Notes - Exploring Intents

Notes from a Twitter Spaces conversation on intents hosted by Celestia featuringNick White (Celestia), Zaki Manian (Sommelier), Henry de Valence (Penumbra), Christopher Goes (Heliax) & Uma Roy (Succinct).

Highlights

- Motivations and definition of intents
- Account Abstraction and Cross-chain UX
- P2P netowrk designs
- Solvers
- Intents and the modular stack
- Intents already exist

Conversation

Motivations and definition of intents

Nick

: What are intents and what problem do they solve?

Zaki

: I like to start with the problem they solve. Why would you need an intent? Millions of people are using blockchains and transactions. Sommelier is this protocol or application for making DeFi easier to use, especially complex DeFi things (leverage, LPs). We have succeeded as long as someone can get into our smart contracts.

You start with a user who has their coins somewhere (CEX, L1, L2, etc) and they want to use your app and gain the benefits. How do I do this? Depending on where you are you have to send money to a particular wallet with particular coins which includes needing to use a specific bridge and IBC. Basically, there have been a bunch of problems with that. How do I navigate? We have meme coins and large number of people enter the market as unsophisticated participants who pay gas fees and suffer poor slippage. We have all of these missing pieces, UX/UI issues. We tried to build routing frameworks that improve this. But when you add cross-chain into this, it becomes a nightmare.

Wat Do?

The idea is that we can build infra where people can say I am willing to trade X for Y and willing to trade it for a minimum of Y coin. They would be able to sign a statement. If some off chain actor figures out how to get PEPE coin into their account, they can then claim the users X coin maybe also including a fee.

Nick

: sounds like a way to solve many user experience problems. Build a system where the users don't interact much with the guts of blockchains.

Zaki

: Ultimately you are describing a wallet that a market maker knows. I am skeptical of anyone's ability to build this.

Henry

: What is a wallet? One of the things that is interesting to do in this ecosystem is imagining you are looking at it and refocus your eyes and see things blurring into other things, and where are the boundaries? If you zoom in, you can see the explicit components and parts. But if you zoom out, how can these boundaries be reconstituted. What is a Wallet even? If you build in the capabilities of the market maker, maybe that is a part of this wallet assemblage.

Nick

: the common through line is we need to take a step back and re-evaluate the base assumptions of how we want to build blockchains.

Uma

: At succinct we are trying to do better more secure interop. We are building this very secure messaging protocol. We need

to run relayers across several different chains. Me as a fairly sophisticated user does not like to manage all these balances across different rollups. It's unrealistic to expect any one company or protocol to maintain these integrations. It feels as if something is broken.

I think the fundamental problem is that today transactions are very declarative. In this very multi-domain world, as a user, you shouldn't need to specify which rollups you want to trade on. I think an intent is saying, you're specifying what you want your outcome to be. I want my PEPE coin, and someone else figures out the best timing and execution as a sophisticated actor. With transactions, the onus is on the user. With intents, users express the end state they want.

Nick

: Seems that people who are working on intents have a good understanding of cross-chain.

Christopher

: Zaki and Uma did a great job of going over the practical UX reasons of why you design a system this way. Personally, I came at the concept of intents just from thinking about what coordination systems do. The OG coordination system is natural language. If you think about the Anoma vision paper, we used the example of hunters trying to encircle a deer

. In principle, if you are trying to encircle a deer what you need to communicate in order to coordinate is a bunch of preferences and plans. You are communicating something about internal states, what you want and what you are planning to do. Typically, in English this would be referred to as intentions, which is how I got the word intents.

Intents can seem nebulous, abstract, and like marketing. I'm sure it is that sometimes, as some words are. In general, intents are credible commitments to preferences over the state space of a system. And there are different state spaces which define the system

. Intents define some preferences a user has over some state space of future possible execution states of the system. Match user preferences and check constraints, so users' preferences are respected. If they said xyz in an intent, the system actually does that. We want this correct atomicity guarantee, just atomic in that either the intent is settled, and the user's expressed preferences are satisfied or not.

