

DarkFi
RAILGUN
Waku

Technology for Parallel Societies: State of the Art and Future



Participants



Amir
DarkFi core dev



Kieran
Rail DAO contributor



Franck
Waku contributor

Agenda

1. Required properties
2. Project presentations
3. Diving in projects' properties
4. Caveats and future work
5. Closing thoughts

Required Properties

Tell me.

What do we need from technology
when building a parallel society?



Required Properties

What do we need from technology when building a parallel society?

Privacy & Anonymity

Censorship Resistance

Free(dom) access

Security

Transparency & Openness

Sustainability & Continuance

**Privacy for the weak,
transparency for the powerful**

Building accountable services as alternative to institutions while protecting individuals from surveillance and oppression

Marketplace of ideas

Favor critical thinking and emergence of truth to enable competing services

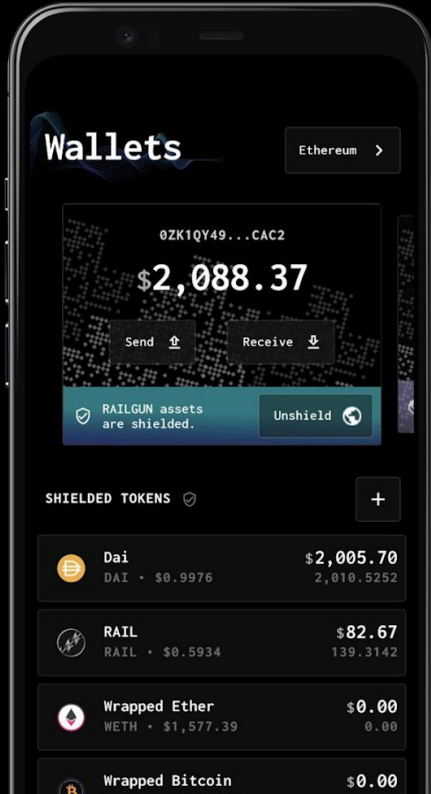
Independent structures

Self-organized, self-sufficient and unmanipulated by institutions for sovereign individuals and communities

Political neutrality

For effective governing services.

RAILGUN_ is on-chain Zero-Knowledge privacy infrastructure enabling fully private use of Ethereum/EVM



```
TERMINAL WALLETS - CLI for 0x and 0zk addresses

TERMINAL

[*] Now arriving at Terminal Wallet v1.0.0... (Featuring RAILGUN Privacy)

Wallet: My Wallet
[Private] 0zk1qyjjr1cwh25t2x6j9104ytdh9tr23yljx45t7a7sah2k4psnsccr3rv7j6fe3z5311qrmids4m3fhfvvr9gq3mcd
[Public ] 0x0c06556dcAB904983f2B0CF8127E09269777cc3c

Relayers: Available

ETHEREUM PRIVATE BALANCES =====
NO PRIVATE Balances...
=====

>> Private Actions <<
Send ERC20s Privately
Unshield ERC20s
Unshield [ETH]

>> Public Actions <<
Shield ERC20s
Shield [ETH]
Send ERC20s Publicly
Send [ETH]

>> Utilities <<
Wallet Tools
Switch Wallet
Switch Network
Add New ERC20 Token
Add / Edit Contact Addresses

Refresh Balances
> Toggle Public Balances
Reset Relayer Connection
Edit RPC Providers
Disable Responsive Menu (experiencing flicker?)

>> 0X SWAP Tools <<
Privately SWAP ERC20 Tokens
Publicly SWAP ERC20 Tokens

Exit?
```

▼ TECH

- philosophy 85 253
- rome-dao
- memes
- community 7845
- philosophy
- rome-dao 81 48
- memes
- community 5
- memes
- community

▼ MISC

- philosophy
- rome-dao
- memes
- community

▼ ROME-DAO

▼ LUNARDAG

0 dev TOPIC DarkFI Development HQ [unread messages 256 / total messages 3994 / RICKAS 83]

20:40 anon1 ipsum dolor sit amet, consectetur
 20:40 anon1 ipsum dolor sit amet, consectetur
 20:41 anon1 ipsum dolor sit amet, consectetur
 20:19 unknowneror

