grincon1
2019.11.22 // c-base berlin

Usability of Grin

Regarding Grin's transaction methods and its utility

@nijynot

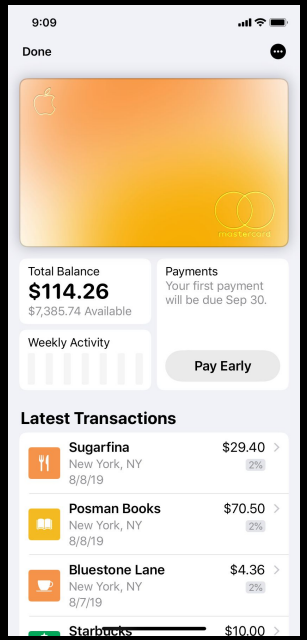
QTUM

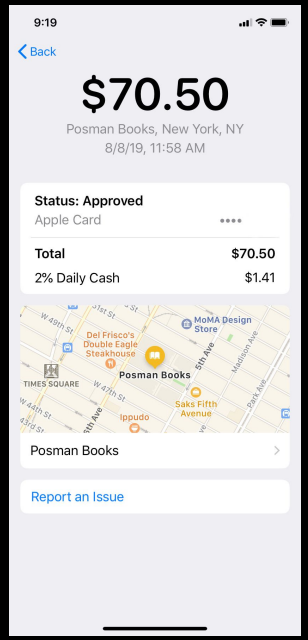
SPARK POOL

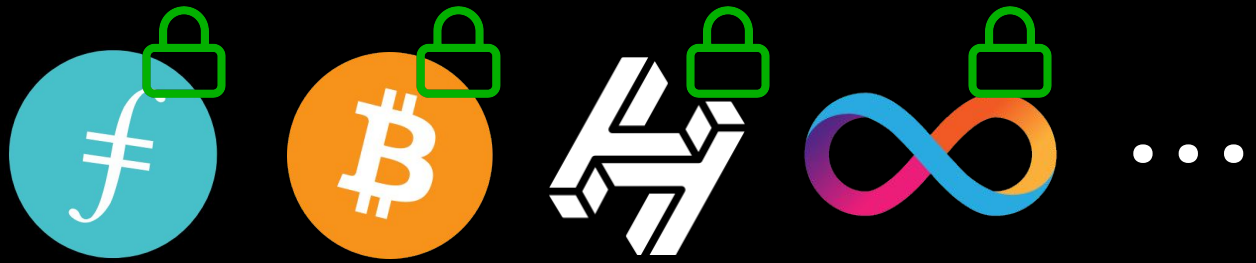
Before usability comes utility

Does not hide **amounts** and are **non-fungible**.
Privacy is a strict requirement for mainstream adoption.

No one would use banks if everything was public.
Same can be said of cryptocurrencies.

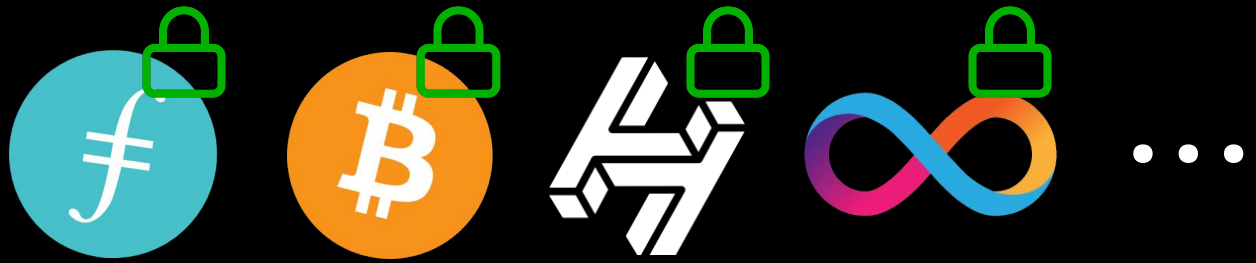






Privacy **built-in** in every cryptocurrency?
Probably not.

Implementation risk.
Privacy is non-trivial to add.



Privacy **built-in** in every cryptocurrency?
Probably not.

Grin aims to be a **privacy-preserving** digital currency.
Hides amounts.

Usability

No addresses.

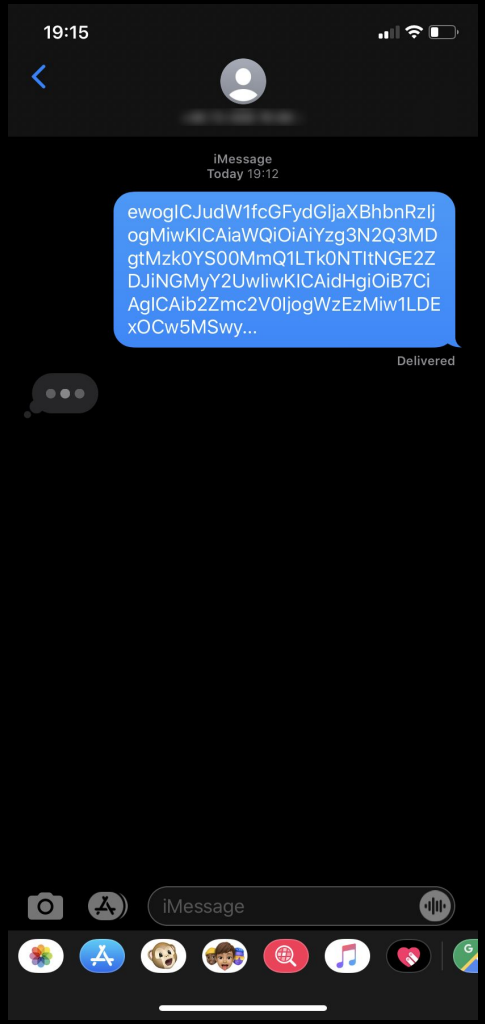
No assumptions at the transaction layer.

