Preface

Below you will find slides and talk track notes from a recent presentation given at the Decentralized credit network(DCN) workshop at AFT 2023. The workshop was organized and moderated by Andrew Miller & Aniket Kate.

This workshop aims at bringing academic and industrial participants together to discuss structures, security, and privacy for credit networks and foster future collaborations towards more inclusive and secure decentralized credit networks. The goal is to offer a platform to discuss the structural intricacies, security against Sybil attacks and node compromises, and privacy enhancements within credit networks.

Slides: https://github.com/0xapriori/Slides/blob/main/AnomaApplications.pdf

Acknowledgements

: Thanks to @degregat, @isheff, @cwgoes, and @Ajmaq for feedback in preparation for this presentation.

Anoma Applications

[

1354×760 14.8 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/2d9f56053e3b7bbd8f793646bac1e2e33064c8c7.png)

Good morning, my name is Apriori, it's an honor and a privilege to be here. Today I'm going to talk aboutAnoma.

First, before we begin, I'd like to thank a few people. Thanks to Andrew Miller and Aniket Kate and the AFT conference organizers for this great event. Thanks to Christopher Goes, Ethan Buchman, Informal Systems, Julio Linares, and the entire Heliax team. Without them, I would not be here today.

Overview

[

1338×448 13.9 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/a487a10b2a632af1e401c54c468c7bb3be370ad1.png)

In this talk we will progressively describe Anoma Applications. The talk is broken into three parts.

A few caveats

before we begin.

- This is not

the true holy version of Anoma.

- This is

a synthesis

of the current working specs, conversations, and ideas from the research forums.

Part 1.

[

1340×750 164 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/73bf4fba355dbe9474fa9c21d2b883ac59b106c4.jpeg)

Application Definition

[

1336×550 27.8 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/c161eb8d2909defaf9c685be5d07345096519e73.png)

Applications may be bundled with the computer and its system software or published separately and may be coded as proprietary or open-source.

The term “app”

often refers to applications for mobile devices, such as phones.

Examples of Web 2 Applications

[

1312×704 41.7 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/850066c34776f930f5fc7c93c0a3f8bb44129ac7.png)

Here is a list of some of the applications that you may use today. Many of the applications listed here have strong network effects and thus own a significant market share of the categories they compete in.

Limitations of Web 2 Applications

[

1328×716 21.2 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/5251969139b0692044af166d54241e978bbfe240.png)

Drawbacks include high switching costs, little to no privacy, censorship, centralized, and rent-seeking behavior. One question may arise; given these drawbacks, what motivates or keeps users “locked-in”?

Affordances & Don Norman

[

1328×672 35.3 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/4e231591a2eaa3e037cb20621a22f6ffe25b0fe4.png)

[Affordances

](https://www.interaction-design.org/literature/topics/affordances) represent the possibilities in the world for how the agent (a person, animal, or machine) can interact with something.

Psychologist James Gibson coined “affordance” in 1977, referring to all action possibilities with an object based on users’ physical capabilities. For instance, a chair affords sitting on, standing on, throwing, etc.

Don Norman later (1988) introduced the term to the design community modified the meaning slightly to make it more appropriate for use by designers. For example, Don Norman defined affordances as perceivable action possibilities – i.e., only actions which users consider possible. So, designers must create objects’ affordances to conform to users’ needs based on these users’ physical and perceptual capabilities, goals and past experiences.

Clear affordances are vital to usability. Users will map the possibilities of what an object does according to their conceptual model of what that object should do (e.g., inserting fingers into scissor holes to cut things). If the affordances of an application are apparent, this can often lead to a great user experience.

Examples Web 3 Applications

[

1334×738 40.3 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/1d0e10791b518c14c7bb3b6b95e1c7ace21f1a7a.png)

With some context, let’s examine these Web3 applications by category. While Web 3 applications are interesting, DeFi so far has proven to be the dominant category. Outside of DeFi and infrastructure applications there is still much uncharted territory. In fact Crypto’s killer application is barely understood. But, we’ll get to that later.

Favorable Properties of Web 3 Applications

[

1334×534 26.1 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/fef874889fe7d5b5212921e899833ace8aac740e.png)

These are favorable properties, now lets look at some limitations.

Limitations of Web 3 Applications

[

1328×692 27.2 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/7abac9c3fcf8e79fb6f12060595c2d8d6022a05d.png)

- High Cost for users and developers
- expensive block space, pay for liquidity
- Security vulnerabilities
- smart contract hacks, phishing scams, social engineering
- Limited Composability
- liquidity fragmentation across domains
- Best UX requires trust
- centralized sequencers, off-chain intermediaries (wyvern), Centralized Exchanges
- High onboarding costs
- steep learning curve - time commitment
- Isolation
- difficult to compose with the “real world”

Is there a way out?

Part 2.

[

1304×756 213 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/cc8d4d345dcc58dae4e30652d87b733998cf7098.jpeg)

There are many misconceptions about Anoma. Today, I’m going to create some more.

