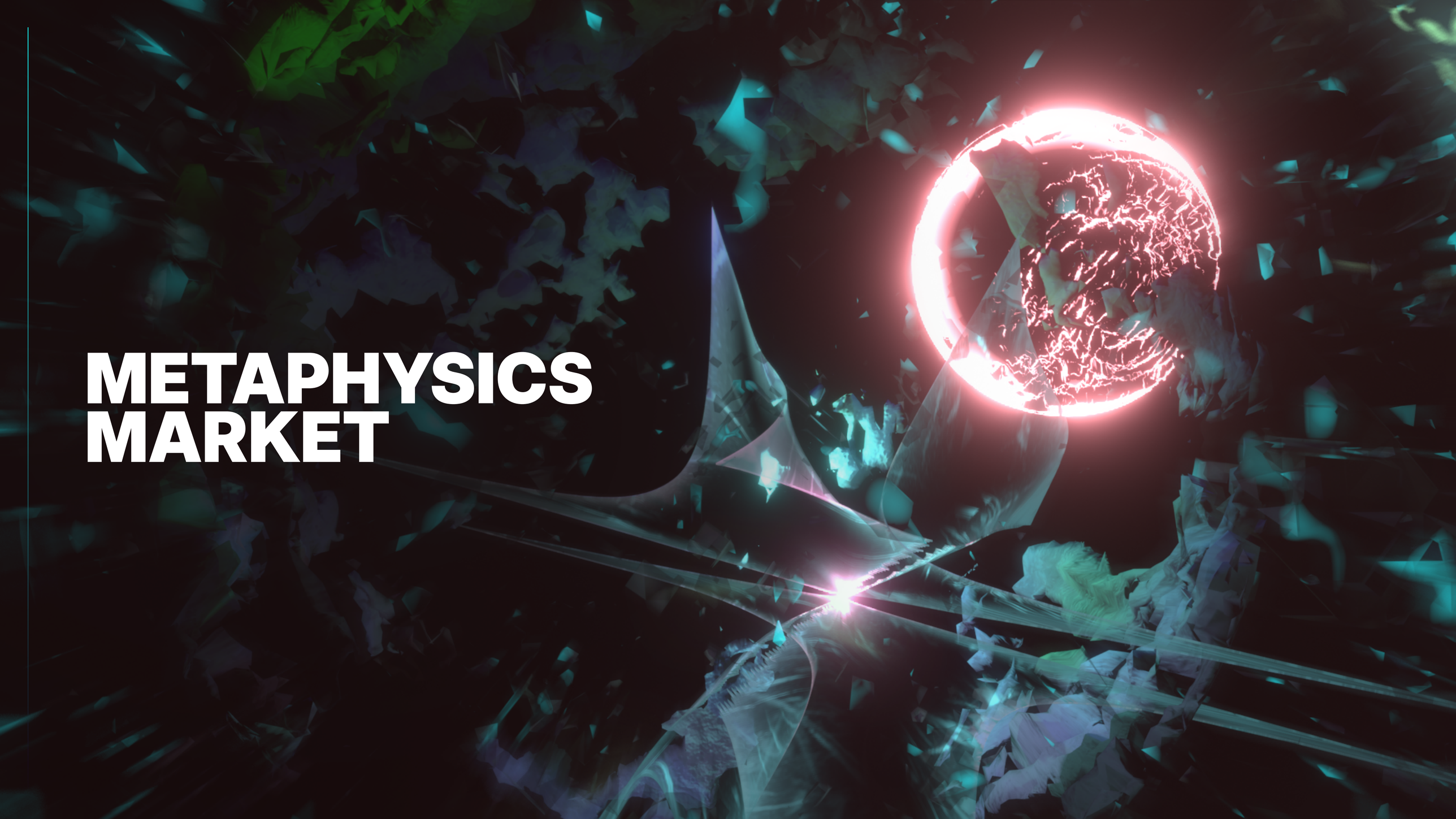
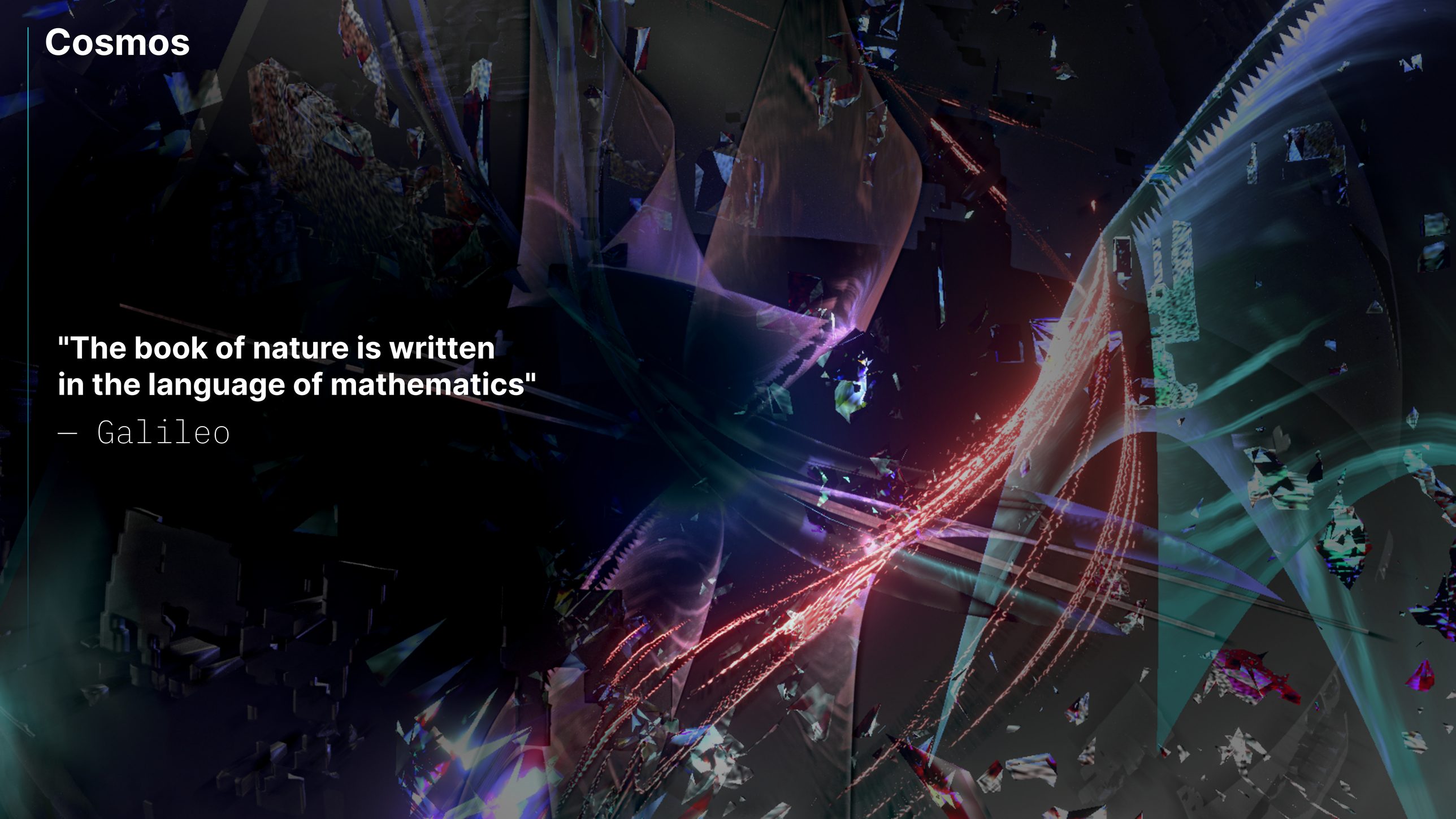