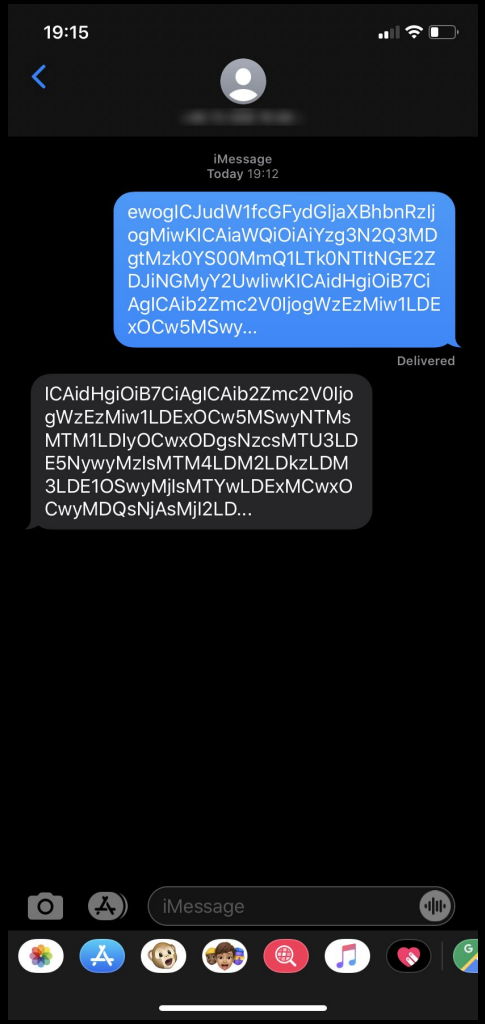
Maybe future proof?

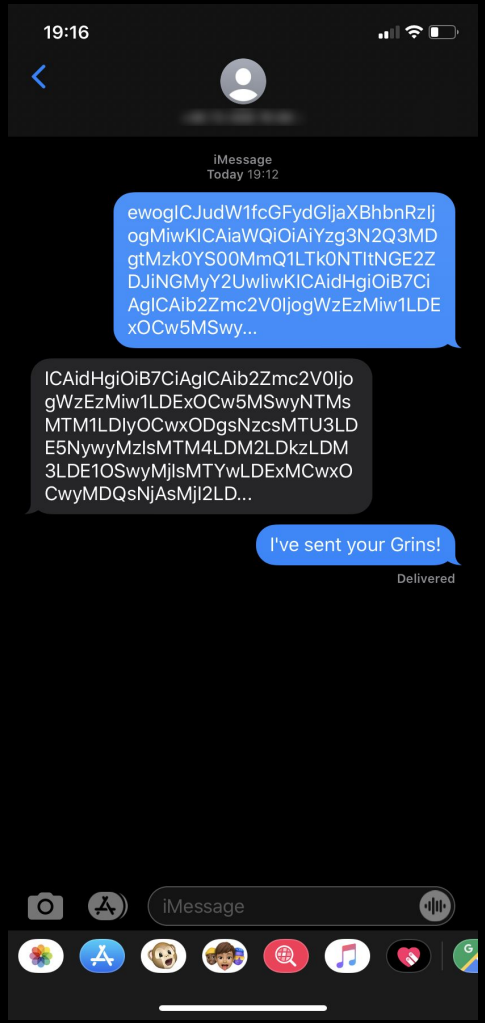
How do you send Grin?

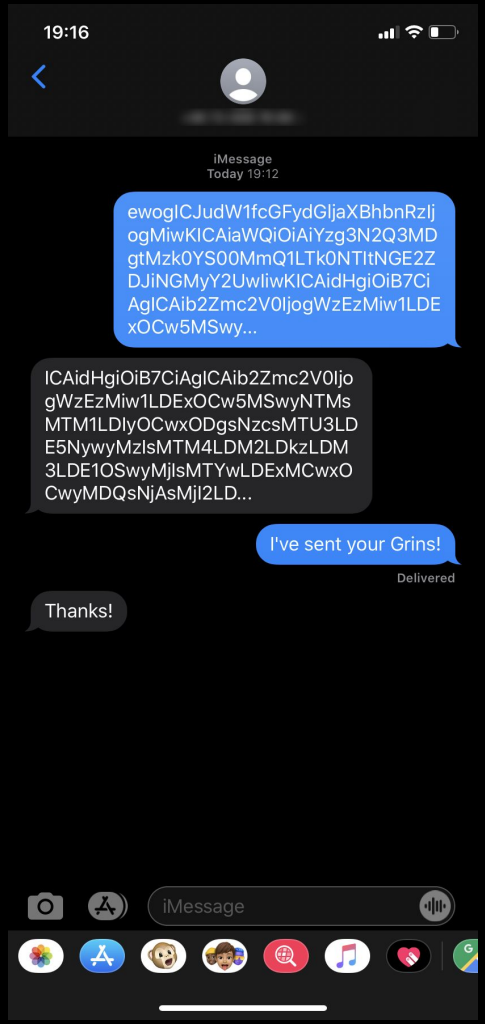
HTTP, HTTPS, File, Base64, Tor, i2p, ...

