



*Polkadot.*

# Saison été : Substratosphere



Découverte de Polkadot



# Meetups B612 Crypto Lyon

- Série de meetup initié François Guezengar (Dapps Nation)
- A venir, saison été animé par



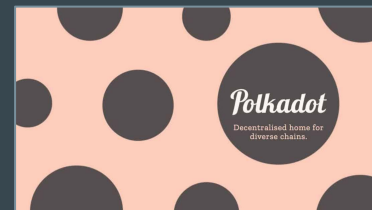
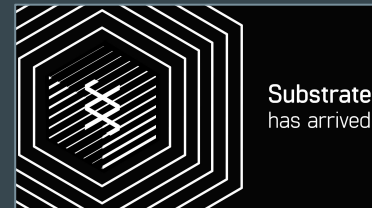
François Branciard



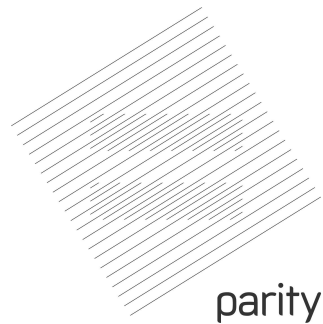
Vladimir Ostapenco

# Saison Été : Substratosphere

- Découverte de Substrate
  - B612 - 12/06/2019
- Découverte de Polkadot
  - B612 - 19/06/2019
- Devenez un validateur Polkadot sur le testnet
  - B612 - 26/06/2019



