Polkadot.

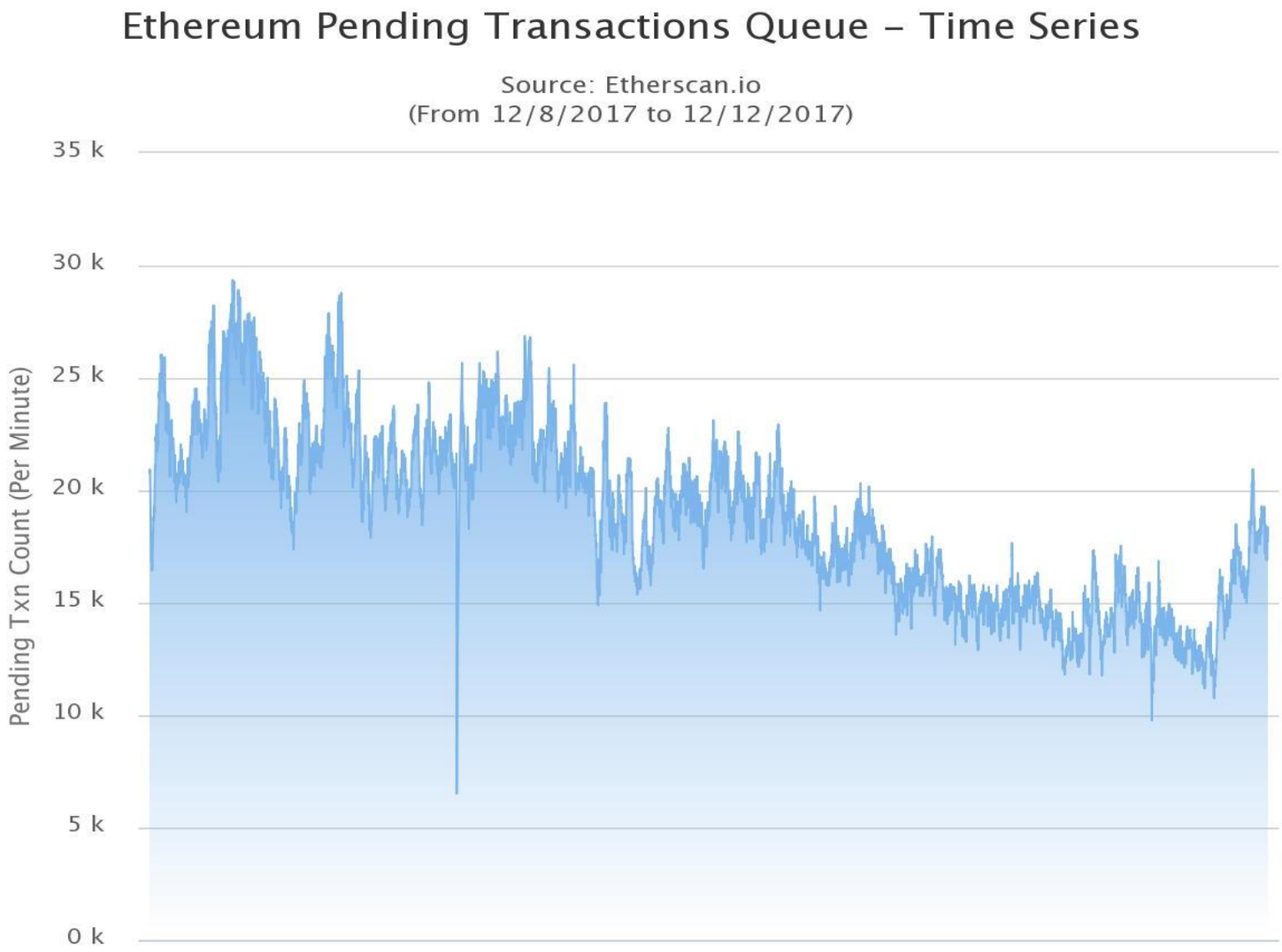
Presentado por
Alberto Ballesteros

Blockchain

- *Blockchains* como gran promesa de utilidad en distintos ámbitos.
  - IoT, descentralización de la web, finanzas, gestión de la identidad…
- Proyectos:
  - Abiertos y con alta funcionalidad (*Ethereum*)
  - De carácter privado (*Zcash*)
  - Operar en privado (Carácter empresarial)
- ¿Despliegue en el mundo real?

