yours isn't because I defined it this way" without clearly describing what you're talking about isn't helpful. Then you're just arguing over semantics for marketing, and everyone else gets confused.

If you're clear and truthful about what you mean, you can start calling your rollups "pancakes" and bridges "bananas" for all I care. In any case, pancakes ≠ bananas (but they're dope when you put 'em together).

Arguing over canonical terminology is probably a lost cause for a while:

If there's anything I've learned in crypto, it's that attempting to standardize terms which:

1) aren't precise and

2) different teams actively have an incentive to craft to their own personal gain

Never works

Just use more specific terms

— Jon Charbonneau (@jon_charb) April 6, 2023

But debating over the real stuff behind them is helpful:

When done in good faith, arguing about terminology or taxonomies can be a useful way to broaden intuitions and generate new ideas

— Dan Robinson (@danrobinson) May 27, 2023

I have little hope for a canonical crypto dictionary anytime soon, but I do still hope we can get a little better at understanding what we're actually building.

Disclaimer: The views expressed in this post are solely those of the author in their individual capacity and are not the views of DBA Crypto, LLC or its affiliates (together with its affiliates, "DBA"). The author of this report has personal investments in ETH, Celestia, and Sovereign Labs Inc.

This content is provided for informational purposes only, and should not be relied upon as the basis for an investment decision, and is not, and should not be assumed to be, complete. The contents herein are not to be construed as legal, business, or tax advice. References to any securities or digital assets are for illustrative purposes only, and do not constitute an investment recommendation or offer to provide investment advisory services. This post does not constitute investment advice or an offer to sell or a solicitation of an offer to purchase any limited partner interests in any investment vehicle managed by DBA.

Certain information contained within has been obtained from third-party sources. While taken from sources believed to be reliable, DBA makes no representations about the accuracy of the information.