METAPHYSICS
MARKET

Cosmos



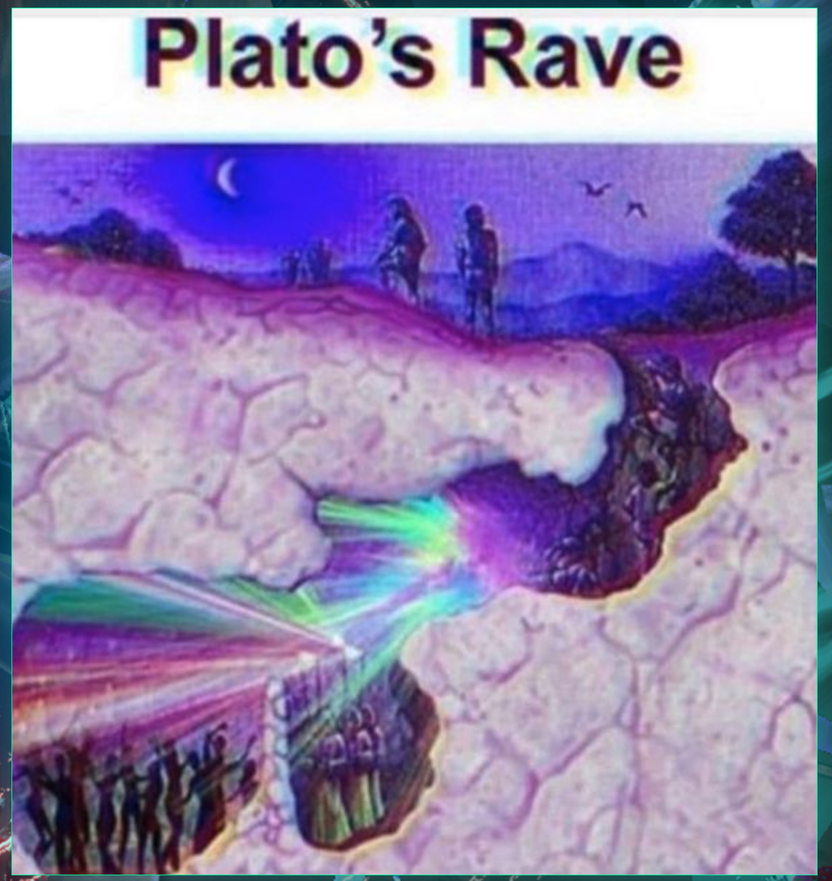
"The book of nature is written in the language of mathematics"