# Who is involved?



## Polkadot in 1 sentence

**Polkadot is a heterogeneous multi-chain technology.**

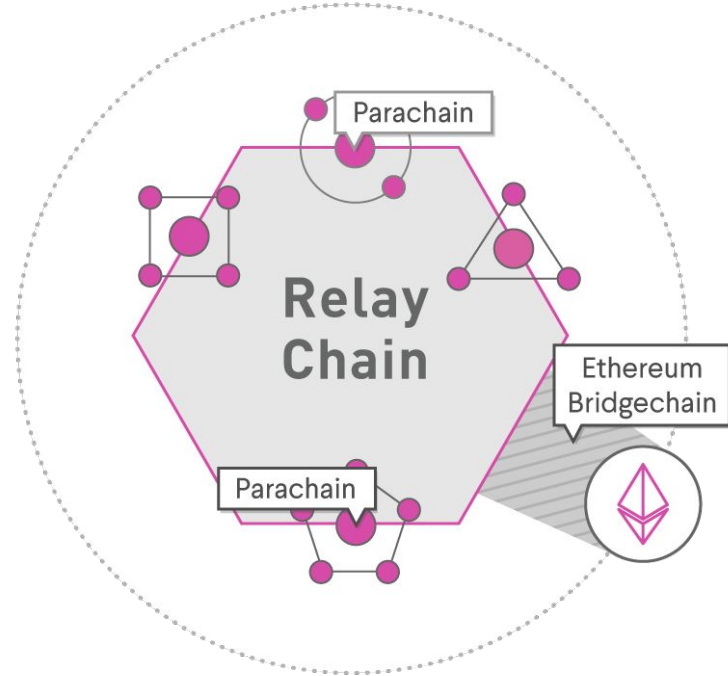
<https://polkadot.network/>



# POLKADOT APPROACH

○ ○ ○ ○ RELAY-CHAIN  
provides pooled security and  
passes messages

○ ○ ○ ○ PARACHAINS  
contain logic and handle  
transactions



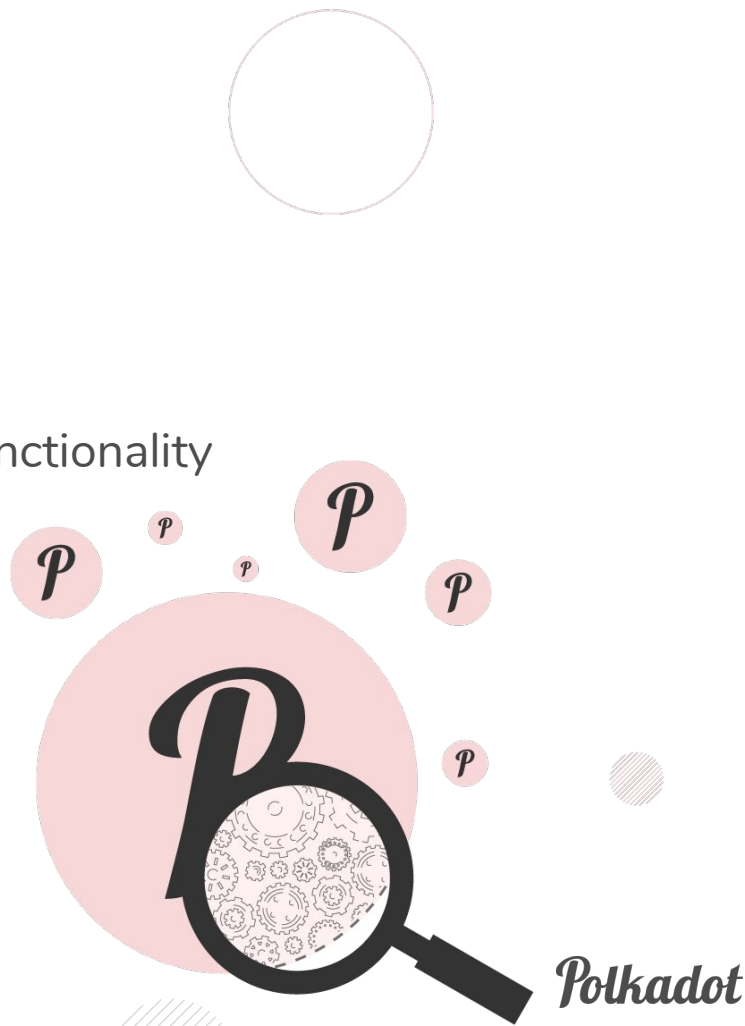
# RELAY CHAIN



Only consensus and governance functionality



