Oct. 25, 2019

Moderator:

Everyone, let's give a warm welcome to Jinglan Wang (Master Chief), Ben Jones (Spartan Ops), and Karl Floersch (The Arbiter) of Plasma Group!

As a reminder for everyone participating—please keep the discussion respectful and on-topic at all times.

PG team—could you start off by giving us a brief bio on your backgrounds as well as how you got started in crypto? And then a short overview of Optimistic Rollups and a brief update on your progress to date? We'll then be off to the races with questions.

Jing:

Hey everyone!

Brief bios:

Jing - MIT bitcoin club co prez, Wellesley dropout, previously Sia, Zcash, Handshake, Nasdaq

Ben - Math and Physics @ Northeastern, previously CBC Casper team

Karl - CS @ stony brook, Ethereum Foundation research team, previously Consensys, Casper FFG

We started as a plasma research team in January of this year. My teammates pioneered the way to build applications on plasma (generalized plasma predicates). However, through user testing we discovered that people wanted more than just high TPS, they wanted fully general solidity contracts. So we went back to the drawing board and now here we are!

Ben:

As for short overview on OR and progress, optimistic Rollup is an L2 scaling solution which uses fraud proofs and on-chain data availability to enable secure autonomous smart contracts on L2. Its benefits are afforded because execution is not performed on chain in the happy case. It turns out that making blockchain data available without processing it gives a much higher throughput and better UX. An intuition for why this scales come from the fact that bandwidth is cheaper than computation.

Our biggest public work to date is the site unipig.exchange, a collaboration with Uniswap to show how contracts can be done in L2. Encourage you all to check it out and remember to join #teamPIGI ;)

Anonymous:

Congrats on the Uniswap + PG demo. What's next for PG? Will we see a more productionized setting where the UI is identical to Uniswap but the feedback loops are faster/cheaper due to the scaling solution?

also, have you thought about porting Compound / other DeFi on your infra, + how difficult would it be? ie what are the main challenges beyond just engineering power

Jing:

Next for PG: probably a rebrand... especially since we're not building just Plasma and it's been confusing to a lot of people who think Optimistic Rollup is a feature of plasma.

Re: productionizing

» This is a priority.

Re: Compound and Defi difficulty

» We'd love to see more defi projects, we're definitely Defi bullish and are building a platform to support and scale all these interoperable defi projects! The main challenges beyond engineering power are the same challenges any project faces: security, bootstrapping network effects, and user experience.

Anonymous:

Is it feasible to port privacy DApps on top of optimistic rollup? For example, would it be possible to build Aztec protocol's stack or mixers on top of optimistic rollups?

Karl:

Absolutely. All smart contracts you know and love on Ethereum are possible on Optimistic Rollup. Additionally, it turns out that privacy contracts are especially well suited for OR because they often require heavier computation which is much cheaper in OR.

Jing:

Participants in OR ecosystem:

- Aggregators (incentivized with network fees)

- Validators (incentivized the same way full nodes in bitcoin are incentivized - for the security and speed of their own transactions. Uniswap would run their own validator, for example)

Oh! And fast exit liquidity providers! Incentivized with fees.

Jing:

Even private transactions on OR are at least an order of magnitude greater than current Ethereum TPS.

Anonymous:

What kinds of projects do you think make sense to build on optimistic rollups? Existing Ethereum projects that are struggling to scale and don't want to wait for Eth2? New projects?

Jing:

Both!

Anonymous:

nice! what kind of network fees? how are the fees determined?

Ben:

One nice thing about L2 is you can handle fees however you like because you're writing the code, and it doesn't require a hard fork like for L1. This is similar to the metatransactions work on Ethereum. We expect to see experimentation here, but at the very least we can do things like change the gas price of EVM operations which currently aren't well aligned (https://arxiv.org/abs/1909.07220)

Anonymous:

another very simple question: can you simply state the differences between zk-rollup and optimistic rollups? are there any other kinds of "rollups" out there?

Jing:

Zk rollup uses snarks for state root validity. Optimistic Rollup uses dispute games for the same thing. In the near term, dispute games are cheaper and can handle general computation. Snarks are super awesome though, mad respect to those building zkrollup.

Anonymous:

thank you! this is helpful. a follow up - does this mean zk rollups cannot handle general computation like smart contracts?

Jing:

Yep, at least that is the case currently.

Karl:

And probably will not support a snark friendly vm similar to EVM for years

Moderator:

Do users submit transactions to a specific aggregator or the entire pool of bonded aggregators?

Ben:

Great question! The answer is you can do it either way. A nice thing of having one aggregator is they can provide stronger guarantees to users instantly about the future state (confirmations with great UX). Having a pool of bonded aggregators has weaker confirmation properties but is nice and decentralized. We favor a hybrid approach which gets the best of both worlds.

Moderator:

Say I'm a developer that's getting ready to deploy my new DeFi primitive. Can you walk us through the most important trade-offs of going with ORs vs. L1?

Jing:

Great question!

Assuming juicy network effects and battle tested production code, you'd have

Cons: Asynchronous comms with L1 including deposits and withdrawal flows. You'd have less than ideal UX (interchain communication ux) for two apps trying to talk to each other on different layers.

Pros: Instant confirmations and low fees. Sweet UX for two apps talking to each other on the same layer.

Anonymous:

Could you explain how you achieve instant confirmations with optimistic rollup when there could be reorgs? Is there some combination of receipts and collateralization?