— Galileo

Cosmos

"The book of nature is written
in the language of mathematics"

— Galileo

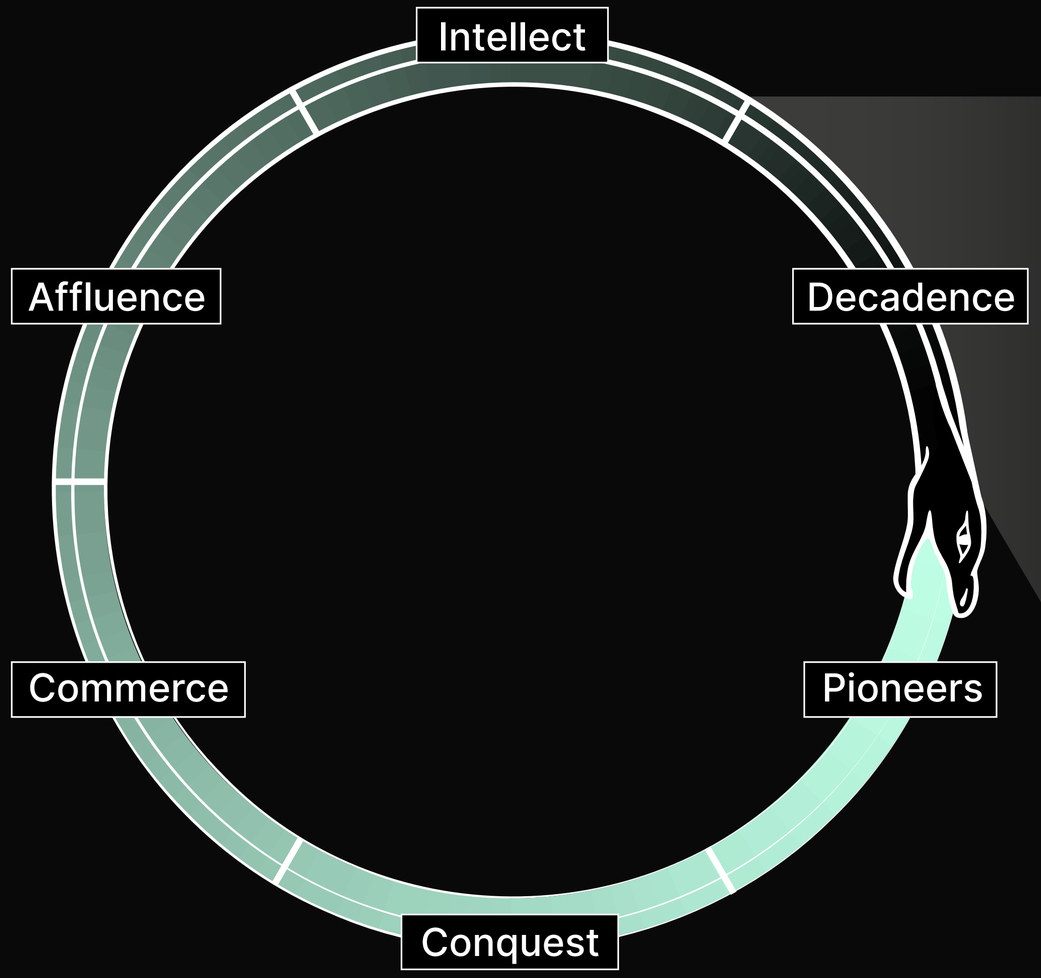


Cosmos

“The universe smiles upon encryption”

— Assange

Nature is Cyclic



undisciplined, over-extended military	massive disparity between rich and poor
desire to live off a bloated state	obsession with sex
bread and circuses	debasement of currency

Nature is Cyclic

“We can win a major battle in the arms race and gain a new territory of freedom for several years.”