Parachain validation logic



# PARACHAINS



Fully validated state machines



Independent public bridge chains



Independent private bridge chains





# WHO POWERS IT?



## VALIDATORS

Verify parachain transactions and pass messages



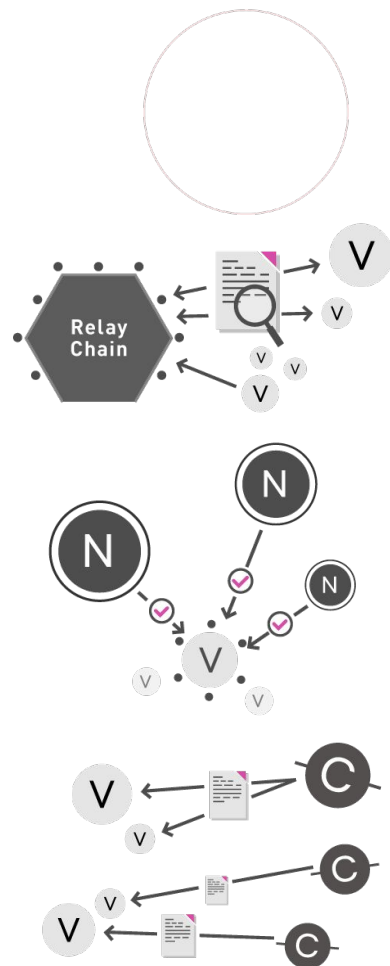
## NOMINATORS

Select good validators and increase economic security



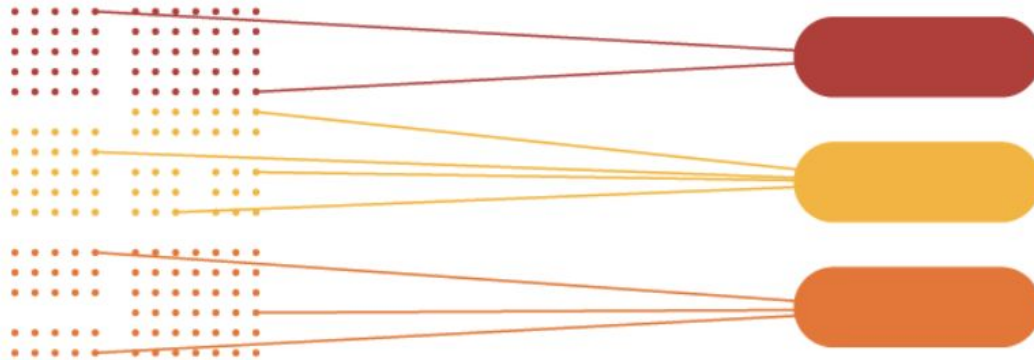
## COLLATORS

Prepare parachain candidates and proofs of validity