Our definition includes privacy

. The concept of the intent is useful because it allows you to describe the relationship of the user of the system and the system very well. The user may not care about the details of execution. In a system like Penumbra, users may care that the fairness of all intents settled in one batch get the same price. A property of an execution path, but not an exact one.

Account Abstraction and Cross-chain UX

Nick

: Now that we have the background established, what is the difference between intents and things like account abstraction or paymasters. Some people say limit orders are just intents. How are intents different to things that already exist?

Uma

: I spoke a lot about this in my research day talk. I think AA is this protocol that can help enforce very specific intents. I want a rate limit on a Smart Contract wallet. You are enforcing some preference over this state space. The smart contract wallet has logic in it to enforce that intent. In particular, SC wallets can enforce rate limits, social recovery etc. It has this concept of a paymaster that can help deal with gas payments for users. Fundamentally AA is a spec and a protocol in service of very specific intents, I think it's limited. 4337 is long and winding and complicated. Authors took 5 main intents and stuffed them into this ERC protocol. It's not a general system, it's very brittle. They worked backwards from how can I enforce these specific intents in a way that compliments Ethereum. AA does not help you solve the problem of I have ETH on Ethereum, I want the best price on PEPE. AA is a single domain protocol. A lot of what intents solve is dealing with multi-domain stuff that intents do solve. Intents are a very useful abstraction, even more so in the cross domain world.

Nick

: AA (account abstraction) is a limited subset of intents. Intents encompasses more.

Zaki

: (Eli Krenzke) One thing that may be familiar to DeFi savvy users is the concept of a liquidation. You have a vault on maker you locked some ETH and minted some DAI. You bind that vault to an intent. Someone has the right to take the ETH out of my vault and sell it to pay back the debt at some price.

There is this whole rich ecosystem of off-chain actors. Can we align off-chain actors with users goals such that we can make blockchain UX 100x better.

Nick

: OH: “Intents turn toxic order flow into non-toxic order flow, and turn bad cross-chain UX into good cross-chain UX.”

Henry

: The reason is that if you are in a mono-chain paradigm, your tx

specifies which execution you want to have happened, and it will all get executed at once. Within that execution, I am specifying very directly. In a cross-chain context, you have all of this asynchronous execution. So you don’t get the same kind of entire tx

succeeded or failed, and you locked the entire world to make it happen. The reason the intents/predicates solution appears is this is the way you can recover from the introduction to asynchrony.

Suppose I’m executing a tx

on Ethereum, in some sense I am paying too much. I am halting the entire world to get the property I want out of my tx

, I’m paying for way too much synchronization there. I don’t care if someone minted an Ape NFT at the same time someone did my swap. As a user, I can’t express this unless I pay everyone else to stop the world.

P2P network designs

Nick:

Now we have an idea of what intents are, what do we have to change in the way we build blockchains to make this possible? How deep does this change need to go?

Christopher

: Right, good question. One interesting aspect of the way intents are playing out at the moment is it seems like this frame is kind of inevitable. Ethereum was designed under the banner of a world computer. Its easy to underestimate the importance of that concept. Where it draws inspiration from, how it thinks about politics, building a hierarchy of different trust domains which settle to the root. The concept was very relevant to the structure of the ecosystem. It seems an intent system is going to exist in Ethereum or on top of Ethereum more broadly. People are going to use these systems when they have preferences. If you don’t need to come to agreement you don’t need a blockchain. I think the economic structure is inevitable. For us its important that we end up with an intent implementation that is compatible with privacy and doesn’t require that information is revealed to the world. I think it’s essential if we want these systems to work. Depending on how you define intents, then privacy becomes part of the definition.

The EVM is a specific implementation choice. I see something like the EVM like a CPU, it’s virtualized. It has the relation to an intents protocol, as does a Haskell program to an x86 chip. One thing to note is that it is not easy to make EVM privacy compatible.

