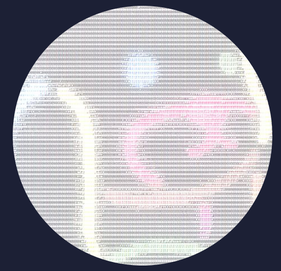
CHANGING THE RECORD: USING SUBSTRATE TO ADD A CUSTOM BLOCKCHAIN TO YOUR IPFS APP

IPFS Camp



Benjamin Kampmann
@gnunicorn

Changing the record

Using substrate to add a custom blockchain to your IPFS Dweb app.

Benjamin Kampmann
Software developer @ Parity Technologies Ltd.

ben@parity.io | @gnunicornBen

How to deploy your dApp?

IPFS **Blogging on the Decentralized Web**

Cool content addresses don't change.

LESSON 1	Link an author to a blog post using its CID
LESSON 2	Update posts with tags and watch their CIDs change
LESSON 3	Build a tag cloud with arrays of links
LESSON 4	Add a new blog post linked to an author and tags
LESSON 5	Add a new tag linked to multiple blog posts
LESSON 6	List posts chronologically with a chain of links
LESSON 7	Traverse through all posts, starting with the most recent

How to “host” that *latest* Cid?

- Through a http server

  But that is centralised again 😒
- Via a DNS entry

  Also centralised … and sooo slooooow 😔
- Libp2p PubSub!

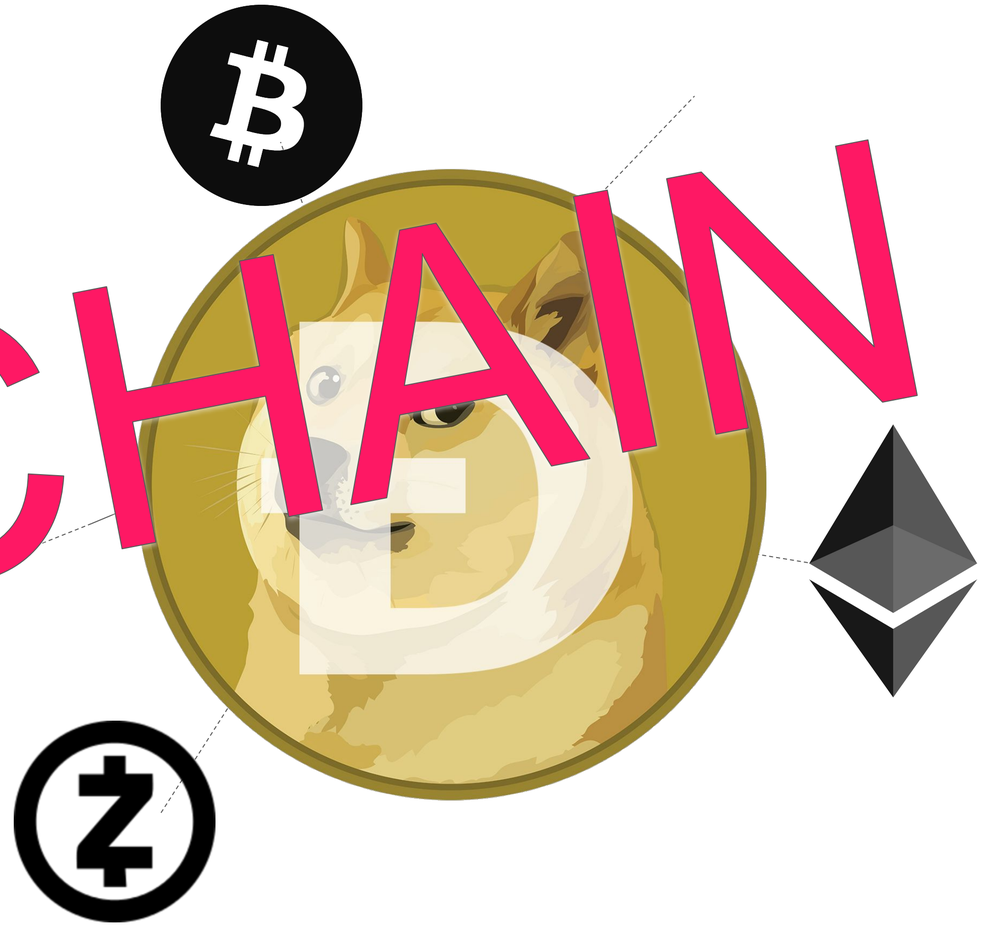
  But allows everyone to write and doesn’t guarantee persistence 😢

Features of our “hoster”

- Global record
- decentralised
- simple KV-datastore
- permissioned rw-access

BLOCKCHAIN

Decentralised
registry (DB)



parity

What is blockchain?