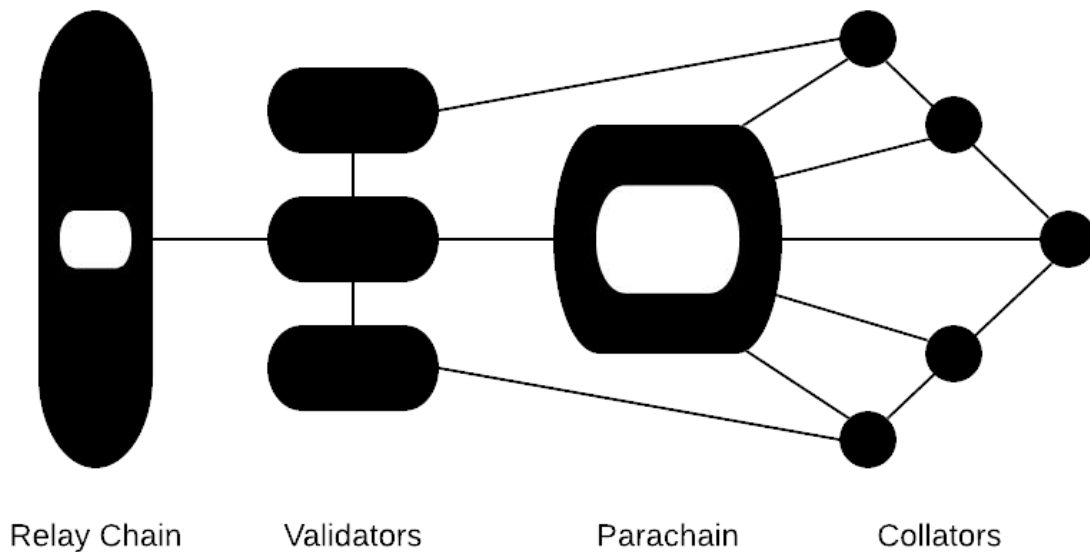


Nominators

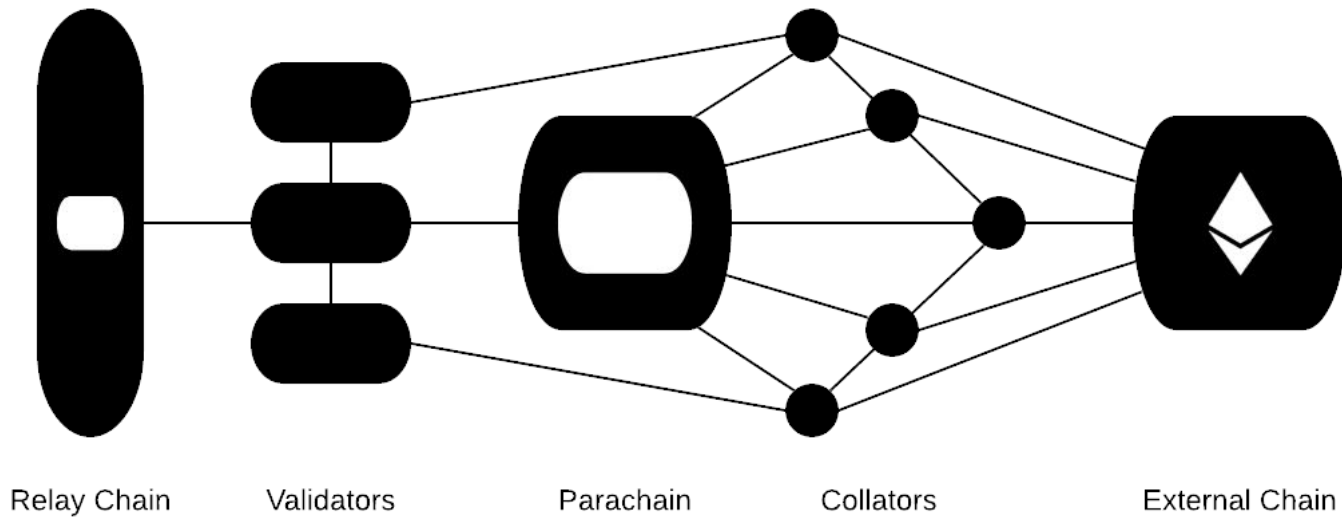
Validators



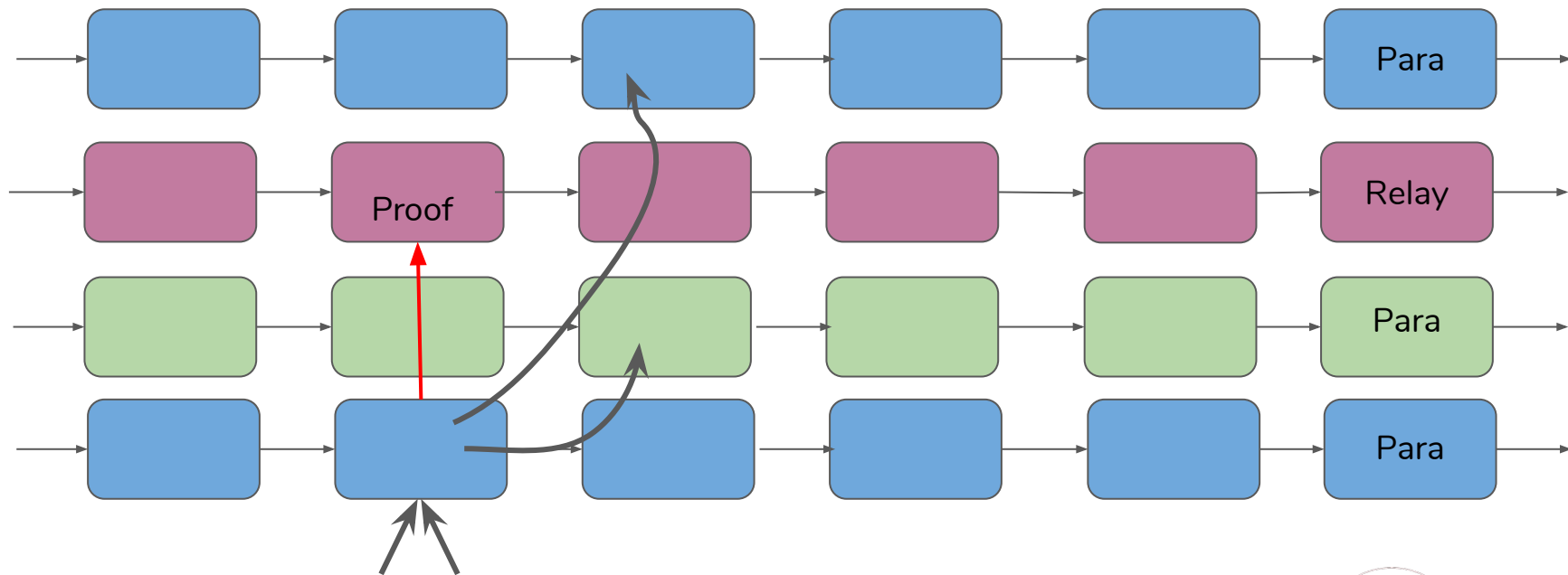
# One Parachain



# Bridged Parachain

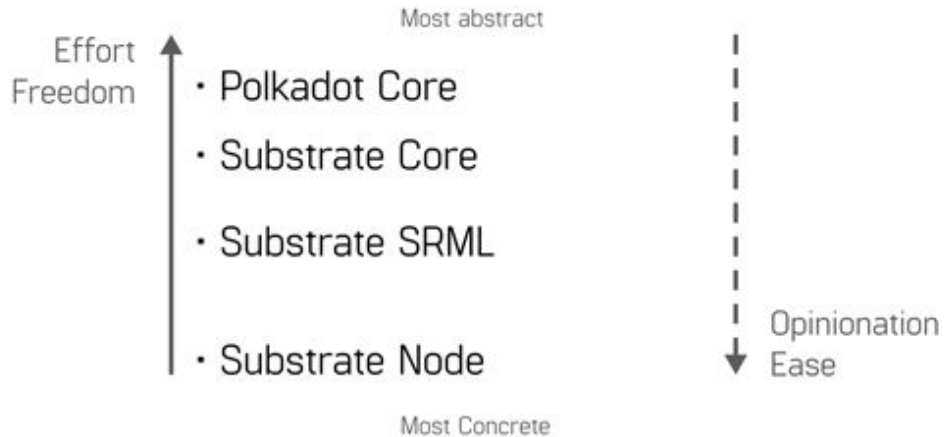


# Future - Polkadot (Multichain)

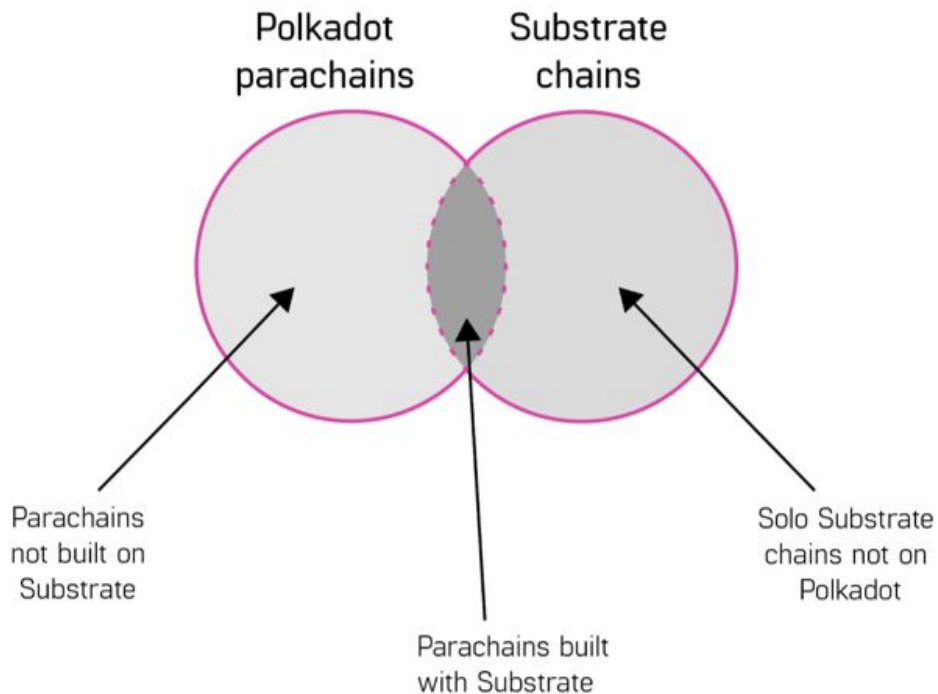


# Polkadot - Substrate : who's who

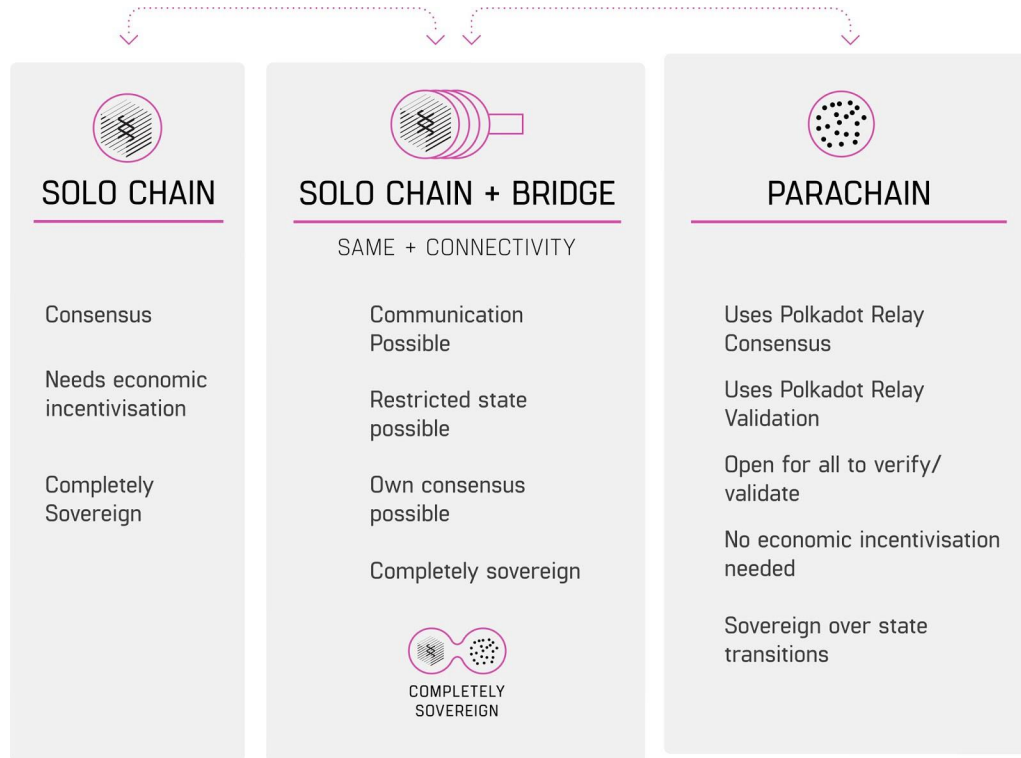
You choose!