Also, what needs to change a lot is p2p network designs. If you zoom out of blockchain literature, I think the weakness is p2p designs. Its clear how to do many things like cryptography, but I think p2p networks have been neglected. The state of security is not very good right now. Structured networks are when you have ideas of who is connecting to who. Unstructured nodes are like DHT. All p2p networks in blockchains I know of are “all blockchains nodes receive all messages”, which doesn’t make sense in a heterogeneous security world. You need to exist in between these structured and unstructured designs. It needs to be designed from scratch. See Recursive internetwork architecture as an example of a research direction.

UMA

: Interesting, you think p2p layer needs the most work. Do you think a design or proposal for a SUAVE-like structure where you have one network surfacing preferences or intents for all domains, is this untenable because of the amount of throughput or volume to process all intents and domains is not possible.

Christopher

: To caveat this, I am not an expert on SUAVE. Perhaps the version I understand is not the one true SUAVE. If SUAVE is one specifically logically centralized location, yes, I think that topology is untenable because you are paying for this logical centralization that you don’t actually need. Many intents have nothing to do with each other, dealing with different security domains, different users, capabilities. If you make them interact, you are paying for the intents to be broadcast to all SUAVE validators, and they will be limited by the throughput of the system and makes it an easier adversary target. If you think about practical applications it just seems weird to me; I want to have my local event, and we create our own intent settlement for the event, why would I send my intent to some global intent matching system.

I think what SUAVE actually proposes to build is a faster system for Ethereum of ways for mapping intents to the EVM. It’s not going to be the one true place that all intents go as I understand the economics. Maybe SUAVE has a nice language and network that is EVM compatible. One practical challenge in how we have thought about things, it is really hard to make long-term privacy EVM compatible. Privacy is not a feature you can add onto systems after you design them. Aztec has decided

not to try and build a private EVM as an example. SUAVE temporarily relying on TEEs is helpful.

The reason I think it's important to have a general p2p protocol, is that it will allow these systems to compose more generally. There are many different separate unstructured mempools. There are specific lines in between like relayers, bridges, or nodes, and that is really just a Venn diagram. You have all of these mempools where people send messages to one mempool that don't impact another and vice versa, leading to partial overlap. If we design p2p well, we can get a protocol that solves for this. Everyone can configure that the way they want, an intent (criteria rules). We aim to work with Flashbots on SUAVE and anyone else who wants to standardize on this layer.

Uma

: I like the abstraction you mention; shared overlapping mempools.

Solvers

Nick

: In these intent architectures there are some new concepts that don't exist today; an actor called a solver, there are these proofs to settle intents, there is this notion of a credible commitment what does that mean? Can someone unpack these details? What is happening, who are the actors in the system, and the different moving parts?

Uma

: A super simple example. A cross-chain RFQ system looks like a proto-intent system. I'm a user I want some OP token on optimism for my ETH, I request a quote and a sophisticated actor is doing a tx

on Optimism and then taking my ETH on Ethereum, and maybe they participate in some auction for the right to fulfill my quote. Some of these already exist in terms of off-chain auctions.

Christopher

: The solver part of the question is helpful for understanding the intent framing. If you take intents to be preferences over the state space of the system. The search problem is, but you don't have polynomial time algorithms in the general case to solve these problems. Part of this problem is unbounded search. You do not want to do this in replicated computation. In our lexicon, solvers are the entities doing the search, they have some choice over execution paths. If you define your fairness criteria clearly, then solvers are entities who you are paying specifically for doing the search. Solvers are basically fungible, you are creating a market for compute with some resiliency properties. Because you can verify the results of the computation, you don't need to trust the solvers at all. Solvers are just doing the search problem in the purest definition.

Nick

: How do I know that a solver got me a good deal or achieved a fair price? Is there an auction mechanism that guarantees this.

Christopher

: I don't think there is a universal mechanism that gives you generally the best properties; RFQ, OFAs, etc. Intents are cheap, so you can send a lot of intents and change the intents over time with some reference clocks (signatures from a validator set). Depending on time preferences, start with high price you like a lot and eventually fill my intent. You can also do something where you restrict the role of solvers to only compute first by committing to an ordering. Fairness criteria could be Pareto efficiency improvements or other welfare metrics localized to a community. In this case because you have separated the roles, validators are threshold decrypting or Witness decrypting the intents, so solvers don't have a lot of freedom to optionally include other things.

