Tash-talking Cables

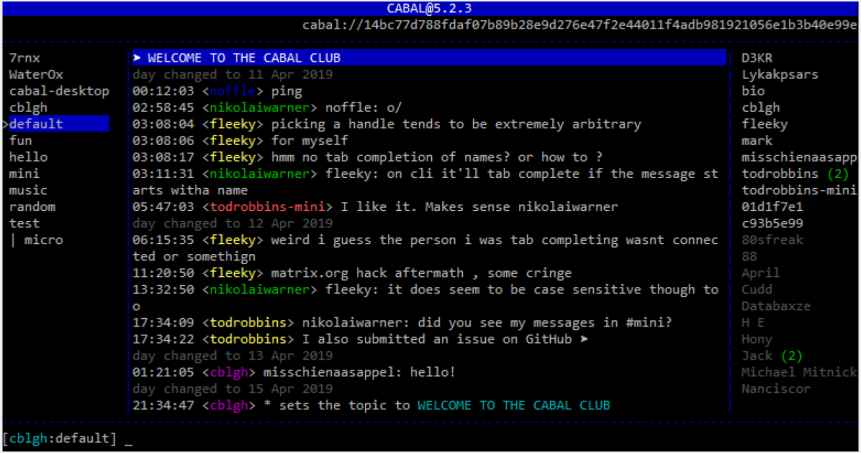
Lightning strikes into Cabal and Erlang

@cryptix@social.coop

Presented for cabletrash 37c3 edition

28.12.2023

ABOUT:CABAL



```
                                        CABAL@5.2.3
                                        cabal://14bc77d788fdaf07b89b28e9d276e47f2e44011f4adb981921056e1b3b40e99e
------------------------------------------------------------------------------------------------------------------
 7rnx           | ➤ WELCOME TO THE CABAL CLUB                                                | D3KR
 WaterOx        | day changed to 11 Apr 2019                                                  | Lykakpsars
 cabal-desktop  | 00:12:03 <noffle> ping                                                      | bio
 cblgh          | 02:58:45 <nikolaiwarner> noffle: o/                                         | cblgh
>default        | 03:08:04 <fleeky> picking a handle tends to be extremely arbitrary          | fleeky
 fun            | 03:08:06 <fleeky> for myself                                                | mark
 hello          | 03:08:17 <fleeky> hmm no tab completion of names? or how to ?               | misschienaasapp
 mini           | 03:11:31 <nikolaiwarner> fleeky: on cli it'll tab complete if the message st | todrobbins (2)
 music          | arts witha name                                                             | todrobbins-mini
 random         | 05:47:03 <todrobbins-mini> I like it. Makes sense nikolaiwarner             | 01d1f7e1
 test           | day changed to 12 Apr 2019                                                  | c93b5e99
 | micro        | 06:15:35 <fleeky> weird i guess the person i was tab completing wasnt connec | 80sfreak
                | ted or somethign                                                            | 88
                | 11:20:50 <fleeky> matrix.org hack aftermath , some cringe                   | April
                | 13:32:50 <nikolaiwarner> fleeky: it does seem to be case sensitive though to | Cudd
                | o                                                                           | Databaxze
                | 17:34:09 <todrobbins> nikolaiwarner: did you see my messages in #mini?      | H E
                | 17:34:22 <todrobbins> I also submitted an issue on GitHub ➤                 | Hony
                | day changed to 13 Apr 2019                                                  | Jack (2)
                | 01:21:05 <cblgh> misschienaasappel: hello!                                  | Michael Mitnick
                | day changed to 15 Apr 2019                                                  | Nanciscor
                | 21:34:47 <cblgh> * sets the topic to WELCOME TO THE CABAL CLUB              |
------------------------------------------------------------------------------------------------------------------
[cblgh:default] _
```