# Polkadot - Substrate : who's who

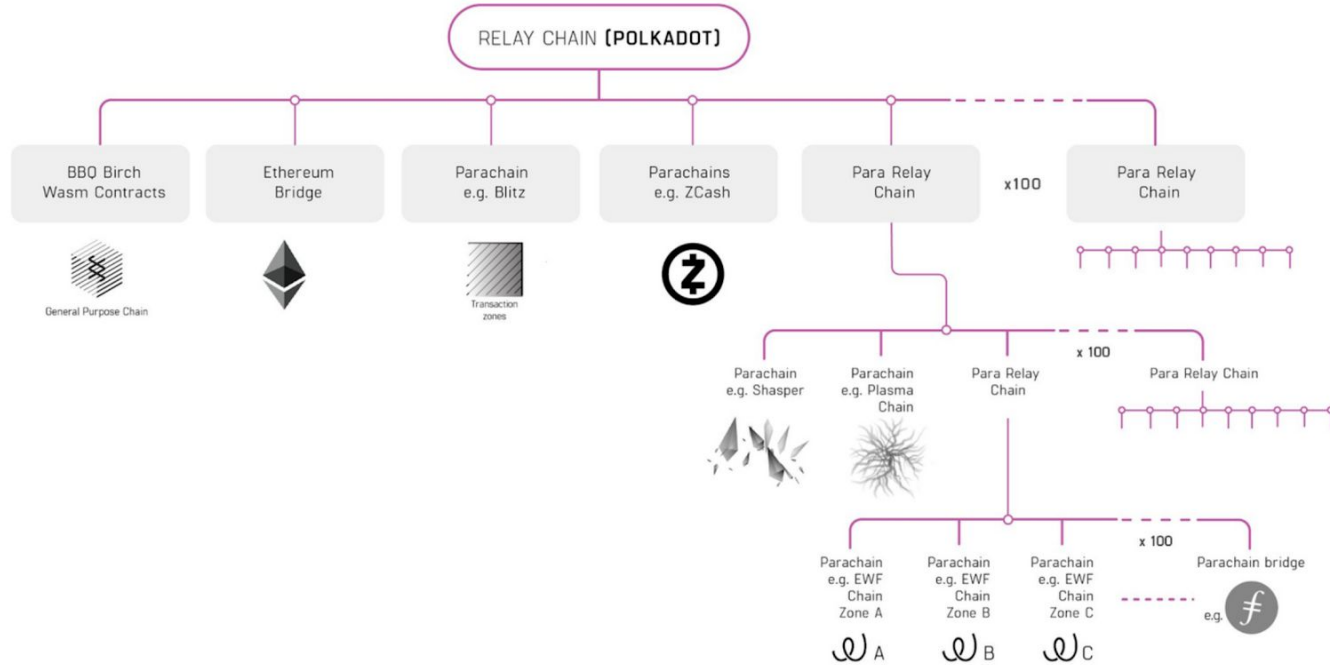


# Possible manifestations of Substrate-based chains.





# Parachains exemples view



# Parachains esthetic view



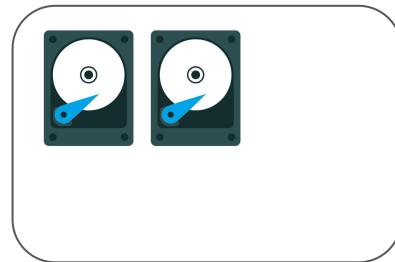
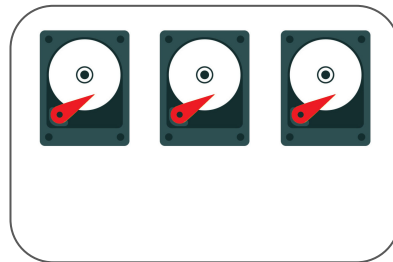
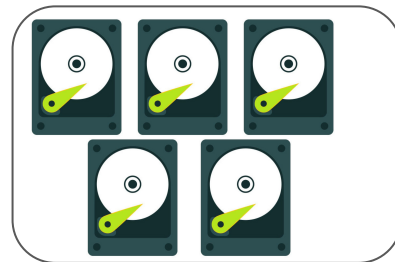
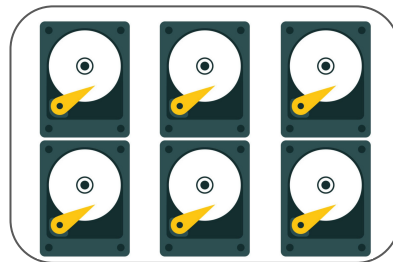
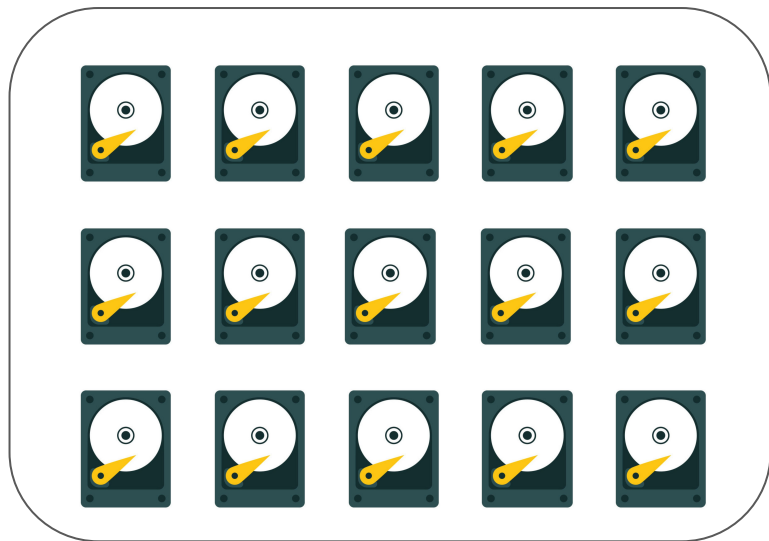
# The Problems