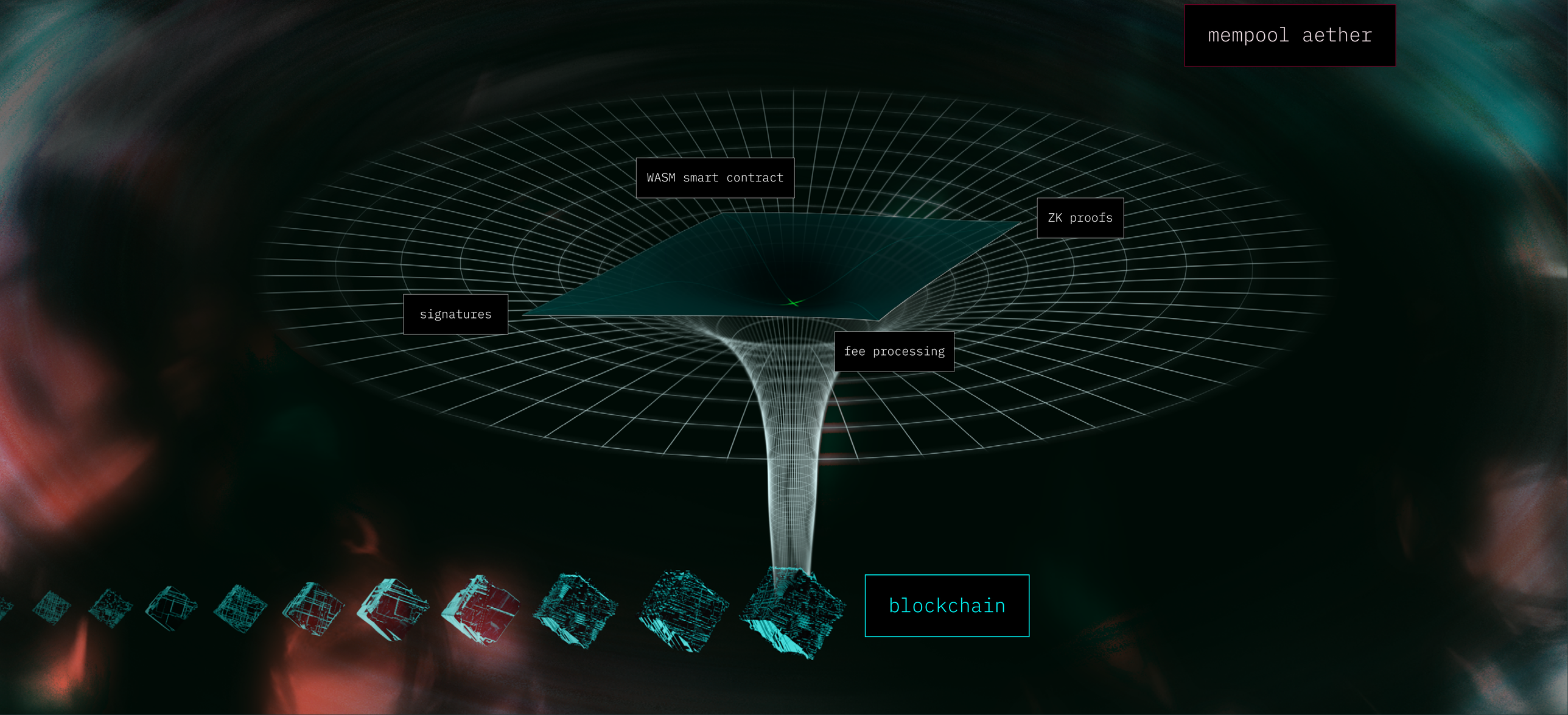
— Satoshi

Cyperpunk Methodology

DarkFi is an L1 for anonymous applications based on zero-knowledge, multiparty computation and homomorphic encryption.

Cyperpunk Methodology

Smart contract architecture
Transaction validation

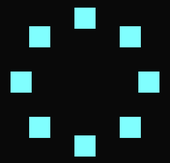


Cyperpunk Methodology

Core primitives

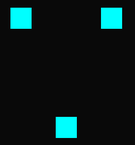
Zero-knowledge proofs

Prove something is true without revealing anything else.



Multiparty computation

Distributed computation on hidden values.