1

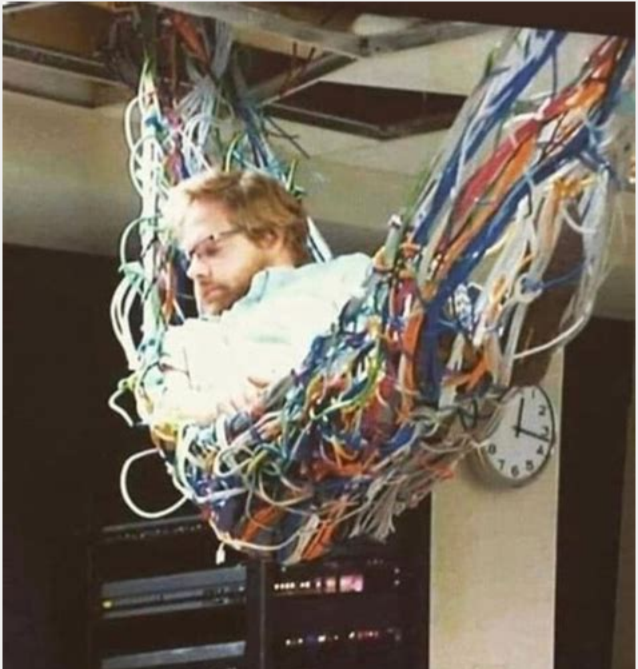
[1] https://github.com/cabal-club/cabal-cli

ABOUT:CABAL

- No servers are needed to join or start a *cabal*
- Offline first: Everything is stored and runs locally
- A cabal can never go down or be taken away
- A cabal is identified by its secret key `(cabal://7d99b453506b974...)`
- Sharing it with your friends lets them find other members

THE CABLE PROTOCOL

- *fairly* simple to implement in any language with **minimal dependencies**
- general enough to be used across different network transports
- useful, even if written as a partial implementation
- efficient in its use of network resources, by
  - syncing only the relevant subsets of the full dataset, and
  - being compact over the wire
- not specific to any particular kind of database backend