- effectively a distributed state-machine
- with a predefined transition agreement system “consensus”
- of sets of transactions, packaged as “blocks”
- based on a historic record, the “chain”
- `Block->Block->Block->…->GenesisBlock`

Smart-Contract-Chain

+ Existing stable network(s)
+ Rel. easy to build & deploy
- Bound to their primitives
- Smart Contract Model
- Limited control over scaling issues & costs: Everything costs the user

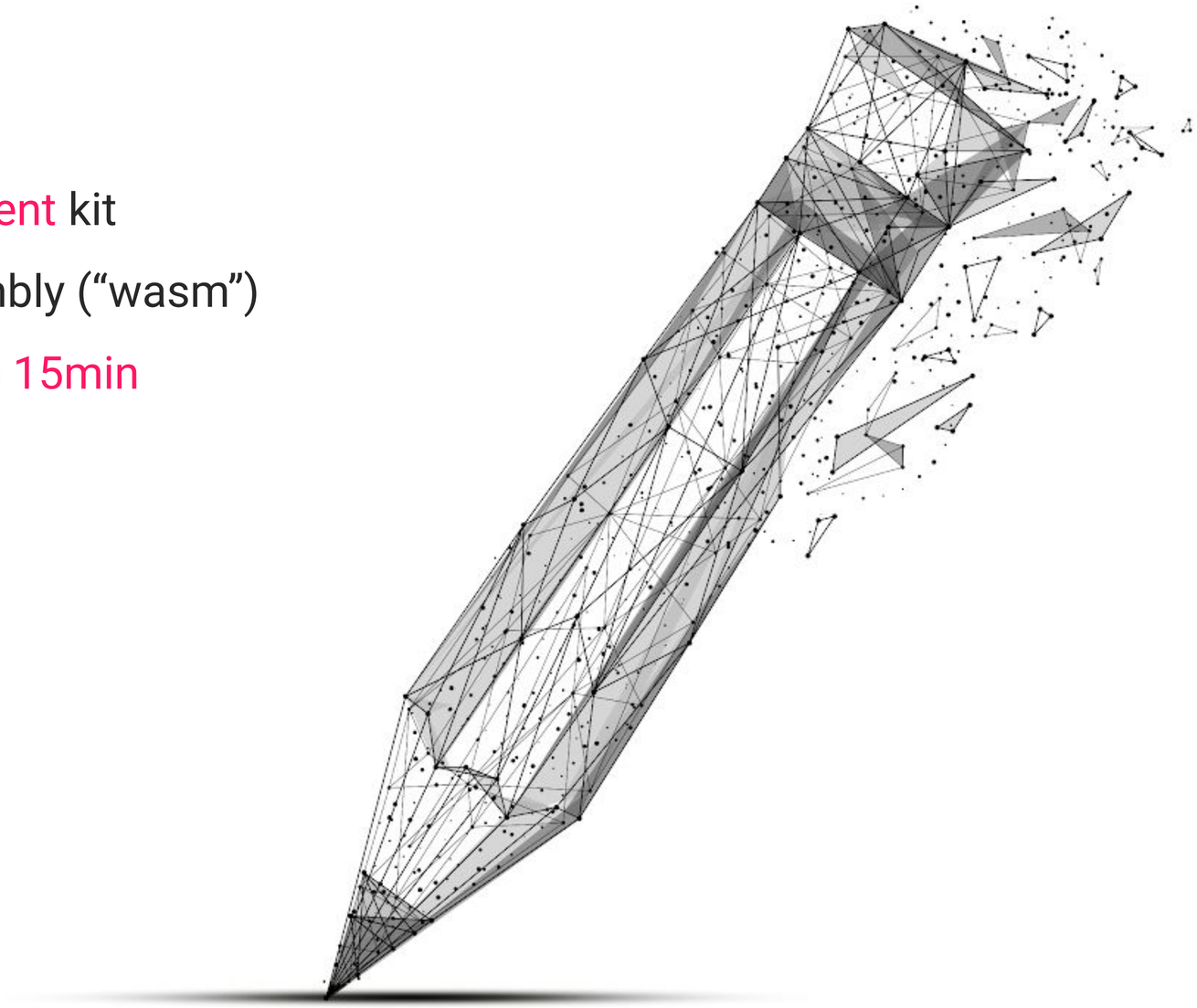
Self-Made Chain

+ Full control over: code, primitives, economics, scalability & costs
- Usually a lot of work
- Needs its own network
- Incompatible with existing networks

parity

Substrate ...

- … is a general purpose blockchain development kit
- … is written in type-safe Rust and WebAssembly (“wasm”)
- … let’s you get started with your own chain in 15min