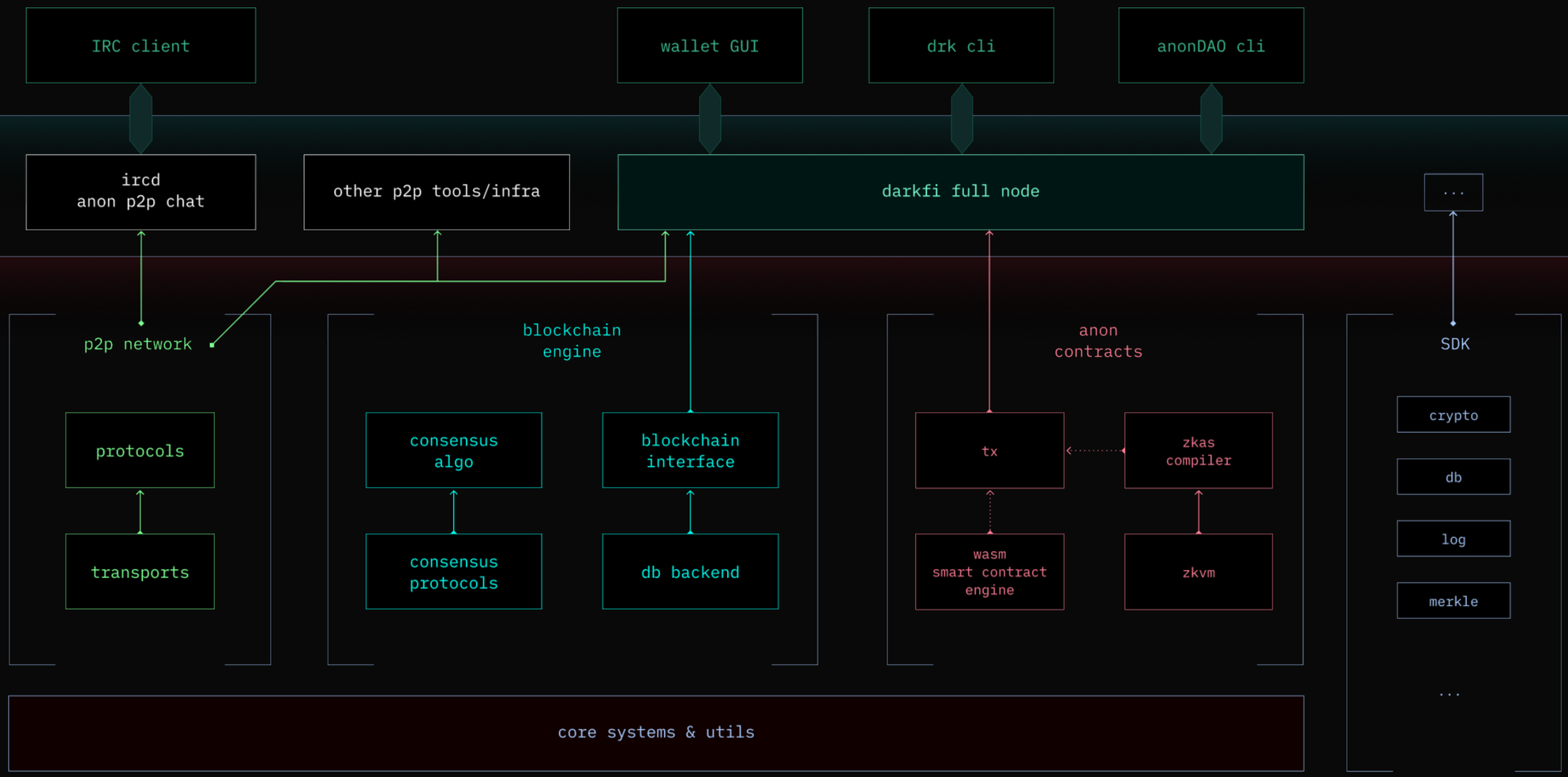


Homomorphic encryption

Encrypt values and perform functions anonymously on ciphertext.

Full Stack Agorism

Architecture overview



Full Stack Agorism

Anonymous coordination

ircd

```
1.darkfi        n/a
  weechat                                                                          jstark
2.darkfi-all                           | execution.
3.  #dev      12:22:34        camacho | aha ok
4.  #math     12:22:46        camacho | Please revert it as this breaks compatibility with the deployed testnet
5.  #design   12:23:40        camacho | Although maybe better if it's just configurable through the toml
6.  #markets  12:23:42            leo | should start new testnet, cause stake should sum to airdrop at genesis
7.  #philosophy 12:26:16          leo | with bootstrap time in the future.
8.  #memes    12:27:07        camacho | Things should be working once we announce the testnet
9.  #random   12:50:24      upgrayedd | gm hackers
              12:50:32      upgrayedd | pushing a cleanup commit
              12:50:45      upgrayedd | leo: 2 things
              12:50:59      upgrayedd | first no need to delete /tmp folder contents, they are getting deleted anyway by
                                      | the system
              12:51:24      upgrayedd | couldn't you read the leaders history from the node log? why create separate
                                      | file?
              12:51:59 commits-notifier | @aggstam pushed 1 commit to master: 4dadf292ec: fmt, fixed broken imports,
                                      | general cleanup
              12:57:24 commits-notifier | @aggstam pushed 1 commit to master: 5044141b24: fmt
              12:59:32            leo | NO, it has to be deleted.
              12:59:35            leo | NO, i can't
              12:59:59            leo | those files aren't for leaders history only
              13:00:32            leo | there used by analytic scripts.
              13:04:20      upgrayedd | yeah I got its usage, just saying that it could be done using patterns read from
                                      | node log, not separate file
              13:04:31      upgrayedd | why a /tmp file has to be deleted?
              13:04:40      upgrayedd | you can distinct them via run
              13:07:40      banu_musa | easier than parsing the log that can change, will be trimmed when done with
                                      | analytics.
              16:49:04             -- | irc: disconnected from server
              16:49:14            --> | jstark (anon@dark.fi) has joined #dev
              16:49:14             -- | DarkFi has changed topic for #dev to "n/a"
              17:06:55         jstark | gm
              [17:07] [9] [irc/darkfi] 3:#dev{1} [H: 1(9), 2]
              [jstark]
16:58:29 [DEBUG] (3) net: reading magic...
16:58:29 [DEBUG] (4) net: Received Pong message 49ms from [Url { scheme: "tcp+tls", cannot_be_a_base: false, username: "", password:
None, host: Some(Domain("alpinewg.parazyd.org")), port: Some(25551), path: "", query: None, fragment: None }]
```