## Problems

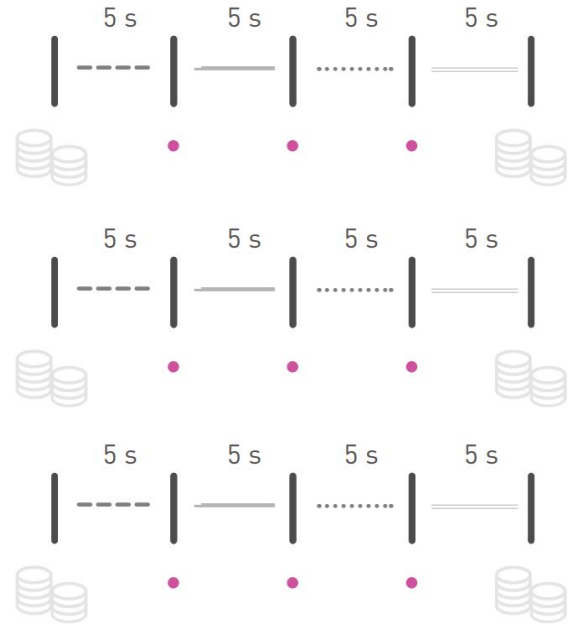
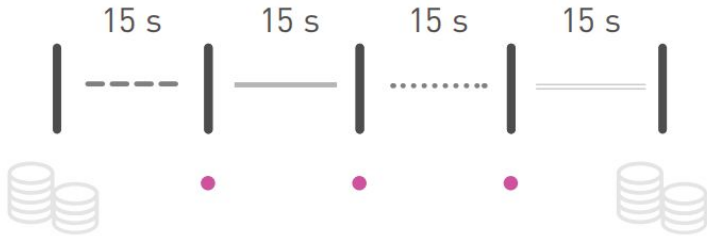
- Scalability
  - Store everything forever & TX per second is low.
- Interoperability
  - Chains can't talk to each other.
- Speed
  - The EVM is inefficient.
- Security
  - Must find new miners for each new chain.
- Privacy
  - Data is public.
- Developability
  - Creating a new chain could be easier.
- Governance
  - Messy with inconsistent coverage.



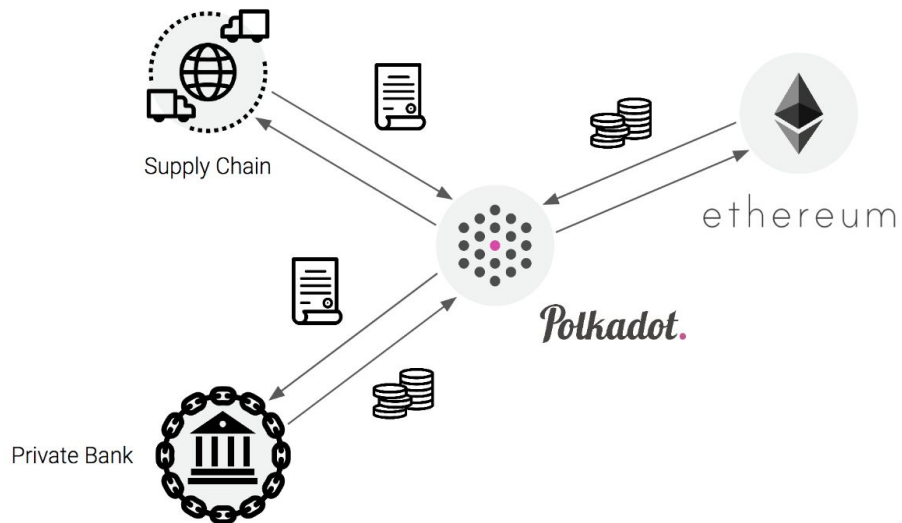
# Scalability - 1 (storage)



# Scalability - 2 (TX/s)



# Interoperability



Polkadot.