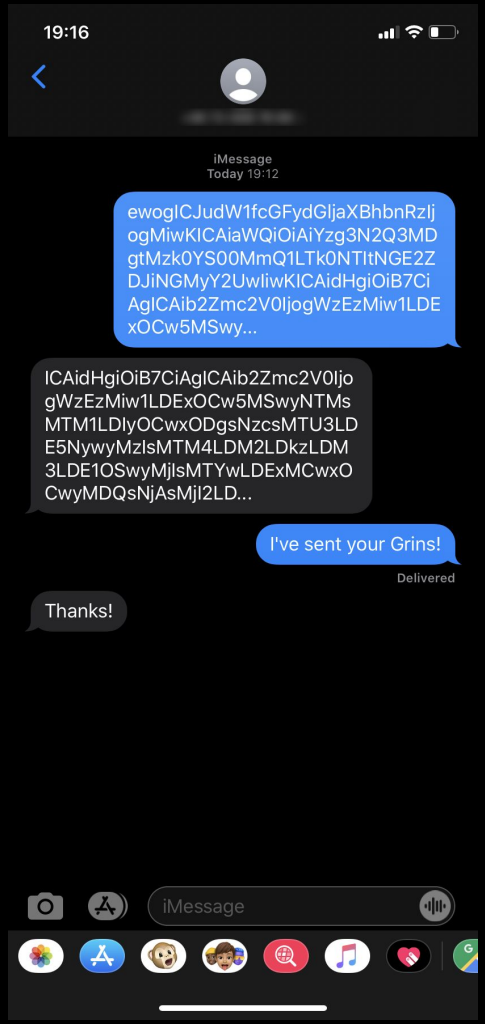
Send in Grin through your favorite chat app.



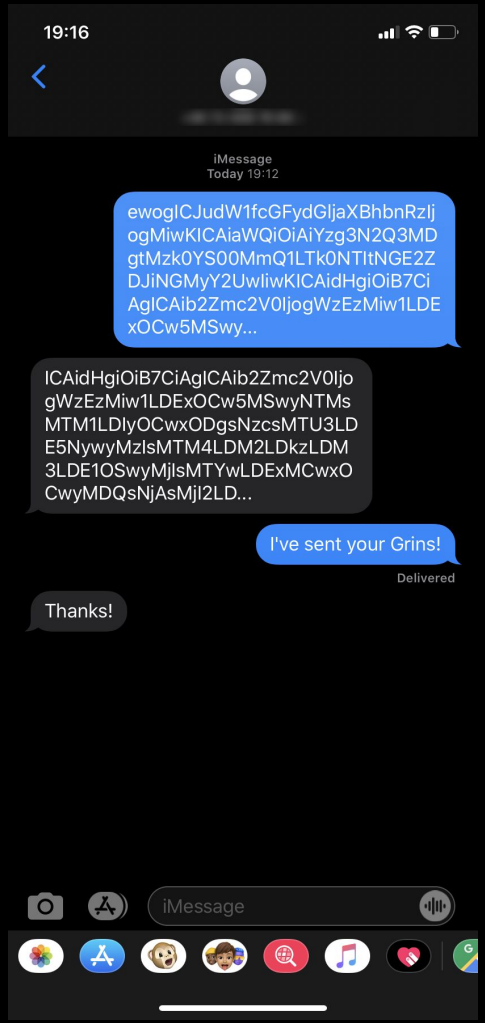

19:15
iMessage
Today 19:12
ewogICJudW1fcGFydGljaXBhbnRzIjogMiwKICAiaWQiOiAiYzg3N2Q3MDgtMzk0YS00MmQ1LTk0NTItNGE2ZDJiNGMyY2UwIiwKICAidHgiOiB7CiAgICAib2Zmc2V0IjogWzEzMiw1LDExOCw5MSwy...
Delivered
ICAidHgiOiB7CiAgICAib2Zmc2V0IjogWzEzMiw1LDExOCw5MSwyNTMsMTM1LDIyOCwxODgsNzcsMTU3LDE5NywyMzIsMTM4LDM2LDkzLDM3LDE1OSwyMjIsMTYwLDExMCwxOCwyMDQsNjAsMjI2LD...
iMessage


19:16
iMessage
Today 19:12
ewogICJudW1fcGFydGljaXBhbnRzIjogMiwKICAiaWQiOiAiYzg3N2Q3MDgtMzk0YS00MmQ1LTk0NTItNGE2ZDJiNGMyY2UwIiwKICAidHgiOiB7CiAgICAib2Zmc2V0IjogWzEzMiw1LDExOCw5MSwy...
lCAidHgiOiB7CiAgICAib2Zmc2V0IjogWzEzMiw1LDExOCw5MSwyNTMsMTM1LDIyOCwxODgsNzcsMTU3LDE5NywyMzIsMTM4LDM2LDkzLDM3LDE1OSwyMjIsMTYwLDExMCwxOCwyMDQsNjAsMjI2LD...
I've sent your Grins!
Delivered
iMessage


19:16
iMessage
Today 19:12
ewogICJudW1fcGFydGljaXBhbnRzIjogMiwKICAiaWQiOiAiYzg3N2Q3MDgtMzk0YS00MmQ1LTk0NTItNGE2ZDJiNGMyY2UwIiwKICAidHgiOiB7CiAgICAib2Zmc2V0IjogWzEzMiw1LDExOCw5MSwy...
ICAidHgiOiB7CiAgICAib2Zmc2V0IjogWzEzMiw1LDExOCw5MSwyNTMsMTM1LDIyOCwxODgsNzcsMTU3LDE5NywyMzIsMTM4LDM2LDkzLDM3LDE1OSwyMjIsMTYwLDExMCwxOCwyMDQsNjAsMjI2LD...
I've sent your Grins!
Delivered
Thanks!
iMessage



Transaction slates are longer than what is shown here.