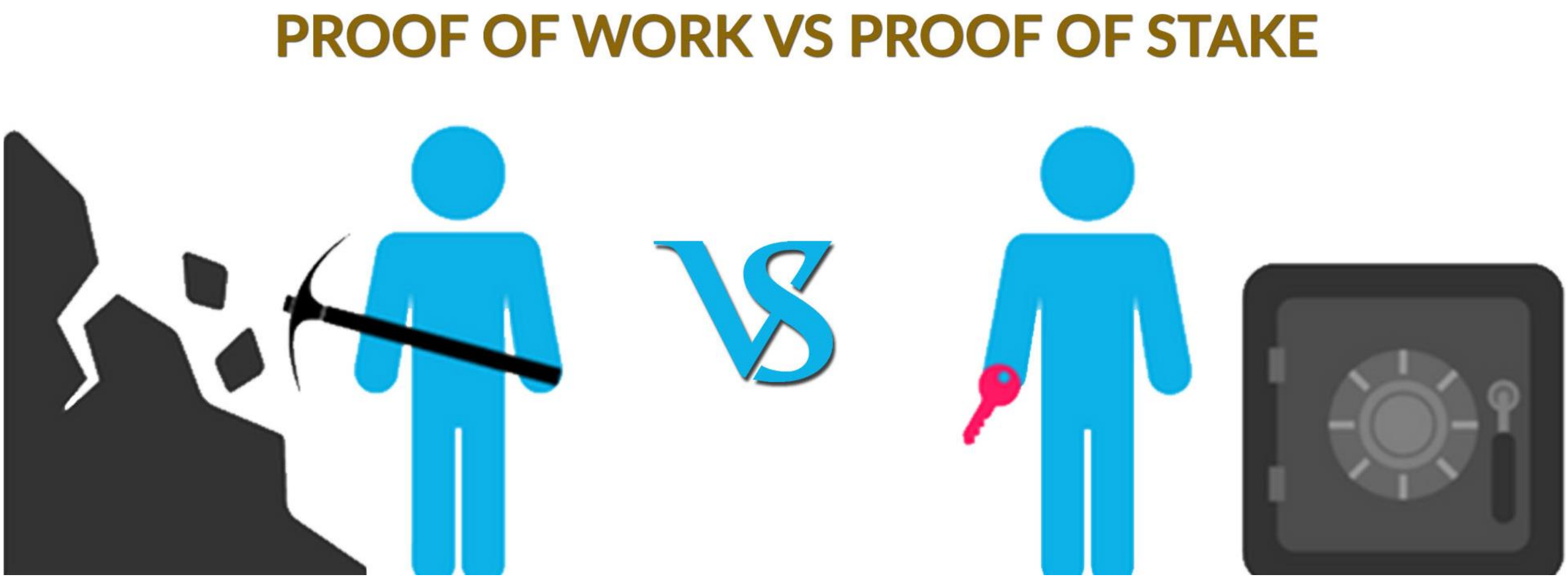
Key points - Escalabilidad

- ETH - https://etherscan.io/txsPending
- BTC - https://blockchain.info/charts/mempool-count



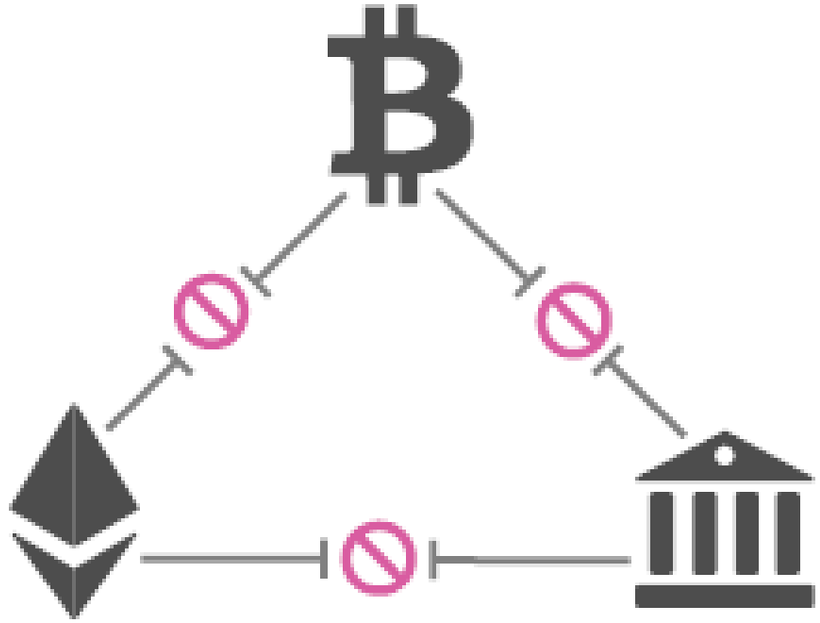
Key points - Gobernanza

- Recompensa a pocos a costa de muchos.