# Speed

EVM

256 bit



256 bit

Native || WASM

32 bit



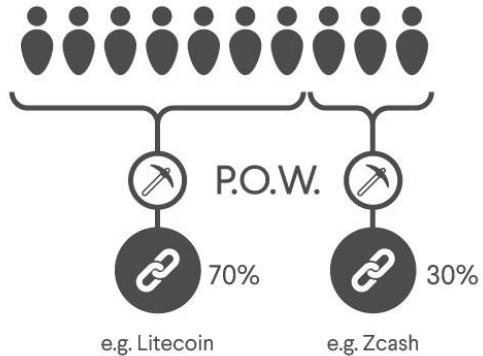
32 bit

WEB3

Polkadot.

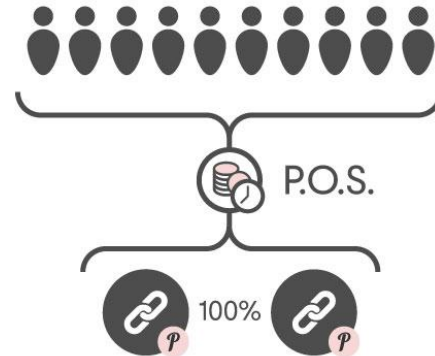
# Isolated Vs. Shared Security

Traditional isolated security



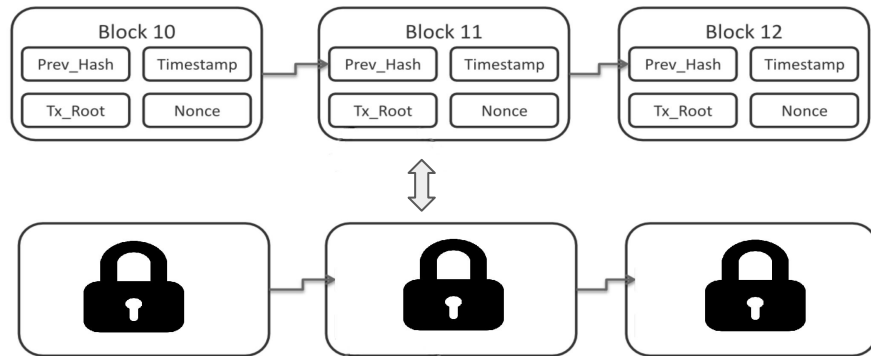
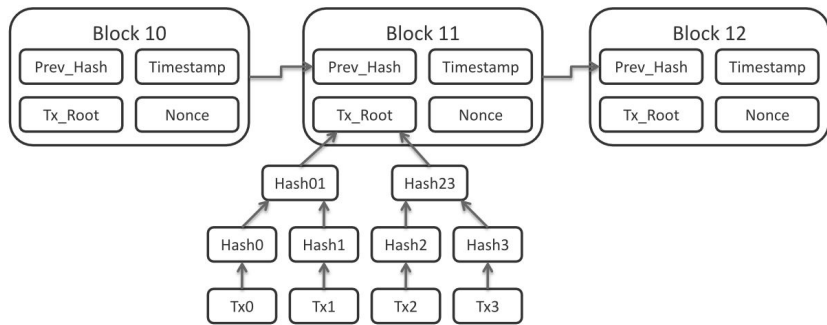
V.S.