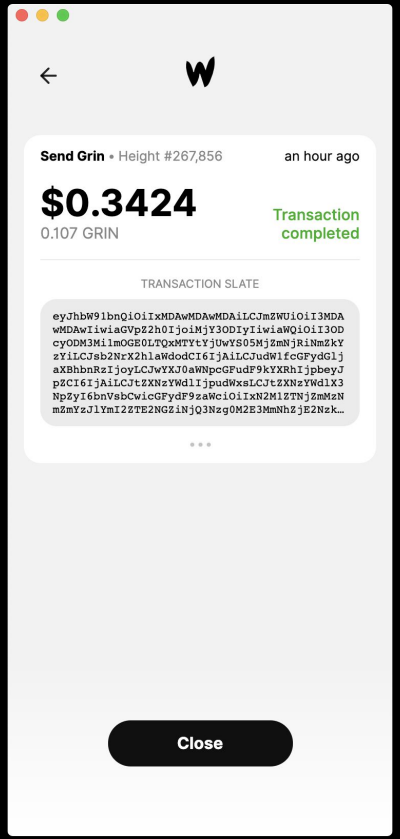
Transaction slates are longer than what is shown here.

Intuitive as the slate are your coins.

Wimble

Does not support HTTP, HTTPS, only file and base64.

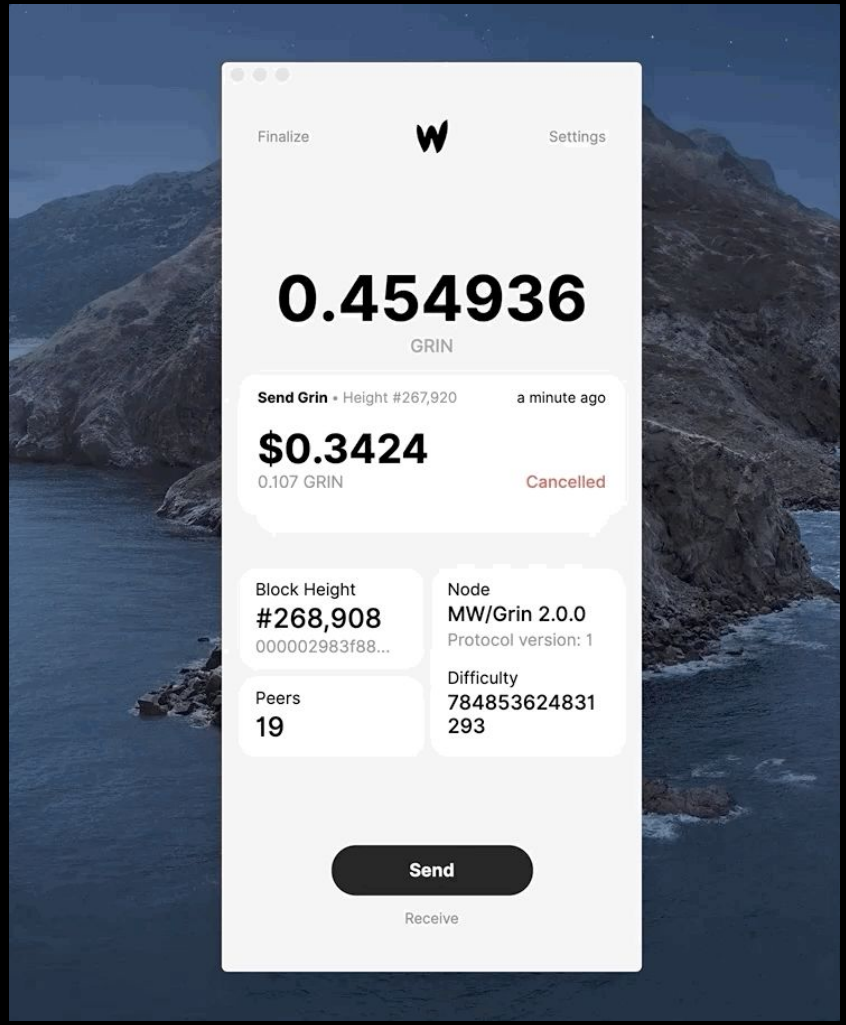
Built with Electron, React and calls JSON-RPC APIs for grin-wallet.