– @apriori

Outline

[

1306×624 15.2 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/691bc5a540893d1672507a7cdaac14dd600061fe.png)

Now that we’re warmed up we will talk about Intents first. Next we will discuss Anoma, the network, the protocol, and its affordances.

Intents

[

1328×528 33.4 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/193c9638cfe7fce6f702db34901105b62c4ca689.png)

Recently There has been much conversation in the community with respect to the term intents. What are intents?

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.

-@cwgoes

Anoma the network

[

1300×664 45 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/d293c2258fbb7eee168706e98779776f463df453.png)

Anoma

is

an intent-based network of autonomous communities. Communities can participate in the Anoma network by running the Anoma protocol.

The current economic network and organizing paradigm restricts autonomy and limits freedom. Communities have two options: to give up autonomy for the sake of interoperability - use infrastructure, protocols, and currencies operated and controlled by someone else, and thereby participate in wider economic networks - or to give up interoperability for the sake of autonomy - opt out of the shared infrastructure and produce everything themselves. Anoma aims to offer a third way - one which preserves both autonomy and interoperability.

Network Comparison Visual

[

1098×722 185 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/ee0bfcdc4b7aa1b3577a4c88b8896a96b9b6dc9d.png)

In this example you see network validators represented by dots. In Ethereum all of the validators run a consensus clients and an execution client. They have a view of the beacon chain and the EVM. All of the Validators are required to participate in global consensus. This means that applications and users always pay for global consensus.

In the Anoma network, validators do not necessarily share the same global view. The Network is composed of many fractal instances which can interoperate. These instances can be persistent or spun up at runtime.

Fractal Instances

[

1406×966 133 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/067f9576f0e807d914b528edb0cdd0368b07a14b.png)

Fractal instances are not

like build your own blockchain. They are a different thing. A better way to think about fractal instances is as consensi on demand.

Currently, the typical user interaction with the blockchain is inverted. You first choose an application which will be hosted by some consensus provider, then you decide what to do. You make the choice of consensus first and action second. Fractal instances invert this, you make the choice of action first. According to the action you are taking, you decide what type of consensus to use.

For example, if you are sending some kind of payment within your organization, you only need organizational consensus. If you are sending the payment across a federated group of organizations, then you need their federated consensus. If you are sending some kind of global payment to someone across the world whom you do not trust, then maybe you need global consensus. However, we want to derive what kind of consensus you need from what you are trying to do.

Anoma the protocol

[

1312×698 46.3 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/ab71148e6e9b03ad30da739e6c6ff23b5e3e0b9f.png)

In the counterparty discovery phase, network participants examine and match compatible intents, forming transactions which enact particular state changes. Transactions then enter the settlement phase for ordering, execution, and confirmation by consensus, after which users can read the updated state.

Intent Lifecycle

[

1336×754 152 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/a5aaa0a3e11745e4cdfdf2ee1003cbac20a883af.jpeg)

Here is a representation of an intent lifecycle. We are not going to spend too much time on this, as it's the most common discussion within the discourse related to Anoma. I refer the listener to the Anoma white paper for details.

Anoma Affordances

[

1318×538 22.4 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/92dd39a0ab2333bad3431b9f07ee9311167df783.png)

For applications, Anoma offers developers and users three key affordances.

Permissionless Intent Infrastructure

[

1326×684 37.8 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/9635cae47cfbd3ef39cf10cd159154c5002c38f5.png)

Anoma supports programmable intents with a general protocol. This means that developers creating new applications don't have to worry about finding or building extra components like;

- validators,
- solvers,

- indexers,
- or any specialized infrastructure.

Developers just need to decide on intent formats and solver algorithms. Each application will likely have specific types of intents that need to be solved. Anoma provides a permissionless substrate for decentralized solving

Information Flow Control

[

1292×570 25.6 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/662292475d52fdb9e4f49cb6f5947be9ca0f668a.png)

This is done with Taiga, a cryptographic library for privacy preserving distributed applications running on Anoma. Taiga will provide private settlement with recursive zero-knowledge proofs. Private counterparty discovery is still an area of active research; including TEEs, MPC & FHE.

- See this awesome blogpost ‘Privacy In tents” for more details

Intent Level Composability

[

1294×416 18.9 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/16d4d87d40353a1039edff1ceb670c4c20dc0e4f.png)

All applications written for Anoma can be composed at the intent level, meaning that intents for different applications can be composed together and executed atomically, without any additional effort or prior coordination on behalf of the application developers.

Example of Intent Level Composability and Solving

[

1126×688 168 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/a4958020e7ce4c0122049170be25bb4c7b4b7412.png)

Part 3. Synthesis

[

1320×752 242 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/c3174bde5eda92af22bf5ac2acc7ff78e7899b86.jpeg)

What?