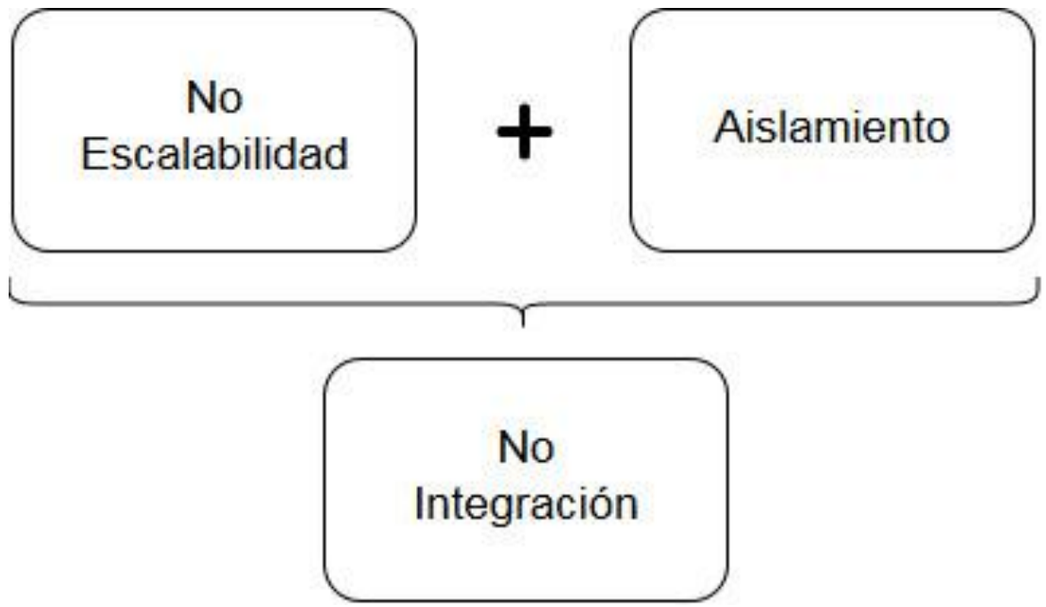
Key points - Aislamiento

- *Blockchains* independientes y aisladas.
- No existe comunicación entre ellas.