dao-cli

```
Usage: drk dao <COMMAND>

Commands:
  create     Create DAO parameters
  view       View DAO data from stdin
  import     Import DAO data from stdin
  list       List imported DAOs (or info about a specific one)
  mint       Mint an imported DAO on-chain
  propose    Create a proposal for a DAO
  proposals  List DAO proposals
  proposal   View a DAO proposal data
  vote       Vote on a given proposal
  exec       Execute a DAO proposal
  help       Print this message or the help of the given subcommand(s)

Options:
  -h, --help  Print help information
bash-5.1$
```

dark-otc

```
Usage: drk otc <COMMAND>

Commands:
  init     Initialize the first half of the atomic swap
  join     Build entire swap tx given the first half from stdin
  inspect  Inspect a swap half or the full swap tx from stdin
  sign     Sign a transaction given from stdin as the first-half
  help     Print this message or the help of the given subcommand(s)

Options:
  -h, --help  Print help information
bash-5.1$
```

tau

```
bash-5.1$ tau show project:darkfid
 ID  Title                                                  Status    Project   Tags
---- ------------------------------------------------------ --------  --------- ------
 19  Finalization queue                                     open      darkfid   +dev
  0  Placeholder for function to calculate tx inclusion     open      darkfid   +dev
  1  task commit to the encrypted note to ensure its valid  pause     darkfid
  3  infra for jsonrpc authentication                       open      darkfid   +dev
 26  wallet infra for consensus coins                       open      darkfid   +dev
bash-5.1$
```

Full Stack Agorism

Testnet V.1

```
darkfid
    Outbound
>>          Null
            tls://node3.testnet.dark.fi:8342 (no remote id)
            tls://node2.testnet.dark.fi:8342 (no remote id)
            Null
            tls://faucetd.testnet.dark.fi:18342 (no remote id)
            Null
            Null
            Null
    Node 3(Offline)
    ircd
        Inbound
            tcp+tls://127.0.0.1:59900 (no remote id)
        Outbound
            tls://alpinewg.parazyd.org:25551 (no remote id)
            Null
            tls://irc0.dark.fi:11001 (no remote id)
            Null
            Null
```

```
Hosts:
      tls://faucetd.testnet.dark.fi:18342
      tls://node0.testnet.dark.fi:8342
      tls://node3.testnet.dark.fi:8342
      tls://node2.testnet.dark.fi:8342
      tls://node1.testnet.dark.fi:8342
```

```
16:59:53 [INFO] consensus::validator: Creating VerifyingKey for zkas circuit with namespace TokenMint_V1
16:59:56 [INFO] consensus::validator: Finished creating VerifyingKey objects for Money Contract (ContractID: 9EUgjxrMd7g3CTP47pj8gumaFC
NsziXLFC4sKHH5WLen)
16:59:56 [INFO] consensus::validator: Deploying DAO Contract with ContractID 9qiynXwcrF5LJz3veTPmvZHmDcQRhCchVnEZSR1TJ39f
16:59:56 [INFO] runtime::vm_runtime: Instantiating a new runtime
16:59:56 [INFO] runtime::vm_runtime: [wasm-runtime] Running deploy
16:59:56 [INFO] consensus::validator: Successfully deployed DAO Contract
16:59:56 [INFO] consensus::validator: Creating ZK verifying keys for DAO Contract zkas circuits
16:59:56 [INFO] consensus::validator: Looking up zkas db for DAO Contract (ContractID: 9qiynXwcrF5LJz3veTPmvZHmDcQRhCchVnEZSR1TJ39f)
16:59:56 [INFO] consensus::validator: Iterating over zkas db
16:59:56 [INFO] consensus::validator: Deserializing namespace
16:59:56 [INFO] consensus::validator: Creating VerifyingKey for zkas circuit with namespace DaoExec
16:59:58 [INFO] consensus::validator: Iterating over zkas db
16:59:58 [INFO] consensus::validator: Deserializing namespace
16:59:58 [INFO] consensus::validator: Creating VerifyingKey for zkas circuit with namespace DaoMint
17:00:00 [INFO] consensus::validator: Iterating over zkas db
17:00:00 [INFO] consensus::validator: Deserializing namespace
17:00:00 [INFO] consensus::validator: Creating VerifyingKey for zkas circuit with namespace DaoVoteMain
```