Polkadot shared security



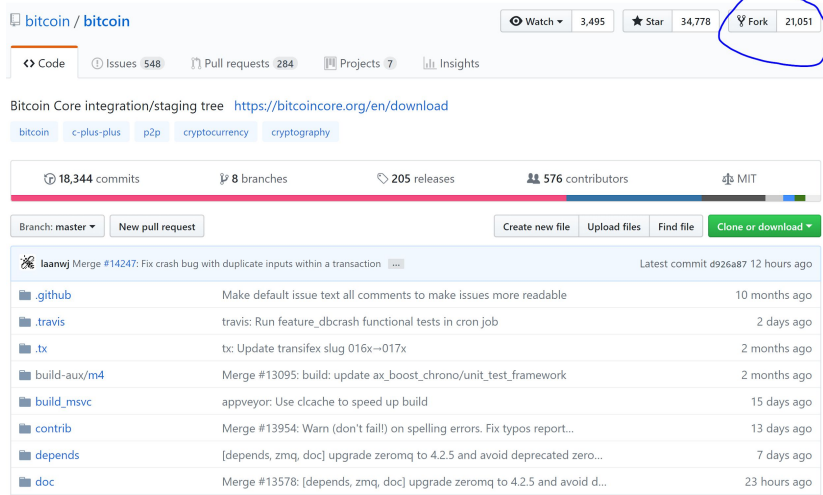


# Privacy



# Developability

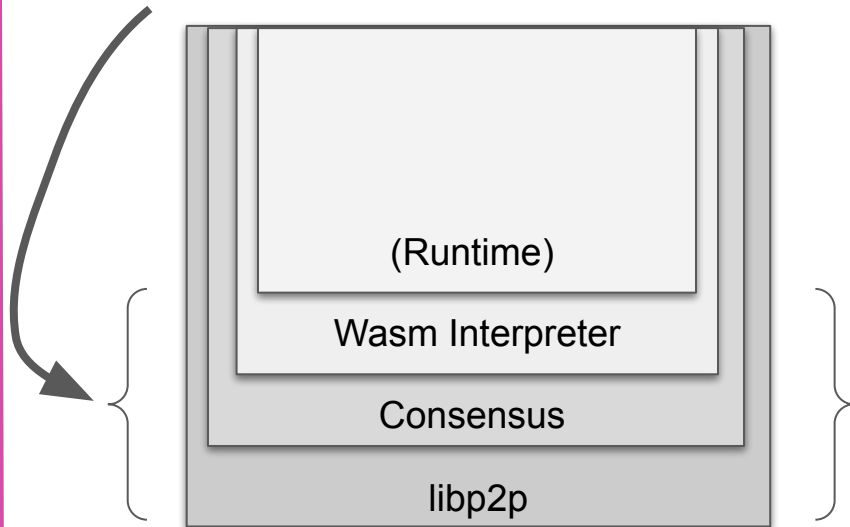
## Copy-Paste Coin



The screenshot shows the GitHub repository for Bitcoin. The repository name is "bitcoin / bitcoin". It has 3,495 watches, 34,778 stars, and 21,051 forks. The "Fork" button is circled in blue. Below the repository name, there are tabs for "Code", "Issues", "Pull requests", "Projects", and "Insights". The "Code" tab is selected. Below the tabs, there is a link to the Bitcoin Core integration/staging tree: <https://bitcoincore.org/en/download>. Below the link, there are tags for "bitcoin", "c-plus-plus", "p2p", "cryptocurrency", and "cryptography". Below the tags, there is a bar showing 18,344 commits, 8 branches, 205 releases, 576 contributors, and MIT license. Below the bar, there is a "Branch: master" dropdown and a "New pull request" button. Below the dropdown and button, there are links for "Create new file", "Upload files", "Find file", and "Clone or download". Below the links, there is a list of recent commits. The first commit is by "laanwj" with the message "Merge #14247: Fix crash bug with duplicate inputs within a transaction" and the latest commit is "d926a87" 12 hours ago. Below the first commit, there is a list of files: ".github", ".travis", ".tx", "build-aux/m4", "build\_msvc", "contrib", "depends", and "doc". Each file has a description and a time ago.

File	Description	Time ago
.github	Make default issue text all comments to make issues more readable	10 months ago
.travis	travis: Run feature_dbcrash functional tests in cron job	2 days ago
.tx	tx: Update transifex slug 016x-017x	2 months ago
build-aux/m4	Merge #13095: build: update ax_boost_chrono/unit_test_framework	2 months ago
build_msvc	appveyor: Use ccache to speed up build	15 days ago
contrib	Merge #13954: Warn (don't fail!) on spelling errors. Fix typos report...	13 days ago
depends	[depends, zmq, doc] upgrade zeromq to 4.2.5 and avoid deprecated zero...	7 days ago
doc	Merge #13578: [depends, zmq, doc] upgrade zeromq to 4.2.5 and avoid d...	23 hours ago

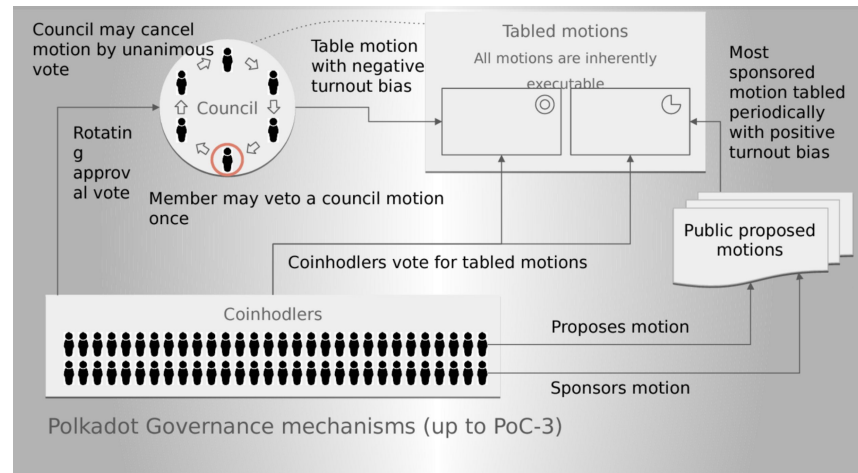
## Polkadot Runtime Environment



WEB3

Polkadot.

# Governance



# The Solutions

## Problems

- Scalability
  - Many chains in parallel.
- Interoperability
  - Arbitrary messaging across chains.
- Speed
  - Native execution
- Security
  - Shared security
- Privacy
  - Private parachains
- Developability
  - Polkadot Runtime Environment SDK
- Governance
  - On-chain binding governance



# Where are we now?

- **PoC-1:** Governance, staking, basic UI, and forkless upgrades
- **PoC-2:** “co-finalization” of non-communicating parachains and basic light client
- **PoC-3:** Implementation of hybrid consensus
- **PoC-4:** Full stacking; Nominated Proof of Stake scheme

# What's Next?

- **PoC-5:** Interchain message passing, Cumulus (Substrate chains can become parachains)
- **PoC-6-8:** Implementation of Validity/Availability game
- **In parallel:** developer tools for parachains



# Demo

- Polkadot Testnet Explorer
  - <https://polkadot.js.org/apps/#/explorer>
- Polkadot Telemetry
  - <https://telemetry.polkadot.io/#list/Alexander>



# Some cool technical details

- Babe : <https://wiki.polkadot.network/en/latest/polkadot/learn/randomness/>
- Grandpa : <https://wiki.polkadot.network/en/latest/polkadot/learn/consensus/>
- Npos: <https://wiki.polkadot.network/en/latest/polkadot/learn/phragmen/>
- Slots: <https://wiki.polkadot.network/en/latest/polkadot/learn/auction/>
- Crypto: <https://wiki.polkadot.network/en/latest/polkadot/learn/cryptography/>