20:48 unknowneror ipsum dolor sit amet, consectetur
 20:56 kolyada1999 ipsum dolor sit amet, consectetur
 20:56 kolyada1999 qui dolorem ipsum quia dolor sit amet adipisci velit, sed quia non numquam eius modi tempora
 incidunt ut labore et dolore magnam aliquam quaerat
 20:58 unknowneror ipsum dolor sit amet, consectetur enim ipsum voluptatem quia voluptas sit aspernatur aut
 odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt
 consectetur enim ipsum voluptatem quia voluptas sit aspernatur aut odit aut fugit
 20:52 anon1 porro quisquam est, qui dolorem ipsum quia dolor sit amet adipisci velit, sed quia non numquam eius
 modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem
 20:52 anon1 ipsum dolor sit amet, consectetur
 20:58 kolyada1999 ipsum dolor sit amet, consectetur
 20:48 loremipsumcontractor ipsum dolor sit amet, consectetur
 20:48 loremipsumcontractor consectetur
 20:19 kolyada1999 ipsum dolor sit amet, consectetur
 20:22 anon1 ipsum dolor sit amet, consectetur
 20:59 kolyada1999 ipsum dolor sit amet,
 20:29 anon1 ipsum dolor sit amet, consectetur
 20:29 anon1 ipsum dolor sit amet, consectetur
 20:18 loremipsumcontractor consectetur
 20:22 anon1 ipsum dolor sit amet, consectetur
 20:23 anon1 ipsum dolor sit amet, consectetur
 20:23 anon1 ipsum dolor sit amet, consectetur
 20:25 loremipsumcontractor ipsum dolor sit amet, consectetur
 20:59 kolyada1999 ipsum dolor sit amet,
 20:29 anon1 ipsum dolor sit amet, consectetur
 20:21 unknowneror sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt,
 20:51 unknowneror sequi ratione voluptate,
 20:55 kolyada1999 ipsum dolor sit amet, consectetur
 20:30 anon1 ipsum dolor sit amet, consectetur
 20:58 kolyada1999 qui dolorem ipsum quia dolor sit amet adipisci velit, sed quia non numquam eius modi tempora
 incidunt ut labore et dolore magnam aliquam quaerat
 20:58 unknowneror ipsum dolor sit amet, consectetur enim ipsum voluptatem quia voluptas sit aspernatur aut
 odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt,
 20:30 anon1 ipsum dolor sit amet, consectetur
 20:29 kolyada1999 ipsum dolor sit amet,
 20:29 anon1 ipsum dolor sit amet, consectetur
 20:29 kolyada1999 ipsum dolor sit amet, consectetur
 20:29 anon1 ipsum dolor sit amet, consectetur
 20:29 kolyada1999 ipsum dolor sit amet, consectetur

anon1 darkfi is going to make anime real



SEEN ONLINE

- kolyada1999
- anon1
- unkownneror
- loremipsumcontractor
- neige
- uncleted
- spez
- jstark
- anon00
- carolvs
- windy@houle
- wolf
- kolyada1999
- anon1
- jstark
- anon00
- carolvs
- windy@houle
- wolf
- darkfoesathunter
- kolyada1999
- unkownneror
- loremipsumcontractor
- neige
- uncleted
- spez
- anon1
- unkownneror:
- loremipsumcontractor
- neige
- uncleted
- spez
- jstark
- anon00
- carolvs
- windy@houle
- wolf
- sovereignindividual

new discord

TYPE: CHAT ▼ DAO ▼ WALLET || TERMINAL +

NAME: name

PUBLIC | PRIVATE

CHANNEL SECRET GENERATE NEW COPY X

a116c7e31463fa116c7e315c84205312b169ea2fa3cd268

SECTION ▼ TECH ▼ MISC

Disc height: 2017295



```

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
Name #10/27line)
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:11081 (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

```

Compiler for the Halo0 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$ ./drk wallet --balance
Token ID | Balance
-----|-----
DARKfZx1utGbz8ZpvtCH6i4onSDZEEGa5MnhoubWPq | 100
BobvFqrDaF32VnhvX6aAdyI9WGFppPYZPBn6rnxHKM | 50
bash-5.1$

```

```

darkfid (offline)
evgrd (offline)
darkirc
outbound
0: tor://bom5siou7a25vocoh43eh52ajuzsn5zcgw27j3mfmmnr4wsv26
miqyd.onion:24661/
1: sleeping
2: tor://mnc5llkxkqt3ssnmw2kqtkyoggevj67244uzzylbtq2mndiqvj4
kuoid.onion:27773/
3: sleeping
4: sleeping
5: sleeping
6: sleeping
7: sleeping
8: sleeping
9: sleeping
10: sleeping
11: sleeping
12: connecting: addr=tor://5s1llgpqmcam5w2ra6gnrozrmanl14jz
hswb17hegw154vlrknw6wd.onion:25551/
13: connecting: addr=tor://ee23j71l1bws6fd25f1p1aswq43aqlf5qo
sc565ova3pegklyb3mpqsad.onion:27771/
14: connecting: addr=tor://xomyqdyh6pmd6homqac2wvcar56vomek1
7g56dxtayq6p4z67woasgad.onion:27771/
15: sleeping
Inbound

```