darkfid

p2p network

Compiler for the Halo2 zkVM language used in DarkFi.

```
Usage: zkas [OPTIONS] <INPUT>

Arguments:
  <INPUT>  ZK script to compile

Options:
  -o <FILE>       Place the output into <FILE>
  -s              Strip debug symbols
  -E              Preprocess only; do not compile
  -i              Interactive semantic analysis
  -e              Examine decoded bytecode
  -h, --help      Print help information
  -V, --version   Print version information
bash-5.1$
```

compiler

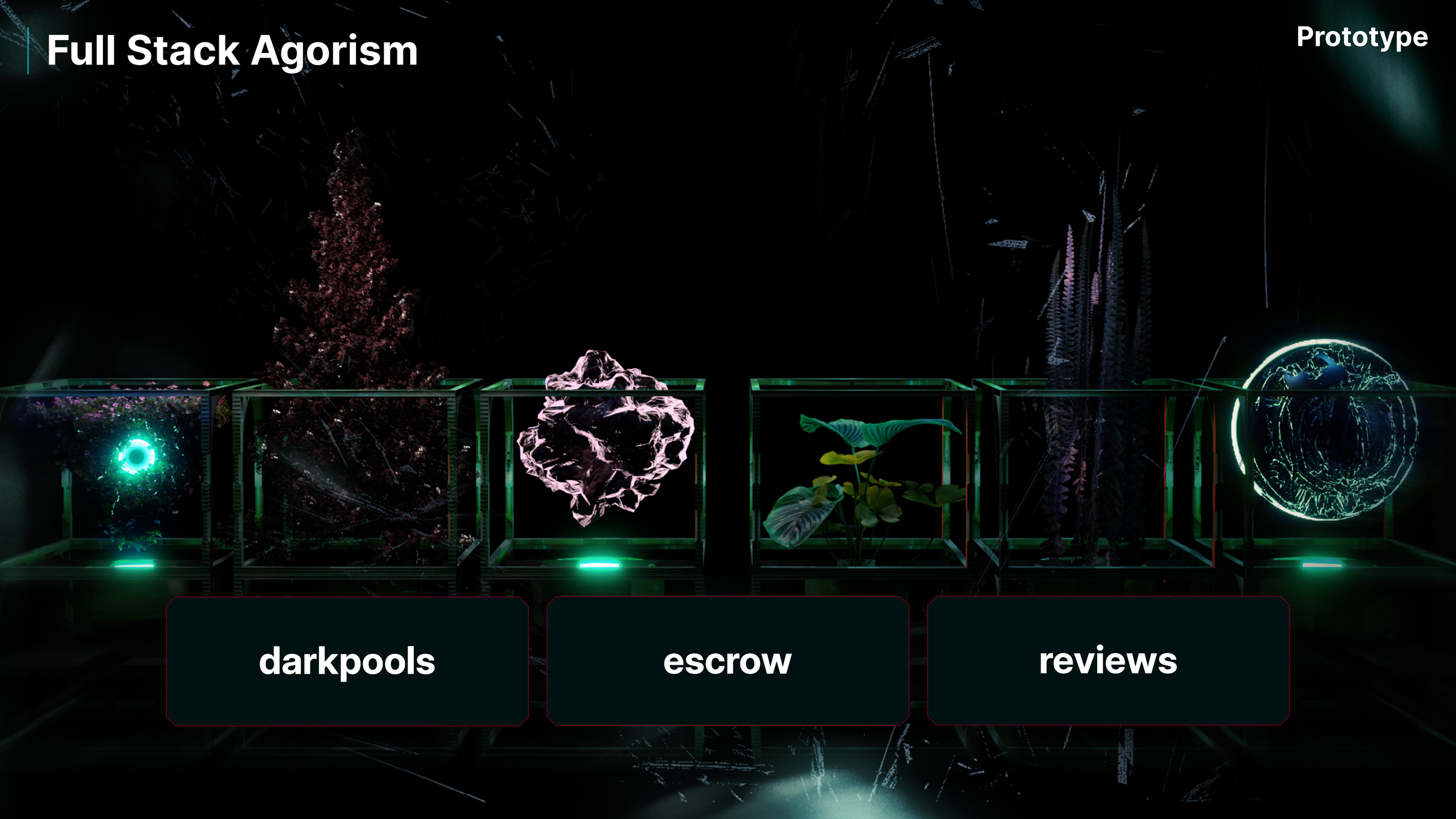
```
bash-5.1$ ./drk wallet --balance
 Token ID                                     | Balance
----------------------------------------------+---------
 DARKf7X1utGbz8ZpnvtCH6i46nSD7FFGa5tMnhoubWPq | 100
 BobvfQrDaf32VNhVtX6Adyi3WGfPpPYZPJBn6rnrxHKm | 50

bash-5.1$
```