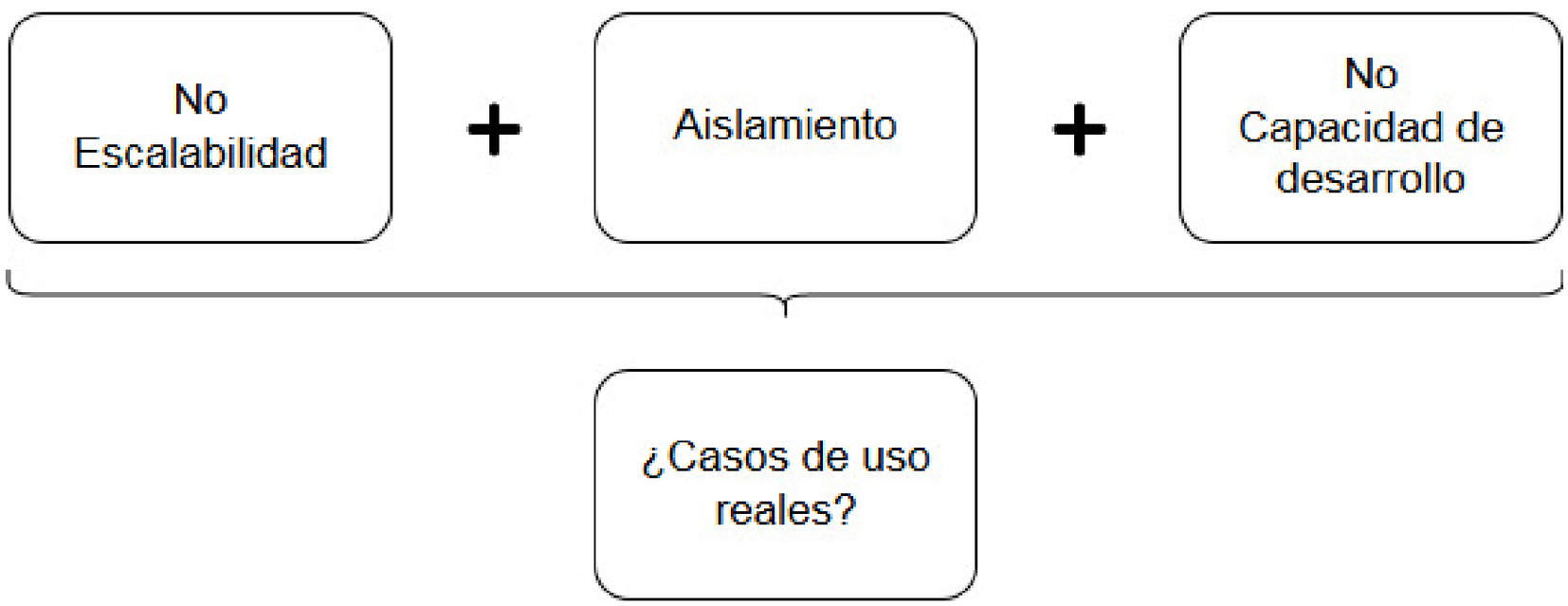
Key points – Capacidad de desarrollo

- Creación de aplicaciones descentralizadas (DApps) limitada.



Key points – Aplicabilidad

- *Blockchain* sigue siendo un planteamiento teórico en muchos casos.
- Existe una brecha entre la tecnología y las aplicaciones reales.



¿Qué es Polkadot?

- Es una red que conecta *blockchains*.
- No tiene en cuenta la tipología de las cadenas.
- Considera todas y cada una de igual forma para que interactúen entre sí.
- Gran red *multi-chain* interoperable e inclusiva con seguridad agrupada.

¿Qué viene a resolver Polkadot?

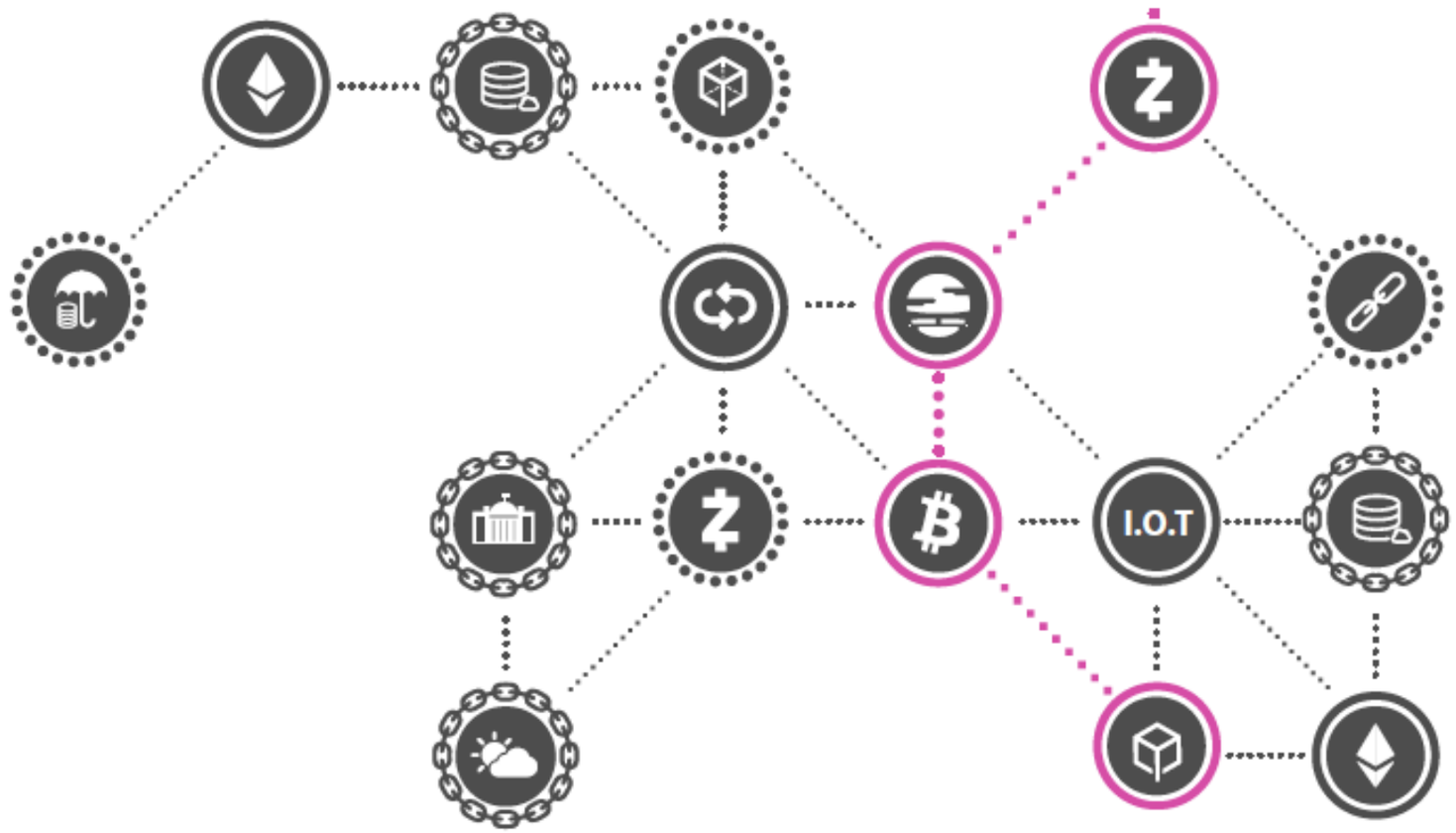
- Interoperabilidad
  - Apps y *smart contracts* de una blockchain capaces de transaccionar con datos de otras cadenas.