```

14:00:26: send: EventGraph::EventPut
14:00:26: recv: EventGraph::EventPut
14:00:26: send: ping
14:00:27: recv: pong
14:00:28: recv: getaddr
14:00:28: send: addr
14:00:31: send: EventGraph::EventPut
14:00:31: recv: EventGraph::EventPut
14:00:40: send: getaddr
14:00:41: recv: addr
14:00:46: send: getaddr
14:00:46: recv: addr
14:00:57: send: ping
14:00:58: recv: pong
14:01:26: send: getaddr
14:01:26: recv: addr
14:01:31: send: addr
14:01:29: recv: pong
14:01:31: send: getaddr
14:01:31: recv: addr
14:01:38: send: getaddr
14:01:38: send: addr

```

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\$

```

sensus:validator: Creating VerifyingKey for zkcas circuit with namespace TokenMint_V1
sensus:validator: Finished creating VerifyingKey objects for Money Contract (ContractID: 9EUgjxrMd7g3CTP47pJgumaFC

```

```

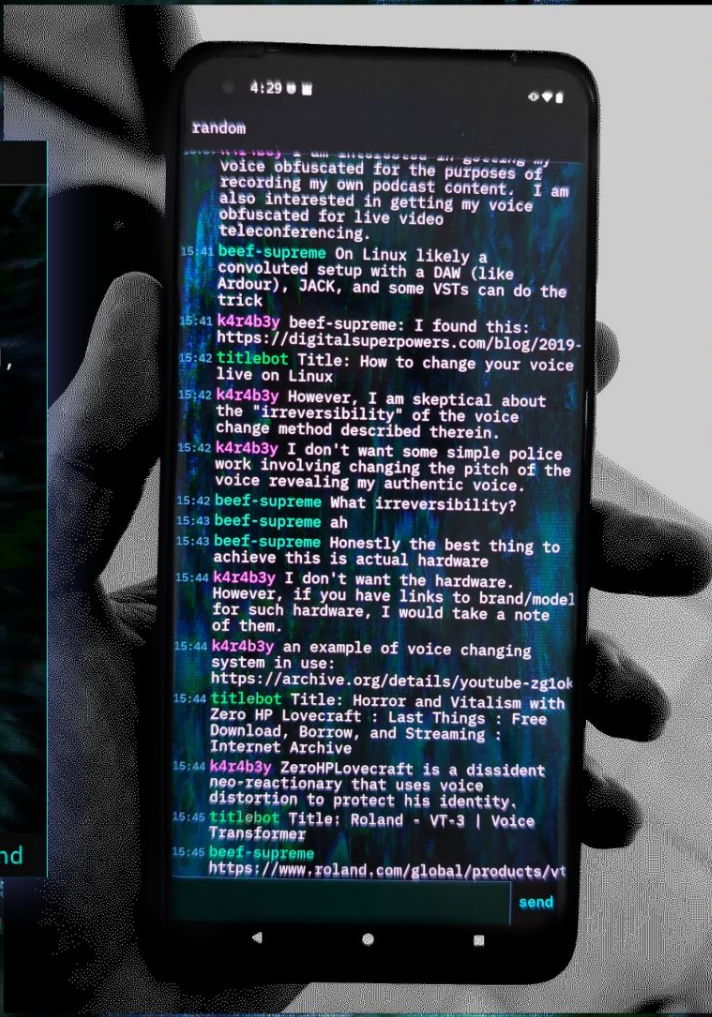
sensus:validator: Deploying DAO Contract with ContractID 9qiynXwcrF5LJz3veTPmvZHmDcQRhCchVnEZSR1TJ39f
time:vm runtime: Instantiating a new runtime
time:vm runtime: [wasms-runtime] Running deploy
sensus:validator: Successfully deployed DAO Contract
sensus:validator: Creating ZK verifying keys for DAO Contract zkcas circuits
sensus:validator: Looking up zkcas db for DAO Contract (ContractID: 9qiynXwcrF5LJz3veTPmvZHmDcQRhCchVnEZSR1TJ39f)
sensus:validator: Iterating over zkcas db
sensus:validator: Deserializing namespace
sensus:validator: Creating VerifyingKey for zkcas circuit with namespace DaoExec
sensus:validator: Iterating over zkcas db
sensus:validator: Deserializing namespace
sensus:validator: Creating VerifyingKey for zkcas circuit with namespace DaoMint
sensus:validator: Iterating over zkcas db
sensus:validator: Deserializing namespace
sensus:validator: Creating VerifyingKey for zkcas circuit with namespace DaoVoteMain

```


random