wallet

Full Stack Agorism

Prototype



darkpools

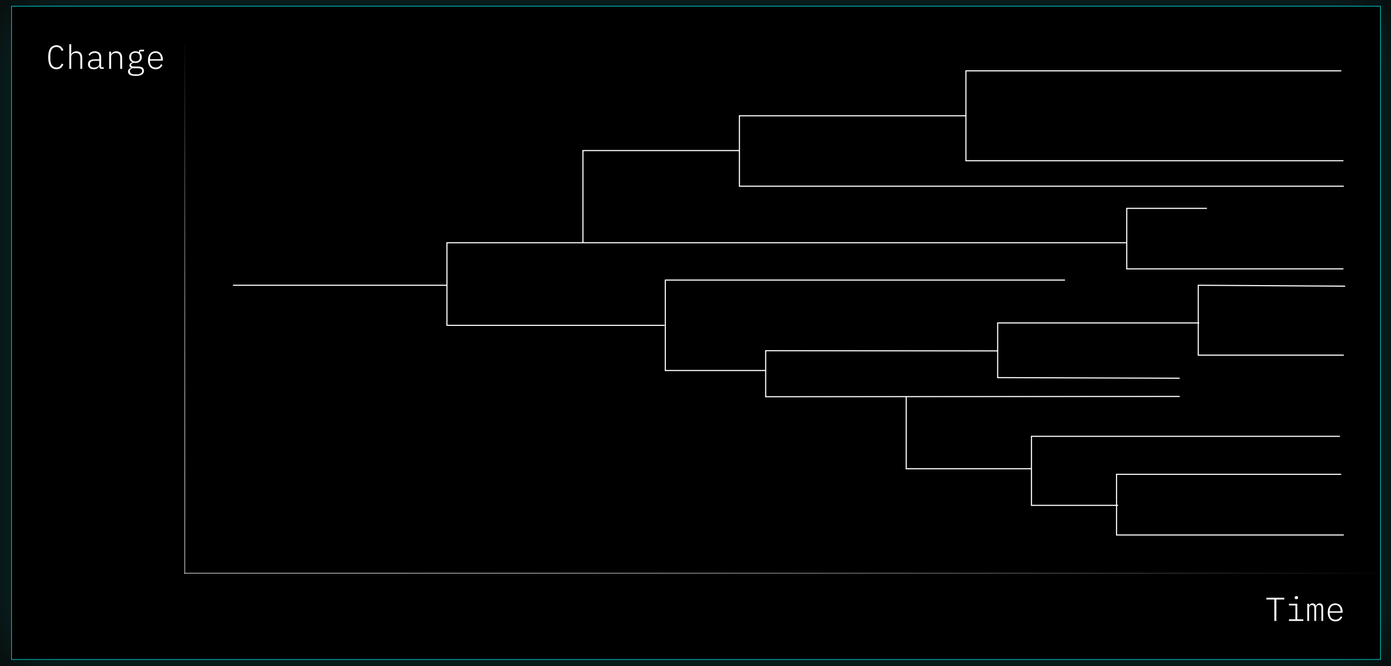
escrow

reviews

Punctuated Equilibrium

**“There are decades where nothing happens;
and there are weeks where decades happen.”**

— Lenin



Complex system builds → Rising complexity → Terminal tipping point → Collapse → Race to occupy niches → Rearrangement followed by stasis

Symmetry & Duality

Let P denote a statement about points and lines.
$P^{\perp}$ is the dual statement `s/line/point/, s/point/line/`

For example

- Statement P — Through two distinct points Q_1 and Q_2 there always pass a uniqely determined line ℓ.
- Statement $P^{\perp}$ — Two distinct lines q_1 and q_2 always intersect in a unique point L.

$$f(X, Y, Z) = aX + bY + cZ = (a, b, c)$$
$$P = (u, v, w)$$
$$f(P) = 0 = au + bv + cw$$

$$g(X, Y, Z) = uX + vY + wZ = (u, v, w)$$
$$Q = (a, b, c)$$
$$g(Q) = ua + vb + wc = 0$$


Born To Fren