- Escalabilidad
  - Ejecución de varias *parachains*, procesando mayor número de transacciones en paralelo.

- Seguridad compartida
  - Aprovechar la seguridad colectiva de todas las cadenas.

Interoperabilidad

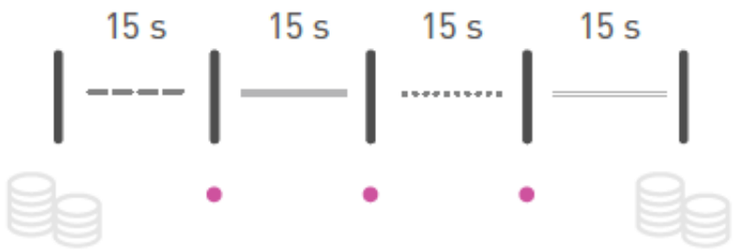
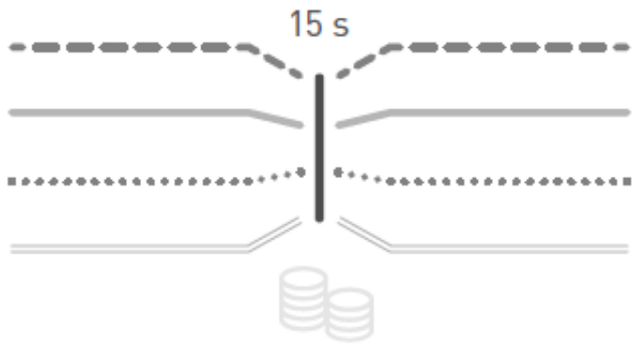
- Existencia de diversas *blockchains* para distintos propósitos.