```
13:47 beef-supreme I reckon you know what you're doing if you disable it :D
13:48 upgrayedd well yeah, but you still need to maintain it manually
13:48 x well yeah, but you must maintain it manually then when it diverges
13:48 anon now my darkirc desktop is not sending messages, yet I can receive
everyone else's messages
13:48 x again, this is a time based protocol, you can't be over the threshold,
aka UTC+EVENT_DRIFT
13:49 anon i guess darkirc cannot see any of these messages? lol
13:49 B1-66ER test
13:49 upgrayedd B1-66ER: still just you and me
13:49 upgrayedd check your clocks
13:49 B1-66ER test
13:50 beef-supreme ++
13:50 beef-supreme But it still shouldn't be causing issues for others though
13:50 B1-66ER yooooooooo
13:50 x it could
13:50 beef-supreme I mean if their clock _is_ correct
13:50 x ah yeah if clock correct then it should see messages as valid and
propagate them
13:51 beef-supreme Yeah
13:52 testbot test back
hello from darkirc ;)|
```

send



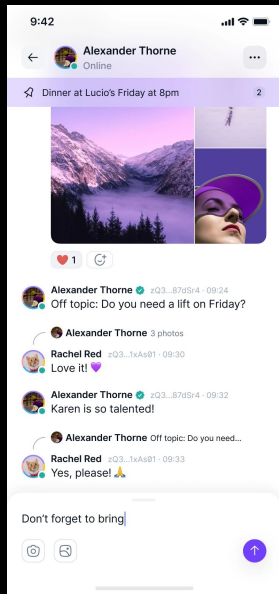
4:29

random

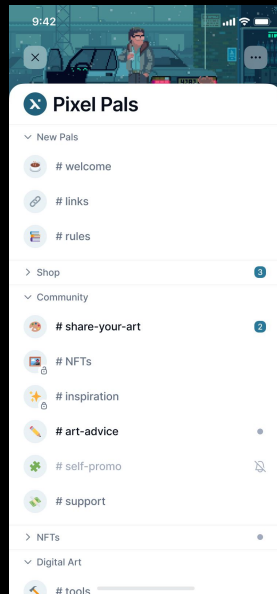
```
voice obfuscated for the purposes of recording my own podcast content. I am also interested in getting my voice obfuscated for live video teleconferencing.
15:41 beef-supreme On Linux likely a convoluted setup with a DAW (like Ardour), JACK, and some VSTs can do the trick
15:41 k4r4b3y beef-supreme: I found this: https://digitalsuperpowers.com/blog/2019-
15:42 titlebot Title: How to change your voice live on Linux
15:42 k4r4b3y However, I am skeptical about the "irreversibility" of the voice change method described therein.
15:42 k4r4b3y I don't want some simple police work involving changing the pitch of the voice revealing my authentic voice.
15:42 beef-supreme What irreversibility?
15:43 beef-supreme ah
15:43 beef-supreme Honestly the best thing to achieve this is actual hardware
15:44 k4r4b3y I don't want the hardware. However, if you have links to brand/model for such hardware, I would take a note of them.
15:44 k4r4b3y an example of voice changing system in use: https://archive.org/details/youtube-zg1ok
15:44 titlebot Title: Horror and Vitalism with Zero HP Lovecraft : Last Things : Free Download, Borrow, and Streaming : Internet Archive
15:44 k4r4b3y ZeroHPLovecraft is a dissident neo-reactionary that uses voice distortion to protect his identity.
15:45 titlebot Title: Roland - VT-3 | Voice Transformer
15:45 beef-supreme https://www.roland.com/global/products/vt
```

send

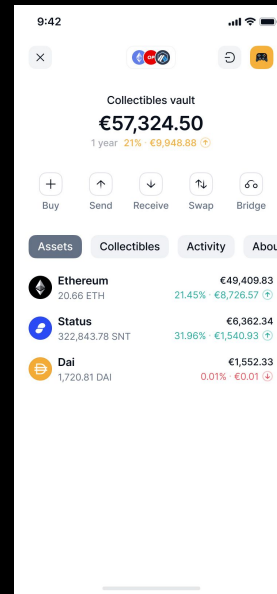
Status Super App



One-to-One Messenger



Communities



Wallet

Application requirements

—

Works on mobile

- CPU
- Battery
- Bandwidth
- Mostly offline

One-to-one chats, group chats, IRC-like

- Broadcast model (vs point-to-point)

What is Waku?

—

All-in-one suite of protocols that handle

- Message routing
- Peer discovery
- Several mode of operations
 - Relay: sovereign, more resource
 - Edge: dependant, yet decentralized
- Reliability
 - Peer-to-peer
 - End-to-end
- Encryption
- Service network

Diving in

How are those properties implemented?

Privacy & Anonymity

**Privacy for the weak,
transparency for the powerful**

Building accountable services as alternative to institutions while protecting individuals from surveillance and oppression

Censorship Resistance

Free(dom) access

Marketplace of ideas

Favor critical thinking and emergence of truth to enable competing services

Security

Transparency & Openness

Independent structures

Self-organized, self-sufficient and unmanipulated by institutions for sovereign individuals and communities

Sustainability & Continuance

Political neutrality

For effective governing services.

Future Work

—

Future Work & Closing Thoughts