[

1286×480 30.6 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/c17fbdc57fcf49b09ccd109a4bc3a57a2cdf4344.png)

An application is a set of resource logics (predicates) and solver algorithms

- Resources are the atomic units of state
- Resource_Logic

specifies under which conditions Resources that carry it can be created and consumed. It is defined by its Predicate

and its Arguments

Resource

data ResourceBody = ResourceBody { resource_logic :: ResourceLogic, prefix :: [ContentHash], suffix :: Nonce, quantity :: Natural, controller :: ByteString, TerminalDAG ExternalIdentity

[

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/5f4f394634ec85bb545877ed3f016b73f63ce09d.png)

This diagram aims to show how Resources decompose into their components. All Fields consist of a content hash, which provides content addressing for all elements of all layers.

The Resource management system can be implemented as a UTXO or account model, or both. That is up to the particular developers and what they want.

Novel Applications

[

1202×468 19.7 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/d31741cd5d69ee67bf48fac1a6c0219829d68025.png)

Do we see any examples ofscale-free money today or reasonable approximations? Let’s take a look at Circles Garden.

See this book

:

- [Debt, The First 5000 Years

](https://files.libcom.org/files/__Debt__The_First_5_000_Years.pdf) by David Graeber

Example; Circles Garden

[

1332×744 111 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/b2130b6d25ad5f29218430fbe4c1cfee4d7420ab.jpeg)

The Circles Garden system architecture has multiple intermediate services to interact with the Blockchain world to overcome different limitations:

Relayer - The Relayer pays for the transaction fees on behalf of the user through meta-transactions (see ERC20 specification) to the Gnosis Chain. It pays for the Safe deployment and the gas fees for all the users of circles.garden. Therefore, the relayer can be used for controlling expenses since writing in the blockchain is always done through this service.

The main bottleneck is scalability. There is only one relayer, which means, this service oversees all the transactions for every user of circles.garden. If there are many transactions asking for payment, these get added to the queue, and worsen the user experience because this translates in longer waiting times (delays).

Circles Entropy on Anoma

[

1224×748 149 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/ce9514bade29e62e06aa2077e225bbb23aeb32b6.png)

Anoma is designed as a unified system, all nodes run - validators, gossip nodes, solvers, edge clients, etc. - just separate configurations to enable or disable processing, storage, signing, etc.

The Anoma node software internally handles P2P network connections, fetching & caching state, verifying signatures (e.g. of validators, running light clients), etc. - no interface should need to implement these, they should just use the local API provided by the node software package.

What else can you build?

[

1264×634 19.4 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/1475cd6f75f30a826f0ce41d5485373696211d4a.png)

Dominant Assurance Contracts

[

1268×652 45.8 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/fb1206e6f02762f901cc4eff99afd842d8fa9b0a.png)

Some Public goods can be created privately by profit-seeking entrepreneurs.

Dominant Assurance contracts

- an entrepreneur can design a contract where the equilibrium has agents contributing to produce the public good as a dominant strategy;
- On the supply side, potential producers of public or private goods, with high upfront cost and lower marginal unit production cost, can craft proposals for what they would produce, with what required upfront cost and individual benefits (for the private/hybrid goods).
- On the demand side, potential consumers of public or private (hybrid) goods can craft proposals for what they want to be produced, with what they would individually be willing to pay.

There is some similarity to existing concepts such as buyer's clubs - consider, for example, a group of DIY enthusiasts grouping together to contract a Shenzhen manufacturer for a large DIY cellphone component order, or a community grouping together to contract a steward to purchase and operate a community maker space.

- Other advantages: Some empirical analysis to make the claim that crowdfunding is indeed a signal for some types of VC investing. Hence, Public Signal.

See these papers for more details

:

- [The private provision of public goods via dominant assurance contracts

](https://mason.gmu.edu/~atabarro/PrivateProvision.pdf). Tabarrok 1996

- [New Technology Assessment in Entrepreneurial Financing - Can Crowdfunding Predict Venture Capital Investments?

](https://arxiv.org/pdf/1608.07182.pdf). Kaminski, Hopp, Tykvova, 2018

- [Jump-starting coordination in a stag hunt: Motivation, mechanisms, and their analysis

](https://arxiv.org/pdf/1601.03162.pdf). Avramopoulos 2016

Time Banks

[

1272×674 55.3 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/7f22327c37d5c300a9dc331ba3bb5bd2b328c251.png)

Time banks allow people to coordinate at a local scale. Individuals sign up to participate and begin “banking time” or earning “time credits” by providing their skills for someone with credits. There are a few different frameworks for time banks including the most popular neighbor to neighbor one just described, which relies on the earning and spending of time credits.

See this paper:

- [‘With a little help from my friends.’ Evaluating time banks as a tool for community self help

](https://www.tandfonline.com/doi/abs/10.1080/0269094032000111048c). Seyfeng, Local economy, 18(3), 257-264, 1998.

The End

[

1264×744 23.8 KB

](https://europe1.discourse-cdn.com/standard20/uploads/anoma1/original/1X/a0b193340d4da67da5a4bc9a3f00fa683bc48d47.png)