- Ecosistema verdaderamente *trustless.*

Escalabilidad

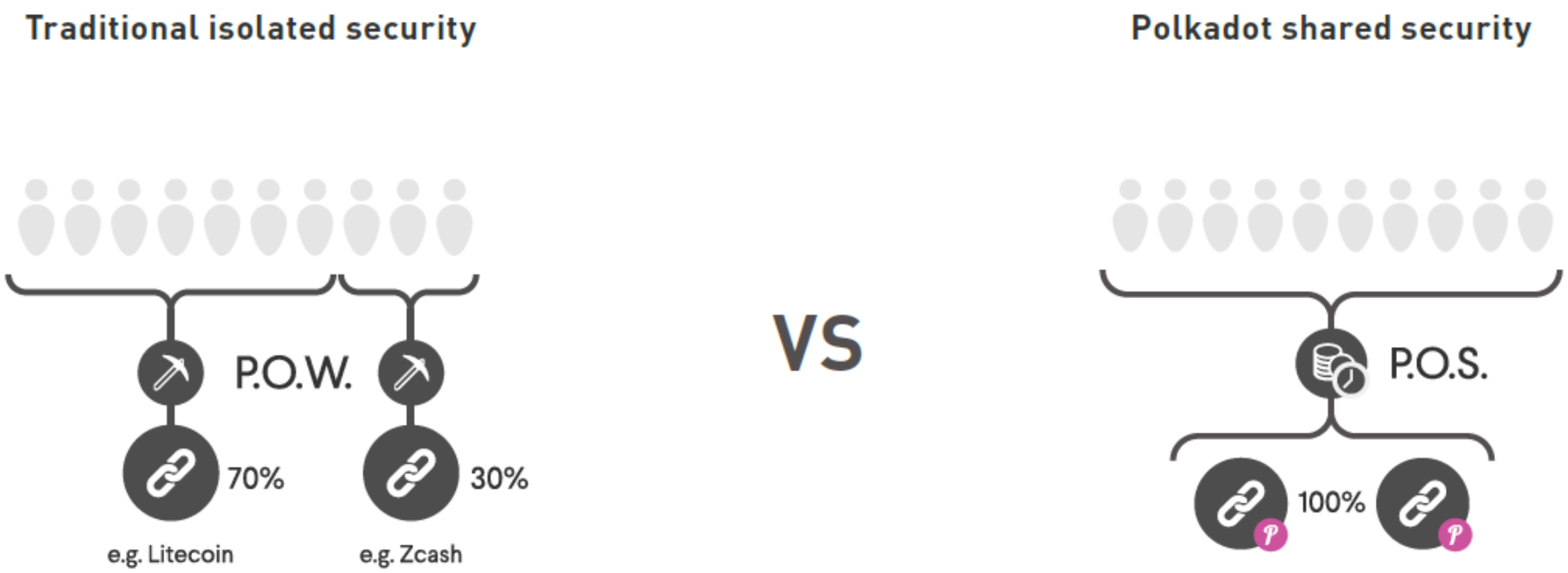
- Actualmente existe un cuello de botella en el procesamiento de transacciones.

Current Method: Single Transactions	Polkadot Method: Multiple Parallelised Transactions
	

- Procesamiento de múltiples transacciones en paralelo gracias a las *parachains*.

Seguridad compartida

- Polkadot agrupa la seguridad dentro de la red.