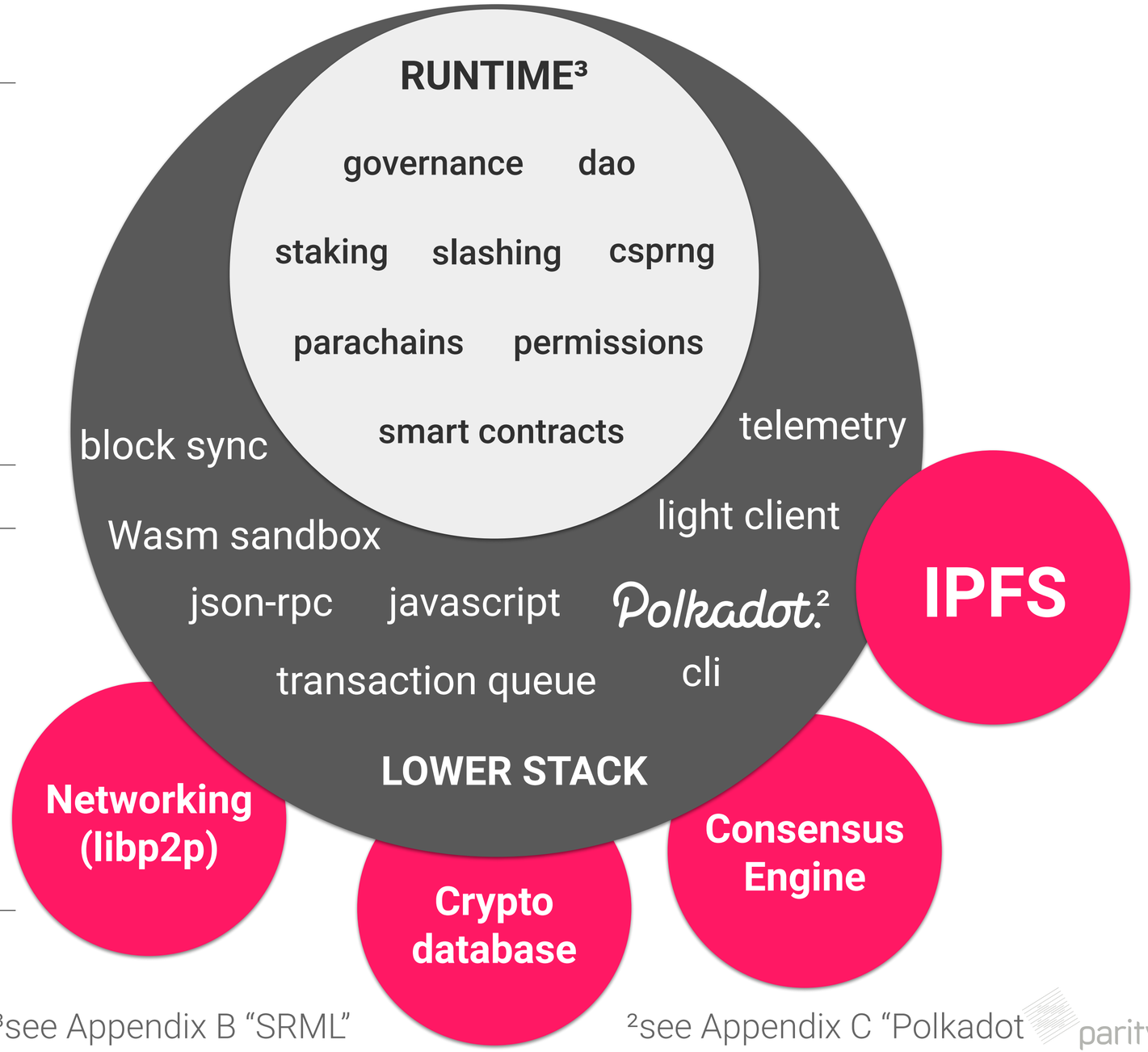
CHAIN-SPECIFIC RUNTIME

Stored & upgradable as WASM-Blob *on-chain**

*(*see Appendix A)*

CLIENT INFRASTRUCTURE

Everything you need to run a blockchain



Architecture of Substrate

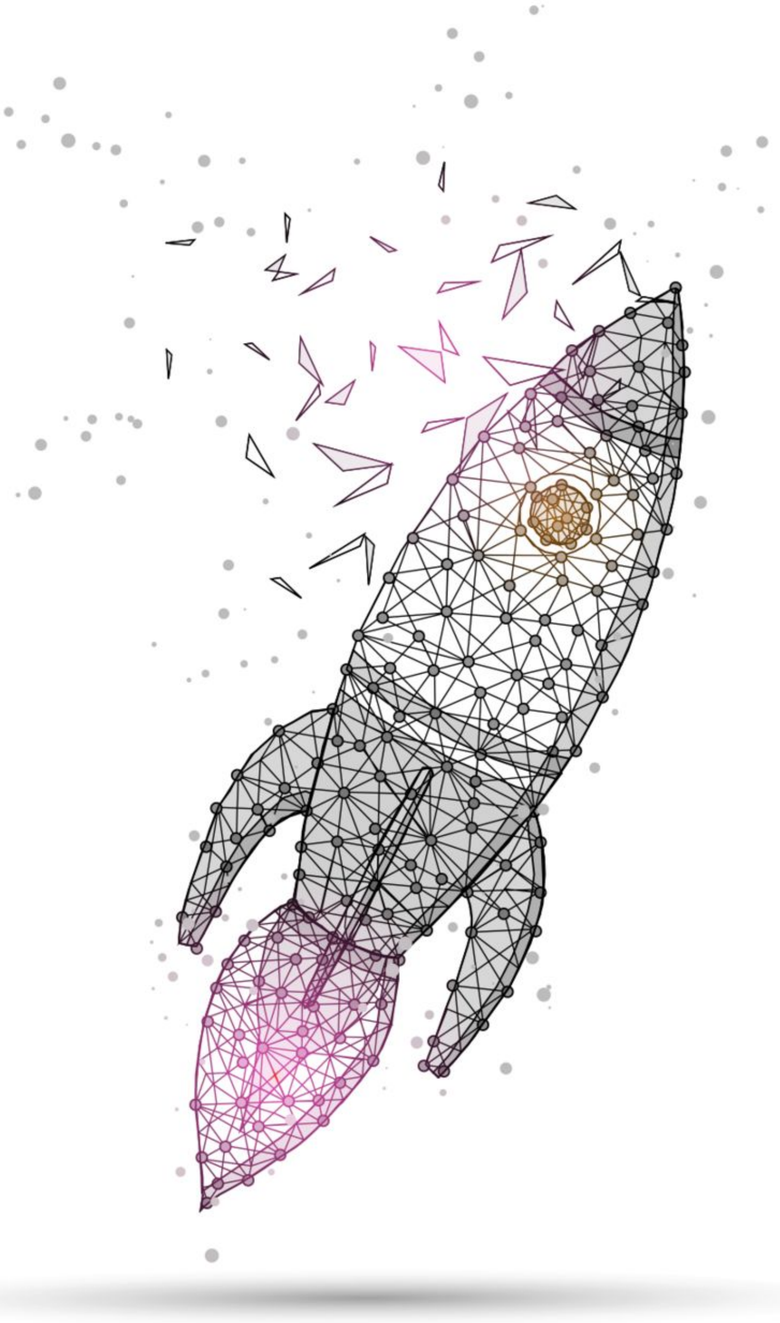
[3]see Appendix B “SRML”

[2]see Appendix C “Polkadot

parity

Get Substrate and launch your chain!