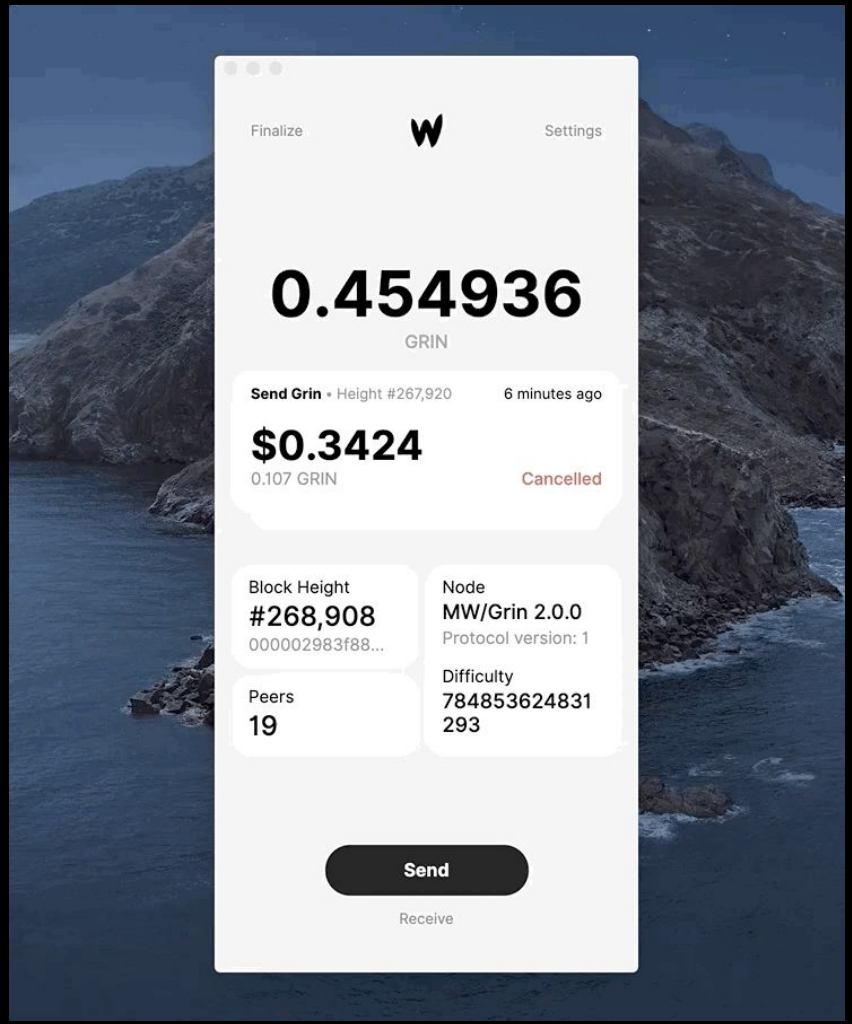


Every transaction
Is a card.

Copy or save the
transaction slate.

Press the dots to
expand the transaction.



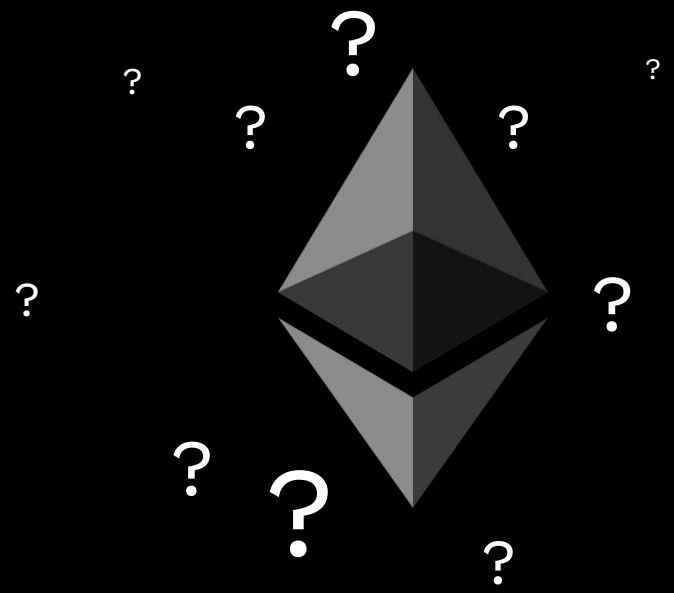


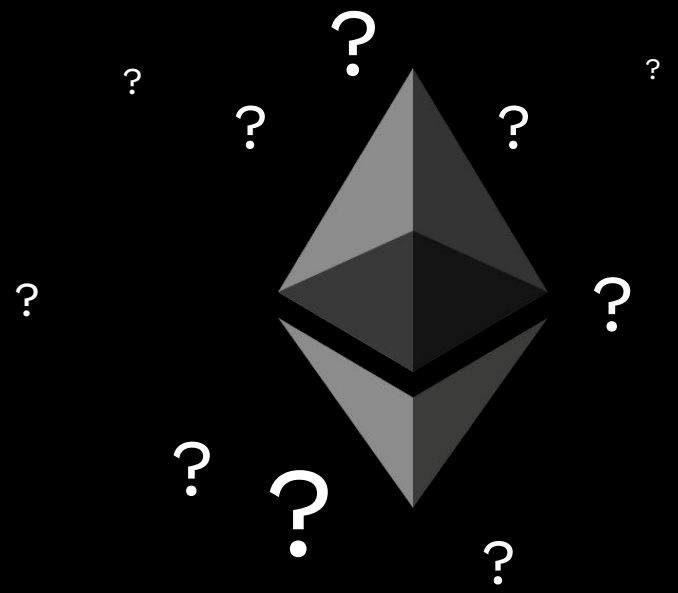
Blur out total
amount by pressing it.

Can we create an even better experience?