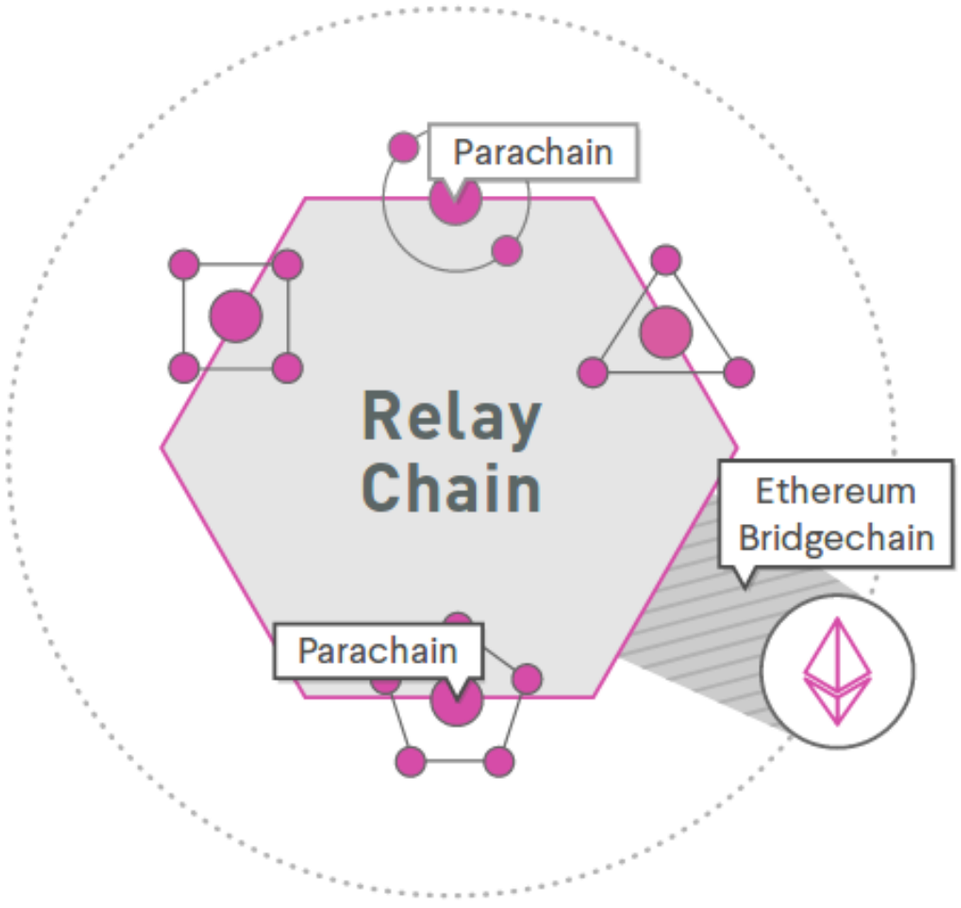


Polkadot

- Tecnología heterogénea multi-cadena.
- Consta de *parachains* con características diferentes.
- Las transacciones se pueden extender a través de las cadenas.
- Polkadot asegura que cada una de estas cadenas siga siendo segura y que cualquier trato entre ellas sea fielmente ejecutado.

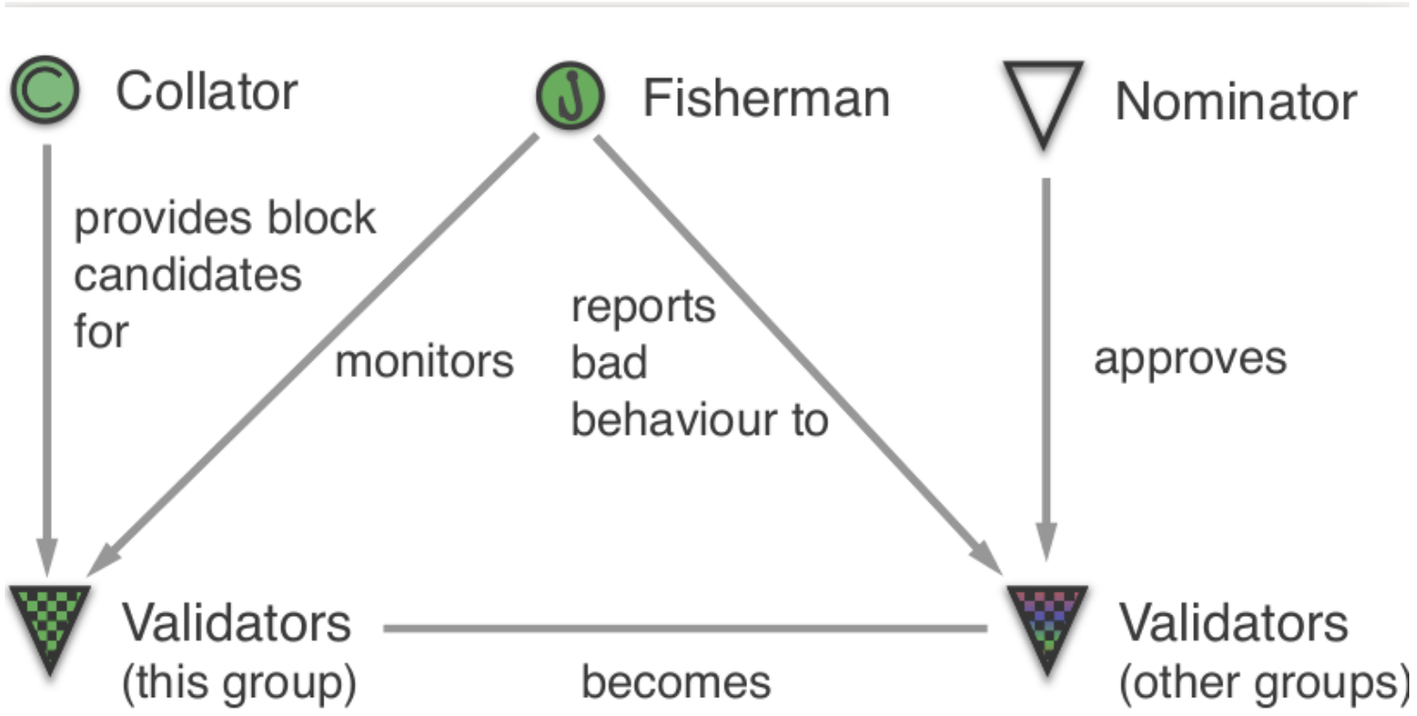
Polkadot

- Relay chain
  - Coordina el consenso y las transacciones entre *blockchains*.
- Parachain
  - Cualquier cadena existente o futura conectada a la Relay chain de Polkadot.
- Bridge
  - Enlace de las *blockchains* con su propio consenso que se conectan a la Relay chain.