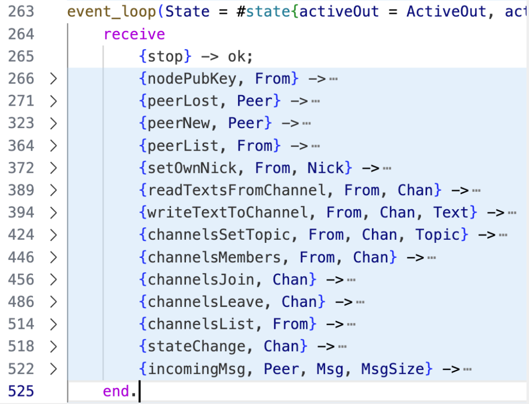


Protocol Outline

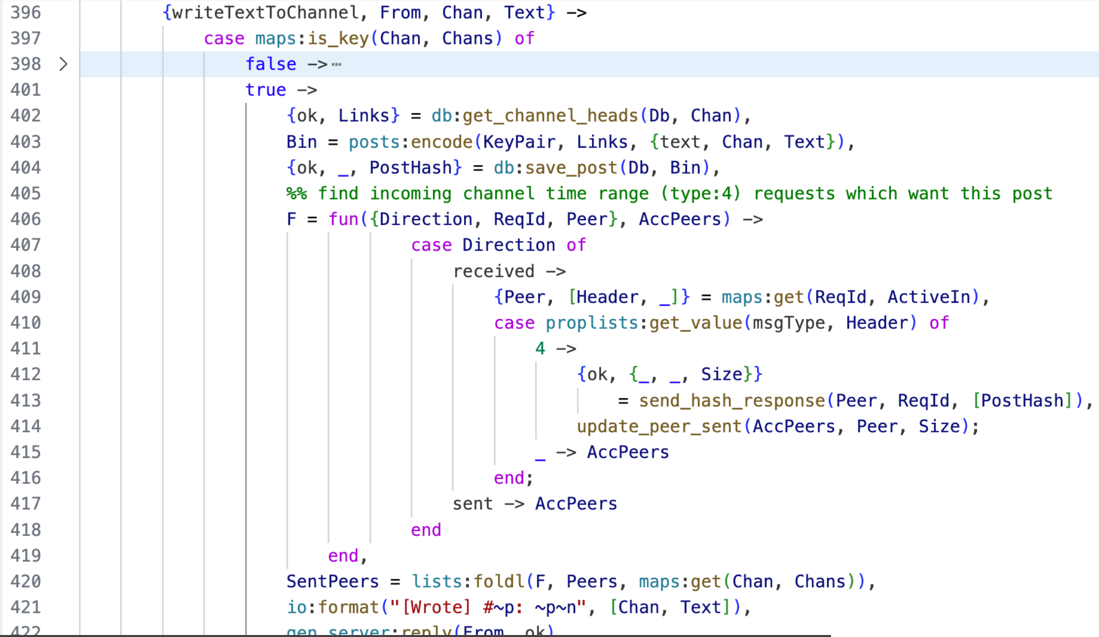
- **BLAKE2b** for hashing
- **Ed25519** for signatures
- Users write different kinds of **Posts** into **Channels**:
  `text`, `delete`, `info`, `join`, `leave`
- Nodes send out **Request**:
  `Channel Time Range`, `Channel State`, `Channel List`
- Their Peers respond with `Post` or `Hash` **Responses**

Enter: CabErl

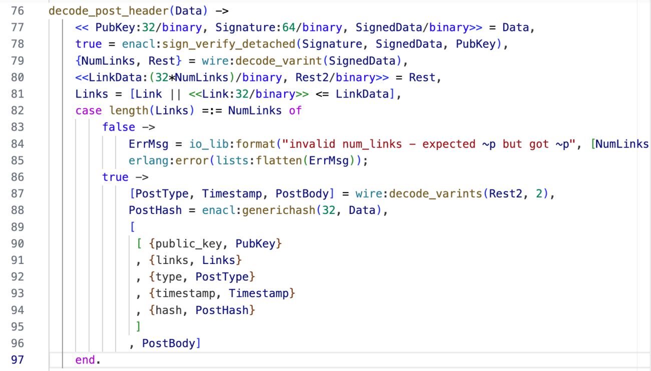
- Took me ca. 21 days (part time)
- Mostly using **gen_server** (internal RPC), **gen_tcp** and SQLite
- ca. 1800 lines of code, including 200 lines of comments
- Error handling: crash and restart automagically
- Pattern match all the things