Can we create an even better experience?

Creating a **contract Grin wallet.**





No privacy built-in.

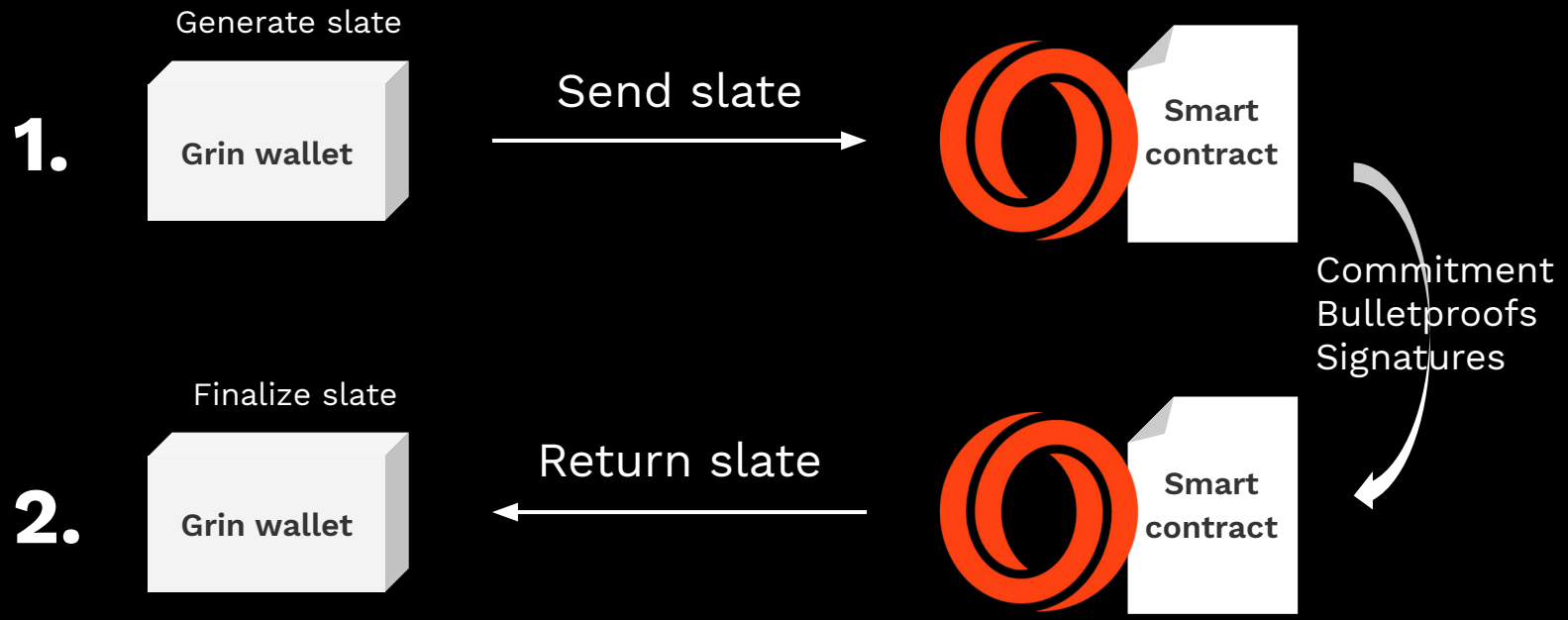
Homomorphic encryption not really here yet.

Then I thought of Oasis Protocol.

Private state machine

End-to-end encryption

Supports Rust contracts


Generate slate
1.
Grin wallet
Send slate
Smart contract
Commitment
Bulletproofs
Signatures
Finalize slate
2.
Grin wallet
Return slate
Smart contract

Always online.

So… does it actually work?

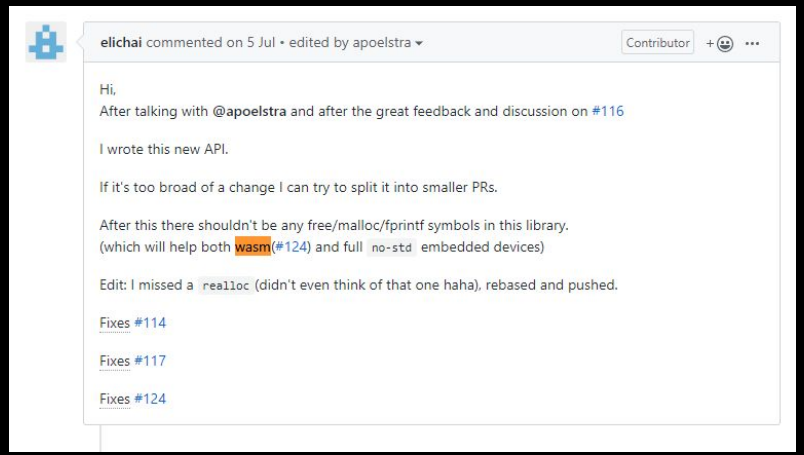
Compiled **mw/rust-secp256k1-zkp** into
WebAssembly Standard Interface (WASI) for Oasis

mimblewimble/rust-secp256k1-zkp @ v0.7.7

Rebase (only secp256k1_commitment)

rust-bitcoin/rust-secp256k1 @ v0.16.0

rust-bitcoin/rust-secp256k1 compiles to WASM.



elichai commented on 5 Jul • edited by apoelstra — Contributor

Hi,
After talking with **@apoelstra** and after the great feedback and discussion on #116

I wrote this new API.