parity.io/substrate



learn substrate
tomorrow @unconf

Thursday
July 4th
12pm - 5.30pm

Carrer de Pau Claris,
162,
Barcelona

Substrate Workshop

Build a Custom Blockchain

Parity updates and events

parity.io/newsletter

ben@parity.io || @gnunicornBen

Appendix A

Forkless live runtime upgrades

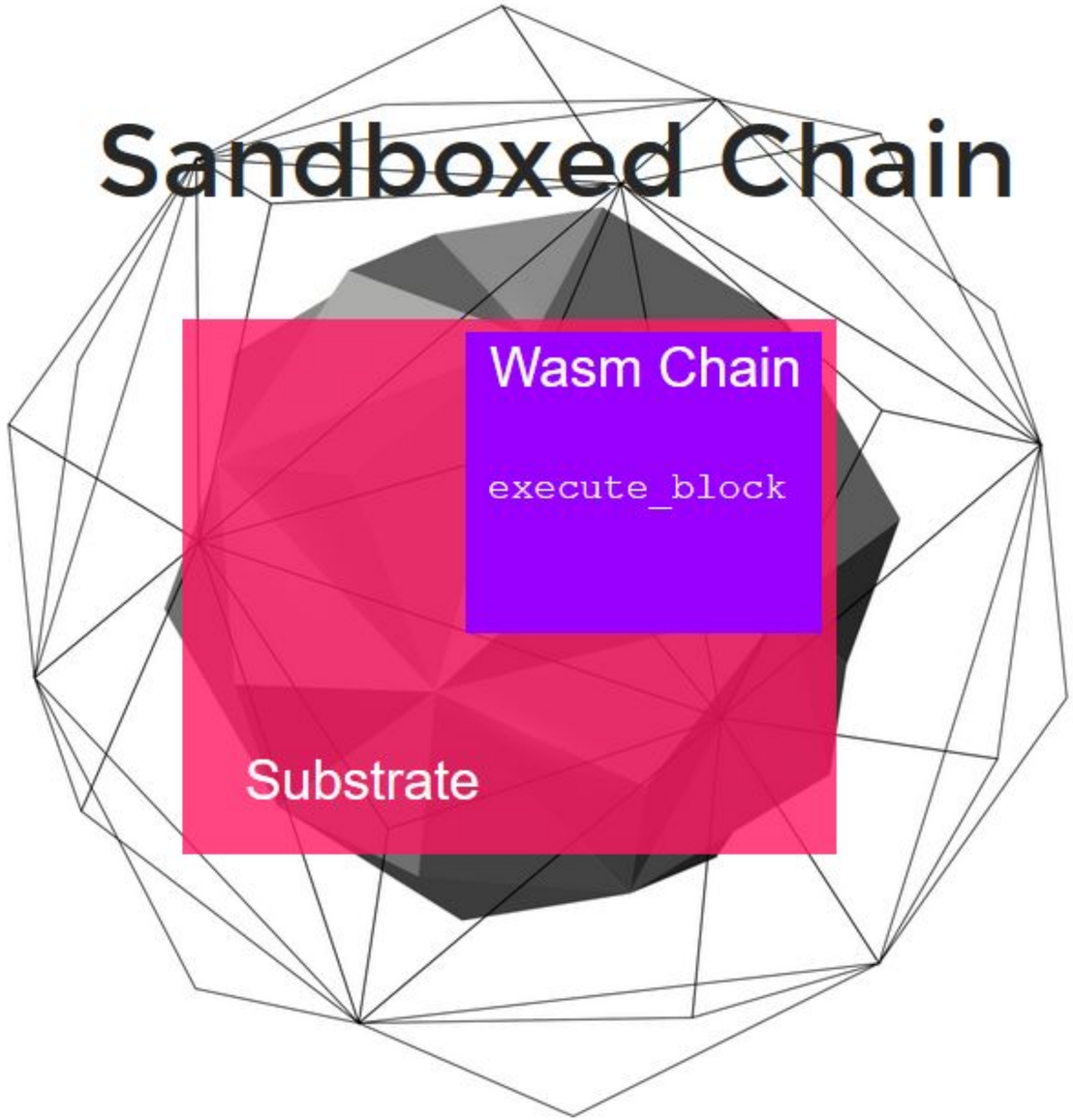
Runtime is compiled to WASM & stored at `:code`