Henry

: For Penumbra we have a different approach to the same goals. Let's try to solve a problem and stumble backward into a good idea. We have two different intent systems, one is never touching a chain, which we use to paper over the complexities of having a UTXO like system for managing notes or other things. In a send tx

within a simple account based system you can debit and credit. In a shielded system, you say I am consuming these state fragments. Planning out your tx

involves UTXO management, which sucks for developers. We ended up building proto or trusted intent system, someone can specify a high level what I want this tx

to do. Our own client stack can translate that into "this is what I want done."

If you think deeply about any one component of these systems, it winds up having similar problems inside that microscale as the full system writ-large.

Intents and the modular stack

Nick

: One topic I want to make sure we touch on quickly, the overlap between intents and modular blockchains. At Celestia, we believe this modular blockchain architecture is going to be how we scale these systems and solve many core problems of blockchains. Intents are a big part of solving this. For me, what jumps out is a modular blockchain future, one where the number of chains proliferate.

It seems that intents would be necessary in this world. If you are interacting with apps living in domains if you want to compose them it is difficult without intents. The complexity explodes. You need to off-load the complexity to more sophisticated actors. Intents are not something that's built into Celestia DA, but curious if you see any reason to have intent style format for Celestia?

Uma

: I think having this super modular stack solves a lot of problems and has many pros, cons are because it's way more fragmented users have to keep track of stuff across different rollups. With the rise of the modular stack, this has become more popular to discuss.

Zaki

: I think one of the things that has become an increasing part of my framing of blockchains; there are probably only 2 layers of blockchains which accrue value. We sell basic commodities

for example DA, execution in shared state with things that are valuable, and artisanal organic non-toxic order flow

. Celestia is canonically a vendor of a base commodity and potentially a shelling point for shared stater execution that might be valuable.

The real goal is to build the farmer's market to artisanal organic non-toxic order flow

. My general view of this is intents are already here; Cowswap, 1 inch fusion, Opens sea order book, MEV-Share. Many people who have used blockchains have interacted with intents already. We keep building systems like this. Intents are going to be a big part of successful systems built on top of a modular architecture, with the goal being elevated to that organic order flow.

Christopher

: Another common intuition, is to separate out the functional components that different parts of the distributed system are providing and come up with interfaces around those components that define them in a sufficiently general way where you can put together these components like Lego blocks. I think if there is one thing you to make sure that you do it is to define interfaces that specify at the correct level of abstraction; not too specific in such a way that restricts people who implement some subcomponent. You want a declarative interface that defines what you want the subcomponent to have. Denotational Design (Conal Elliott) provides a methodical formulation of what it means to design a system this way. At every layer you define what you want an underlying protocol to do as an observer.

The way the Anoma architecture thinks about Data Availability is that a user wants data to be stored for some period of time. The consumer of that interface has a DA intent. They want DA in a way that's compatible with their preferences. They might want the data to be stored for a specified time. The providers may be the Celestia validator set or the Ethereum validator set, whom provide DA for a fee (readily available by most blockchains). If you architect an intent-centric blockchain in this way, you get intent-centricity at every layer.

Nick

: So you are saying there could be an intent layer for each service, including DA? You set your preference for a security threshold?

Christopher

: The interface pattern holds generally. Designing things correctly means Anoma and Celestia will be compatible without even trying. Talking about things like dependency inversion or something, I think we have symmetries in how we think about modular design. Design a maximally general interface for something like DA. You can parameterize who, what, and how long data is stored. But you end up with compatible interfaces magically; i.e., I don't need to go talk to Celestia. Having compatibility which doesn't require people to talk to each other is a huge boon.

Intents already exist

Nick

: One last question. Zaki gave an outline of a few systems that are live right now that have some version of intents

implemented. What is the current state of intents; different projects building them?

Projecting three years into the future when this stack is built out and people are actually using it, what does it look like and what world will we be living in? Do I even open my wallet, am I switching chains? Is it one portal? What does this look like if this all works?