If it's too broad of a change I can try to split it into smaller PRs.

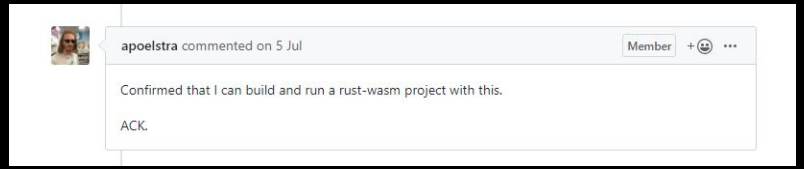
After this there shouldn't be any free/malloc/fprintf symbols in this library.
(which will help both wasm(#124) and full `no-std` embedded devices)

Edit: I missed a `realloc` (didn't even think of that one haha), rebased and pushed.

Fixes #114

Fixes #117

Fixes #124



apoelstra commented on 5 Jul — Member

Confirmed that I can build and run a rust-wasm project with this.

ACK.

rust-secp256k1-zkp-wasi

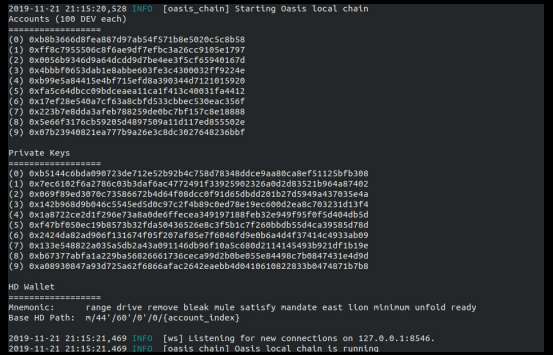
only secp256k1_commitment

$ oasis chain

```
2019-11-21 21:15:20,528 INFO  [oasis_chain] Starting Oasis local chain
Accounts (100 DEV each)
==================
(0) 0xb8b3666d8fea887d97ab54f571b8e5020c5c8b58
(1) 0xff8c7955506c8f6ae9df7efbc3a26cc9105e1797
(2) 0x0056b9346d9a64dcdd9d7be4ee3f5cf65940167d
(3) 0x4bbbf0653dab1e8abbe603fe3c4300032ff9224e
(4) 0xb99e5a84415e4bf715efd8a390344d7121015920
(5) 0xfa5c64dbcc09bdceaea11ca1f413c40031fa4412
(6) 0x17ef28e540a7cf63a8cbfd533cbbec530eac356f
(7) 0x223b7e8dda3afeb788259de0bc7bf157c8e18888
(8) 0x5e66f3176cb59205d4897509a11d117ed855502e
(9) 0x07b23940821ea777b9a26e3c8dc3027648236bbf

Private Keys
==================
(0) 0xb5144c6bda090723de712e52b92b4c758d78348ddce9aa80ca8ef51125bfb308
(1) 0x7ec6102f6a2786c03b3daf6ac4772491f33925902326a0d2d83521b964a87402
(2) 0x069f89ed3070c73586672b4d64f08dcc0f91d65dbdd201b27d5949a437035e4a
(3) 0x142b968d9b046c5545ed5d0c97c2f4b89c0ed78e19ec600d2ea8c703231d13f4
(4) 0x1a8722ce2d1f296e73a8a0de6ffecea349197188feb32e949f95f0f5d404db5d
(5) 0xf47bf050ec19b8573b32fda50436526e8c3f5b1c7f260bbdb55d4ca39585d78d
(6) 0x2424da82ad906f131674f05f207af85e7f6046fd9e0b6a4d4f37414c4933ab09
(7) 0x133e548822a035a5db2a43a091146db96f10a5c680d2114145493b921df1b19e
(8) 0xb67377abfa1a229ba56826661736ceca99d2b0be055e84498c7b0847431e4d9d
(9) 0xa08930847a93d725a62f6866afac2642eaebb4d0410610822833b0474871b7b8

HD Wallet
==================
Mnemonic:      range drive remove bleak mule satisfy mandate east lion minimum unfold ready
Base HD Path:  m/44'/60'/0'/0/{account_index}

2019-11-21 21:15:21,469 INFO  [ws] Listening for new connections on 127.0.0.1:8546.
2019-11-21 21:15:21,469 INFO  [oasis_chain] Oasis local chain is running
```

```
$ oasis build
$ node deploy.js // deploy contract
$ node client.js // test against chain

=>Commitment(0950929b74c1a04954b78b4b6035
e97a5e078a5a0f28ec96d547bfee9ace803ac0)
```

$ oasis chain



- Costs a lot of gas (not optimized).
- Oasis hasn’t launched & adoption unclear, not proven.
- Sender can send dummy txs slates and not finalize.