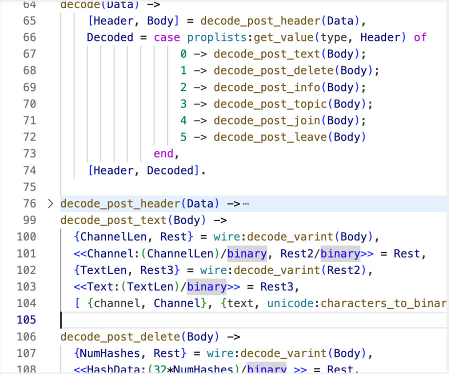
```
event_loop(State = #state{activeOut = ActiveOut, act
    receive
        {stop} -> ok;
        {nodePubKey, From} -> ⋯
        {peerLost, Peer} -> ⋯
        {peerNew, Peer} -> ⋯
        {peerList, From} -> ⋯
        {setOwnNick, From, Nick} -> ⋯
        {readTextsFromChannel, From, Chan} -> ⋯
        {writeTextToChannel, From, Chan, Text} -> ⋯
        {channelsSetTopic, From, Chan, Topic} -> ⋯
        {channelsMembers, From, Chan} -> ⋯
        {channelsJoin, Chan} -> ⋯
        {channelsLeave, Chan} -> ⋯
        {channelsList, From} -> ⋯
        {stateChange, Chan} -> ⋯
        {incomingMsg, Peer, Msg, MsgSize} -> ⋯
    end.
```



```erlang
        {writeTextToChannel, From, Chan, Text} ->
            case maps:is_key(Chan, Chans) of
                false ->⋯
                true ->
                    {ok, Links} = db:get_channel_heads(Db, Chan),
                    Bin = posts:encode(KeyPair, Links, {text, Chan, Text}),
                    {ok, _, PostHash} = db:save_post(Db, Bin),
                    %% find incoming channel time range (type:4) requests which want this post
                    F = fun({Direction, ReqId, Peer}, AccPeers) ->
                                case Direction of
                                    received ->
                                        {Peer, [Header, _]} = maps:get(ReqId, ActiveIn),
                                        case proplists:get_value(msgType, Header) of
                                            4 ->
                                                {ok, {_, _, Size}}
                                                    = send_hash_response(Peer, ReqId, [PostHash]),
                                                update_peer_sent(AccPeers, Peer, Size);
                                            _ -> AccPeers
                                        end;
                                    sent -> AccPeers
                                end
                        end,
                    SentPeers = lists:foldl(F, Peers, maps:get(Chan, Chans)),
                    io:format("[Wrote] #~p: ~p~n", [Chan, Text]),
                    gen_server:reply(From, ok)
```



```
decode_post_header(Data) ->
  << PubKey:32/binary, Signature:64/binary, SignedData/binary>> = Data,
  true = enacl:sign_verify_detached(Signature, SignedData, PubKey),
  {NumLinks, Rest} = wire:decode_varint(SignedData),
  <<LinkData:(32*NumLinks)/binary, Rest2/binary>> = Rest,
  Links = [Link || <<Link:32/binary>> <= LinkData],
  case length(Links) =:= NumLinks of
    false ->
      ErrMsg = io_lib:format("invalid num_links - expected ~p but got ~p", [NumLinks
      erlang:error(lists:flatten(ErrMsg));
    true ->
      [PostType, Timestamp, PostBody] = wire:decode_varints(Rest2, 2),
      PostHash = enacl:generichash(32, Data),
      [
       [ {public_key, PubKey}
       , {links, Links}
       , {type, PostType}
       , {timestamp, Timestamp}
       , {hash, PostHash}
       ]
      , PostBody]
  end.
```



```
decode(Data) ->
  [Header, Body] = decode_post_header(Data),
  Decoded = case proplists:get_value(type, Header) of
         0 -> decode_post_text(Body);
         1 -> decode_post_delete(Body);
         2 -> decode_post_info(Body);
         3 -> decode_post_topic(Body);
         4 -> decode_post_join(Body);
         5 -> decode_post_leave(Body)
       end,
  [Header, Decoded].

decode_post_header(Data) ->⋯
decode_post_text(Body) ->
 {ChannelLen, Rest} = wire:decode_varint(Body),
 <<Channel:(ChannelLen)/binary, Rest2/binary>> = Rest,
 {TextLen, Rest3} = wire:decode_varint(Rest2),
 <<Text:(TextLen)/binary>> = Rest3,
 [ {channel, Channel}, {text, unicode:characters_to_binar

decode_post_delete(Body) ->
 {NumHashes, Rest} = wire:decode_varint(Body),
 <<HashData:(32*NumHashes)/binary >> = Rest,
```

Fin!

- https://cabal.chat
- Spec: https://github.com/cabal-club/cable
- (WIP) Implementations: cable.js[a], cable.rs[b], cabErl[c]
- **‼ -vv**:https://youtu.be/PQvXn6plVHY

[a] https://github.com/cabal-club/cable.js

[b] https://github.com/cabal-club/cable.rs

[c] https://git.sr.ht/~cryptix/caberl