WebAssembly ...*"wasm"*

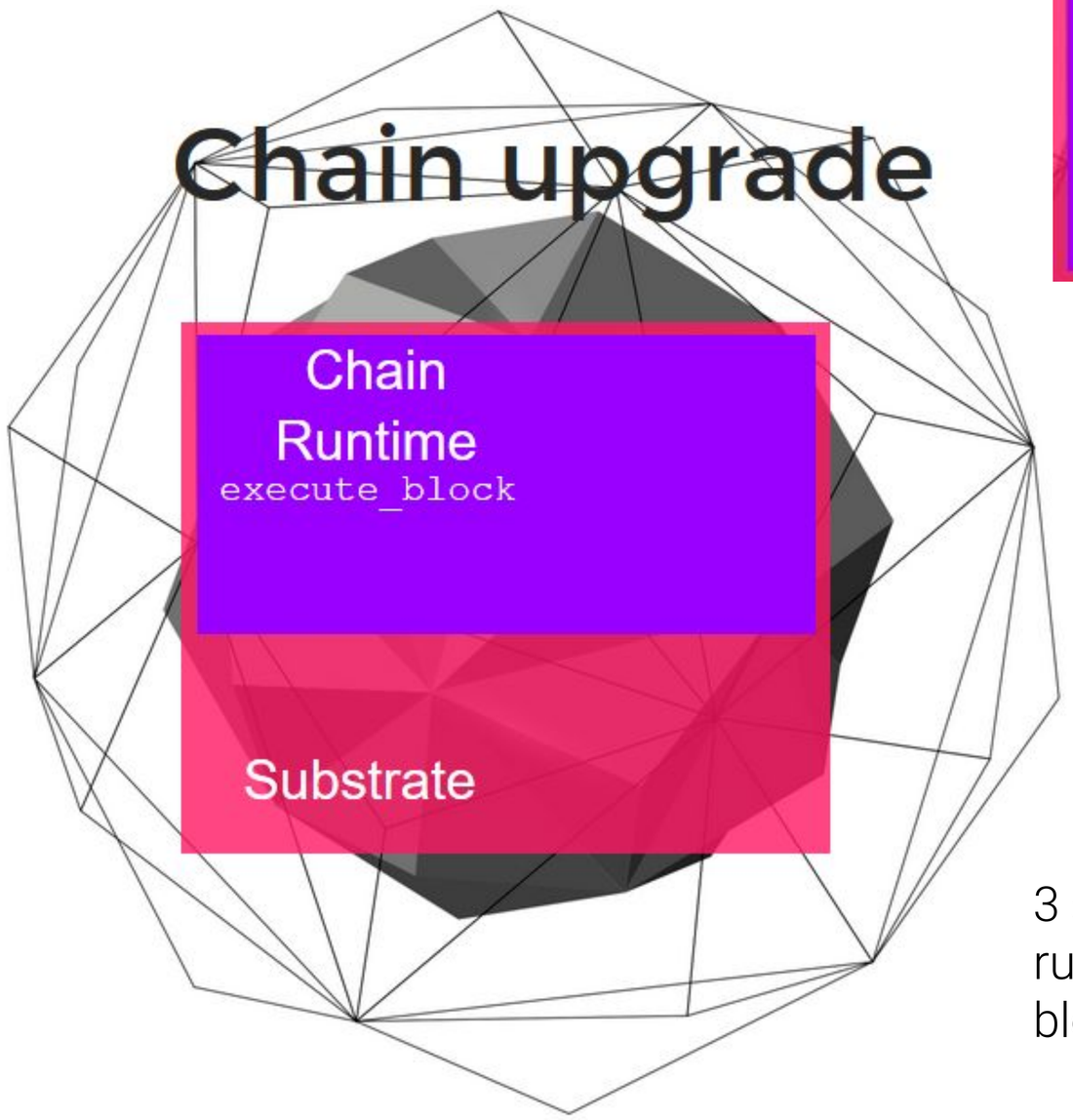
.. is a web standard for an assembly like compile-target to run code in Web Browsers as almost native speed