Karl:

Yep! There are a number of ways to achieve this both at a smart contract level and top level. The simplest is at the top level give priority to an aggregator & allow signed receipts (with state channels it can be fully backed) from that prioritized aggregator

Moderator:

Gotcha, super helpful. Now, let's say I have a mini-ecosystem of DeFi primitives committed to deploying on ORs. Can they deploy to a DeFi-specific rollup? Throughput is much greater than L1, but not infinitely so

Ben:

You can have multiple rollup chains, but again you run into the issue of inter-chain communication. This is easier between rollup chains than L1<>L2, but not perfect. Cross-chain comms generally throw a wrench into money legos, things like cosmos' IBC are non-trivial. Luckily a single chain can support all applications at once, so we see this as the likely future for now. There isn't a throughput increase to having two rollup chains instead of one, from the perspective of L1 costs/ideal max throughput.

Moderator:

Gotcha. How would you describe the security guarantees of OR vs. L1? If I'm a user who holds a significant amount of funds in a contract deployed on OR, what am I most worried about?

Karl:

I'm most worried about a 51% attack of Ethereum. Next I will want to make sure that there is someone I trust validating the rollup chain — which can be myself. If both of these security assumptions hold true then you're secure—barring software bugs / smart contract/client developer error

Moderator:

Makes total sense. Let's say you're validating and you notice misbehavior. What happens next?

Karl:

You will submit an auto generated fraud proof to the main chain. That fraud proof will execute immediately, delete the offending OR block, and slash whatever aggregator submitted it

Moderator:

Excellent. And I get some % of their bond?

Karl:

Yep! But some must be burned to prevent free miner griefing

Anonymous:

are any other projects currently working on building on optimistic rollups right now?

Jing:

There are some application specific rollups being built, but none that are optimizing for fully general solidity contracts (to our knowledge).

Anonymous:

What's the status on combining optimistic rollups with other L2s such as channels?

Jing:

We believe that the current TPS of OR is enough to scale the current needs of the network. That said, state channel and plasma contracts can be deployed to OR and as more users flood into crypto, this will be awesome.

There are also use cases that are better suited to channels, like micropayments and games, so maybe we'll see channel contracts on OR earlier

Anonymous:

What other L2 systems allow fully general solidity contracts and how do they compare to OR?

Karl:

No other L2 supports smart contracts with the same security guarantees & recoverability as OR. Plasma can run fully general smart contracts but then you must introduce complex data availability challenge logic

Anonymous:

How much state does an OR validator need to hold?

Karl:

Great question. OR as we've designed it uses a stateless client model and so some state can be forgotten. That said, things like state rent still apply here

Anonymous:

So users are responsible of their own data/storage, and include that in their transactions as proof?

Karl:

What you described is exactly the stateless client model and will likely be implemented once the state size of OR becomes too large. That said, we can use cryptoeconomic light clients so normal users often don't have to deal with this complexity, it's more for power users / full nodes

Anonymous:

ORU is account based model, are there mass exit attacks here?

We put a lot of work in plasma cash to mitigate mass exits, can't an aggregator make a large invalid state transition and exit the whole value of the chain?

Ben:

There are not mass exit attacks—the way to think about this is that this was an issue in plasma because the state could progress off-chain, but proving that the state progressed invalidly required putting a bunch of it on chain—this was the mass exit. Because data is put on-chain up front, this can't happen for OR. As for the "large invalid state transition," we inherit gas metering from L1 and use that to bound the size of the fraud proof. Since only 1 fraud proof is ever needed, it's quite cheap, even small in comparison to the rollup state itself.

Moderator:

Are there any specific projects that you think would be well-suited towards transitioning to OR?

Jing:

In our biased opinion, we think all projects should transition to OR heh ;). We believe that DeFi is particularly well suited, due to tight coupling between the money legos

This is the same thing that makes them ill-suited for plasma and channels

Moderator:

Gotcha. Which phase/when can OR be deployed on Eth2?

Jing:

Phase 1, or whenever eth 2 provides data availability. This would be steroids for OR scaling (proportional to the # of shards)

Moderator:

That's really interesting...perhaps that will provide an impetus for projects to move from Eth1 L1 to OR

Jing:

Hopefully that incentive exists even without Eth 2

It's great that OR allows you to take advantage of Eth 2 while preserving Eth 1.0 synchronous calls - key to money legos

Anonymous:

How can PG monetize this product?

Run an aggregator & collect fees?

Jing:

That's one way :)

Anonymous:

What could be the problem that halts the development of OR and proceeding to find a better alternative?

I.e. for Plasma it was the inability to run general smart contracts.

Jing:

That's a good question, especially considering that was what Optimistic Rollup did to Plasma for us.

To clarify, Plasma could run general contracts, it was just incredibly complex.

This is a difficult question to answer, hindsight is 20/20 but currently very little is in the way of OR for V1 on ETH 1.0

Some possibilities:

- Market shifts and defi dies, payments becomes the main use case for crypto... then plasma and channels are better

- Mass adoption surges into crypto but there is no innovation in data availability oracles, this would be a bottleneck

- It turns out nobody cares about security or decentralization, then sidechains may reign supreme

Anonymous:

Another question, what would be the effect of OR on the L1 state size, can it lead to accelerated bloating?

Jing:

No, OR massively reduces state bloat on the mainchain by only recording state roots and not state... this is why OR scales

Anonymous:

it bloats history not state

Anonymous:

what were you all excited about a year ago? what do you think you'll be excited about in a year?

Jing:

Scaling ethereum! Then and in the future. We were stoked on plasma a year ago, and hopefully Optimistic Rollup works so well that the time to get excited about plasma will come again

Moderator:

Alright everyone, I think we're at time! Thanks so much Jing, Karl, and Ben for coming on Crypto AMA. What's the best way to stay apprised of PG/OR developments as well as the best way to get in touch?

Jing:

Twitter @plasma_group and you all have our telegram handles now, feel free to shoot a DM any time