Zaki

: My suspicion is that intents are the capstone of the last 10 years of blockchain infrastructure building. We have had a lot of unsolvable problems; consensus, DA, bridging, what should your language for Smart contracts be? All this concrete progress has been made. Especially during the pandemic period where we had many users, it became clear where this system breaks down.

I don't think people will do everything with intents. Sometimes it just will not be worth it, especially if you have one of one type of things. It's easy to specify a path. But the future wallets will be able to abstract over many workflows that confound users today. In an intent world, you don't need to know whether the NFT you want to buy is on a specific security domain. The intent world is going to abstract over and commoditize

the differences between ecosystems. Most users will just open up a wallet that speaks intent language and go ahead and buy the NFT they want without thinking about the path.

Uma

: I think the state of intents today is already here. There are a bunch of apps for app specific intents. I think there will continue to be more app specific intents. At Succinct, we care about making the interop UX much better. We want users not to even think about what a bridge is. The step to building is having another proto-intent or bridge intent system, Hopefully we can talk about a more general abstraction. There is going to be some needed coordination. I think the general solution will have many benefits, like decentralization.

Christopher

: I think some parts of the existing system are inefficient in ways that don't matter much but also some ways that matter a lot, like the p2p systems. I think the nice thing in thinking about systems like this is that if we do it well, it ensures a sort of future compatibility.We have valuable state on current blockchains that will want the future world to reference that state and build upon it. That will be rendered possible by building these more proto-intents systems.

One thing we are working on is a general, abstract definition for intents. The Turing machine is a nice abstract definition for what a computer does, for example. We are trying to come up with such a general thing for an intent system which includes privacy. Its more generally expressed as information flow control. Defining what it is, an intent-centric system must be rendered as correct. Maybe the optimization frontier will move to algorithmic choice. The only thing I'm specifically worried about is that I think it's difficult to make systems compatible with privacy. If you embed transparent verification as a specific design assumption, it may not be compatible with privacy preserving systems. Important to think about at this stage.

Nick

: Closing thoughts, anyone?

Henry

: I don't want to shill too hard, we are building some cool stuff if people want to check it out. I think what people should take away is that intents are already here in these different manifestations. Also, it's interesting and important to look at systems both in a component by component approach and a holistic approach to ask what are the boundaries between these components. You can see intent systems already in place, the thing is to take the raw material and flesh it out and chisel away at it, so we get this beautiful future.

Zaki

: I do think this does represent a pretty big change over like what layer one protocol designers have considered their priorities.

Christopher

: I would second both of those sentiments. Maybe he won't shill penumbra, but I will. It's a great solution optimized around privacy preserving trading but designed to such a level of precision and a careful reflection of what the product does, it winds up as this specific carnation the illuminates the whole concept.

One reason we find intents helpful is they provide a good way of framing the general problem. What is it these systems are supposed to be doing? Intents don't provide a specific answer to these questions. If users don't know what they want, that is not a problem that economic problems solve. I think as we think about things in this intent-centric way, it can give a useful lens into what part of the stack are under prioritized- VM design and p2p design.

What does privacy mean in an intent-centric world? Examining that question is also important and helpful. I just hope we

think about the components clearly, that we keep talking about things and come to a good social consensus that achieves an appropriate distribution of labor.

Zaki

: I just want to say when I initially was thinking about this. I questioned if the privacy component was essential and whether we could roll out the practical use cases with privacy. You want to reveal some information with your intent, but not all of it. If you want to not have highly interactive processes where a user's device has to be online interacting with its counterparty, you need a non-interactive system with privacy. I am convinced you need privacy when building these systems.

Uma

: Not too much more to say other than the most interesting thing to say is research and community meets UX and I think that is one of the biggest problems in crypto. People who normally don't talk have started engaging. At a meta-level, I hope that continues.

Nick

: I am grateful we had you here to explain this. There is much more conversation to be had on Twitter. We will be having a ton of intents content this year at modular summit in Paris. We will continue the conversation in Paris.

{fin}