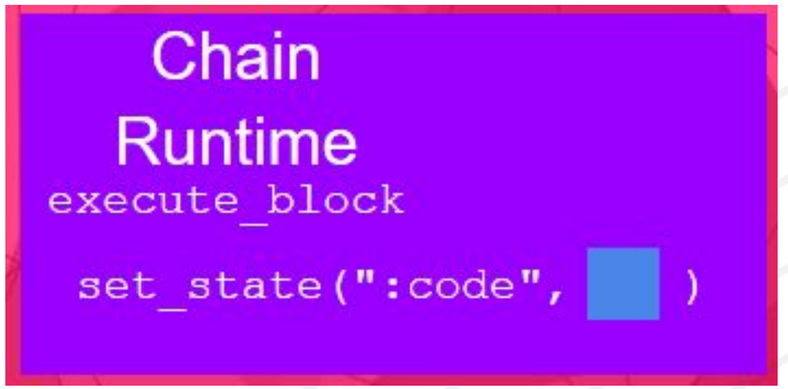
.. can be compiled to from many system languages (C, C++, rust, ...)

.. is execute in a sandboxed virtual environment



parity





1 a block comes in that triggers a set of :code

2 When the next block comes

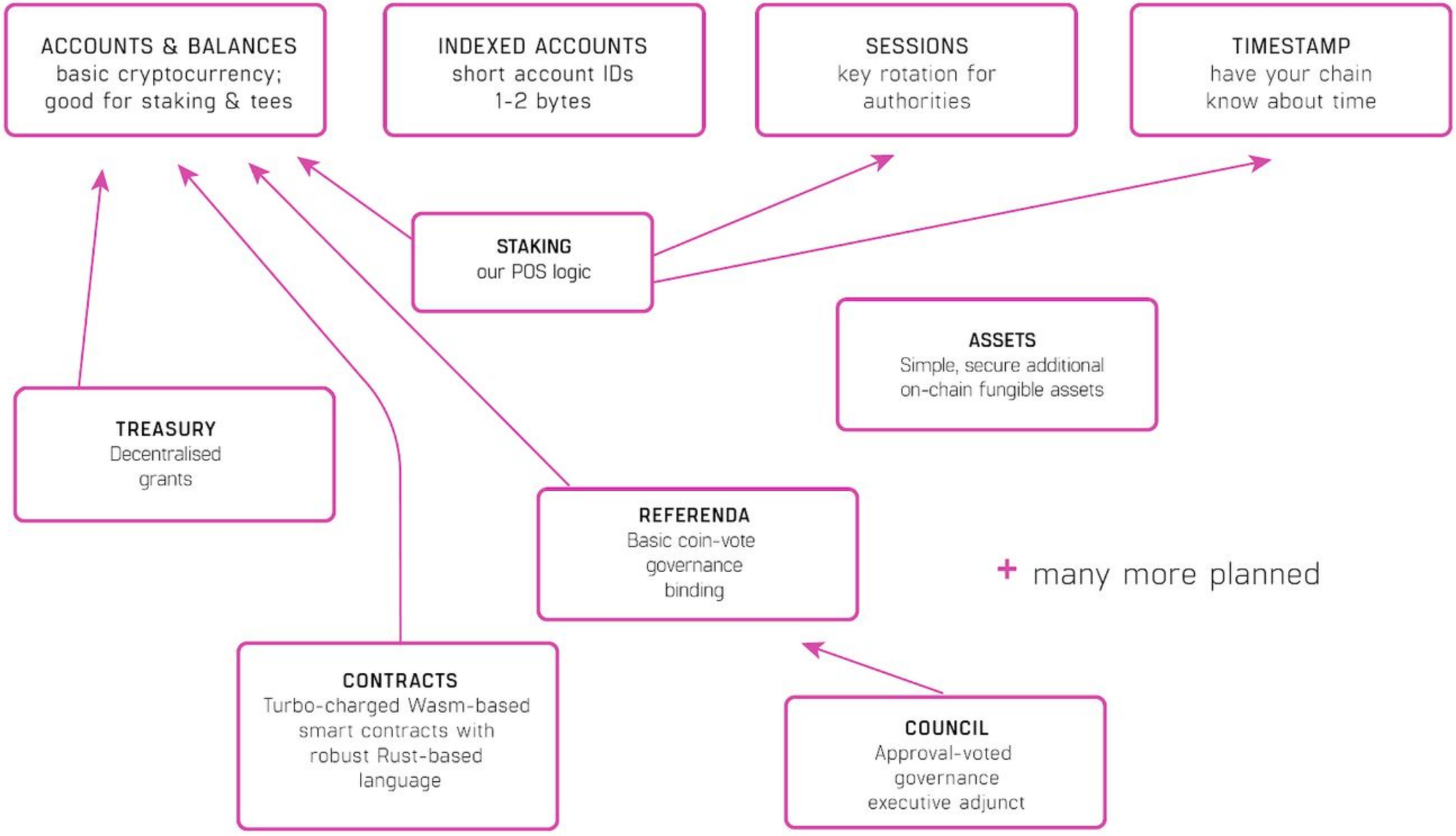
3 substrate notices the new runtime and executes the new block with it from now on