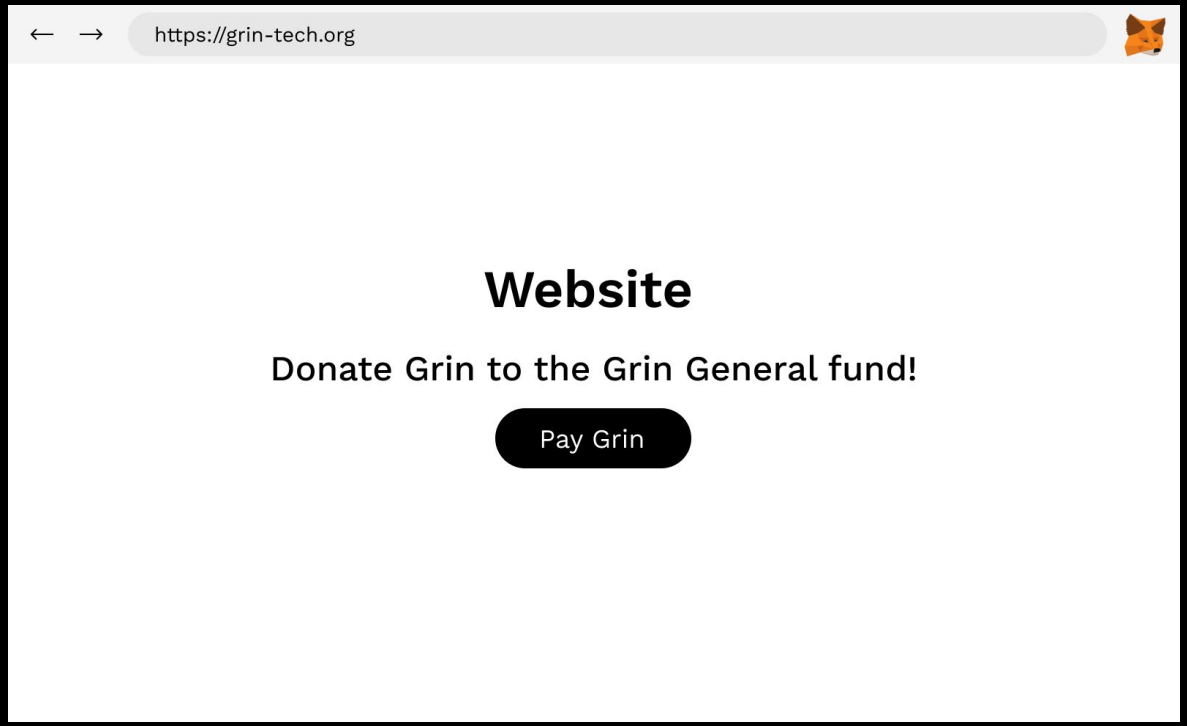
- Implies a “Grin address” (`0x...` from Oasis).

- Costs a lot of gas (not optimized).
- Oasis hasn’t launched & adoption unclear, not proven.
- Sender can send dummy txs slates and not finalize.

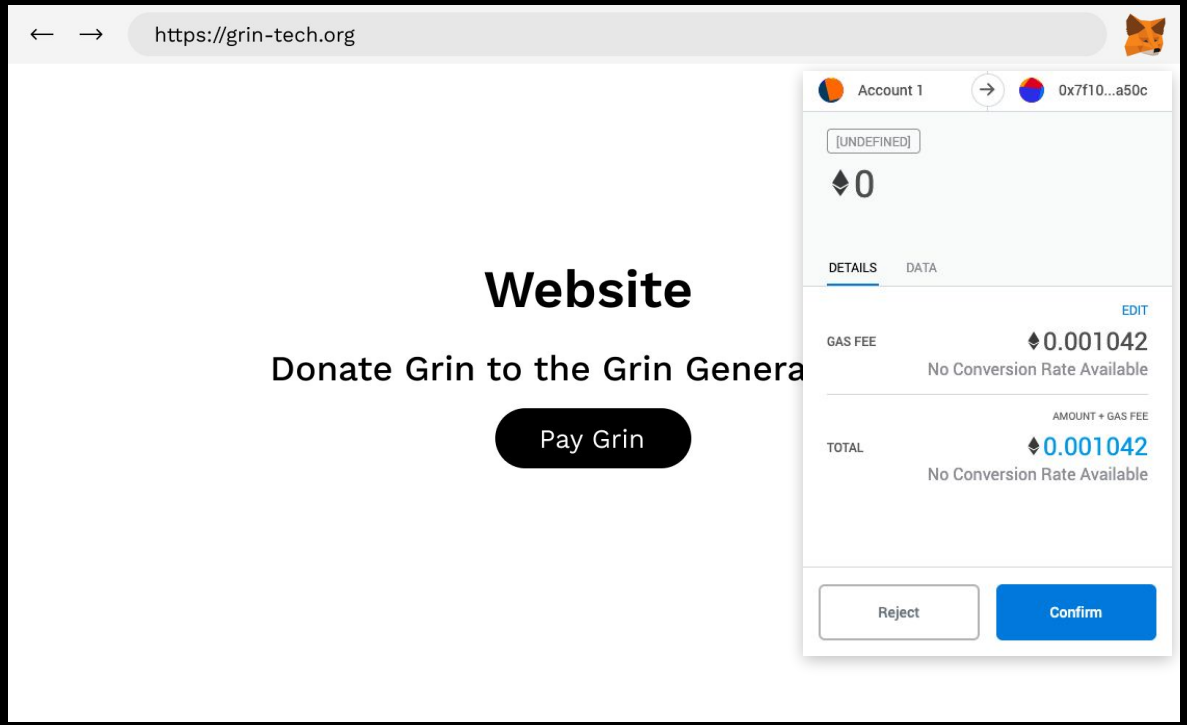
- Implies a “Grin address” (`0x...` from Oasis).

What more, if it works?

Accept Grin payments in the browser.



Accept Grin payments in the browser.



Only a vision, not meant to be used today.

Questions?