And as all clients have agreed on the new `:code` on-chain, they must execute it or can't author blocks anymore.

Of course, you can still fork, but it doesn't happen by accident anymore - Substrate itself comes with a Wasm Executor that will be used to run the code if the native version isn't sure it is compatible. From a passive threat, forking now requires intervention and makes it an active act.

Appendix B

Substrate Runtime Module Library
(SRML)


ACCOUNTS & BALANCES
basic cryptocurrency;
good for staking & tees
INDEXED ACCOUNTS
short account IDs
1-2 bytes
SESSIONS
key rotation for
authorities
TIMESTAMP
have your chain
know about time
STAKING
our POS logic
ASSETS
Simple, secure additional
on-chain fungible assets
TREASURY
Decentralised
grants
REFERENDA
Basic coin-vote
governance
binding
+ many more planned
CONTRACTS
Turbo-charged Wasm-based
smart contracts with
robust Rust-based
language
COUNCIL
Approval-voted
governance
executive adjunct

Appendix C

polkadot.network

Polkadot is ...

... a heterogeneous multi-chain technology.

... a protocol that allows independent blockchains to exchange information.

... an interoperability layer, that enforces order and the validity of the messages between the chains

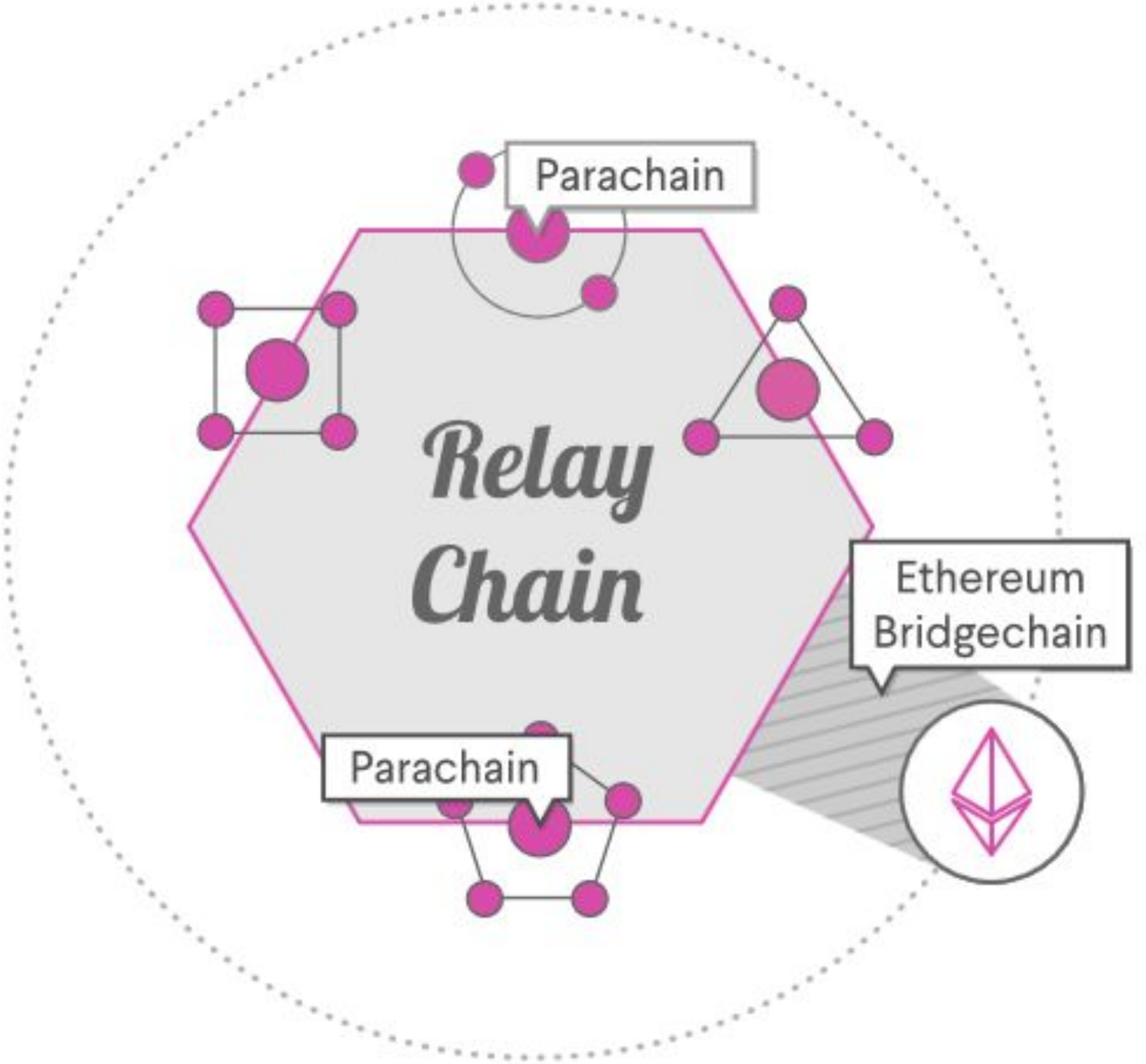
polkadot.network

but how?

Relay Chain, a blockchain which relays messages of other chains, at the core of network.

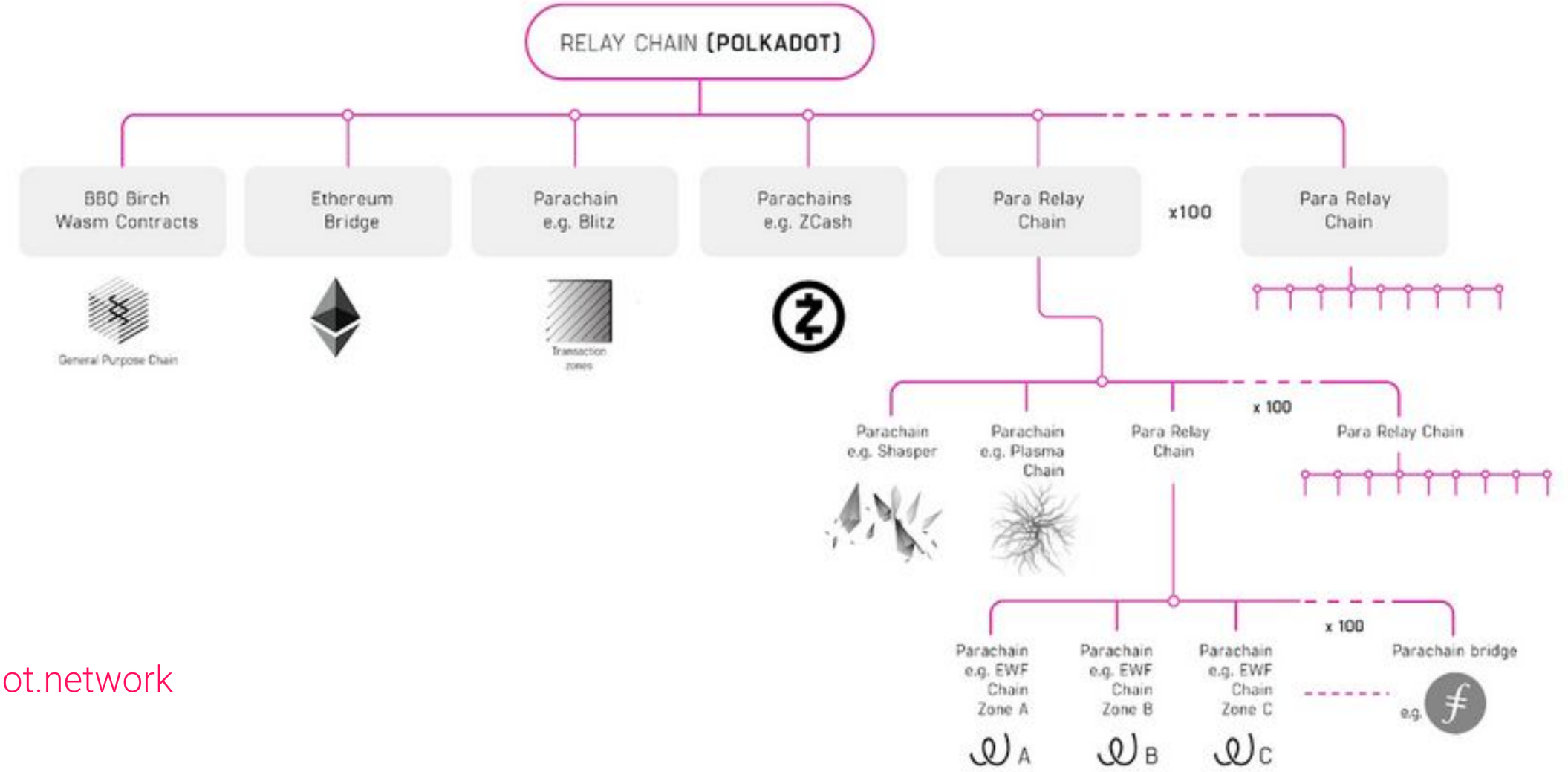
Parachains are separate chains run in and with direct knowledge of polkadot.

& bridges allow interactions with 3rd Party chains.



polkadot.network

Composable



polkadot.network