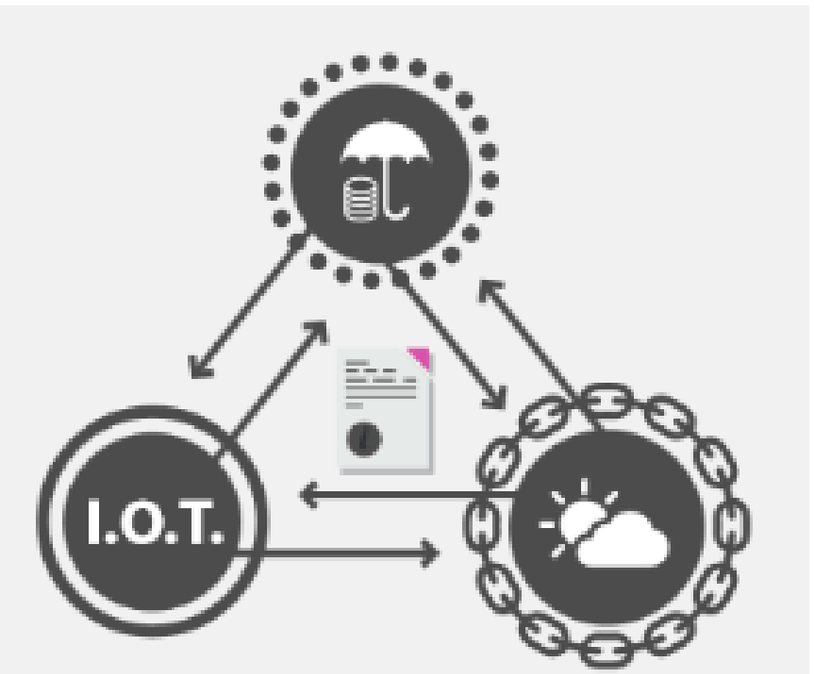
Participación en Polkadot

- Validator
- Nominator
- Collator
- Fishermen



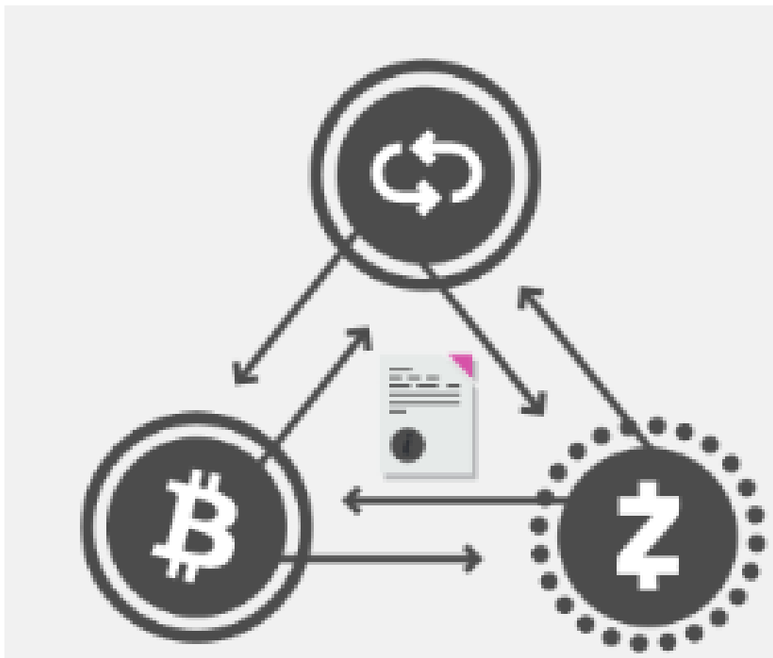
Casos de uso

Catástrofe natural



Crowdsale

Exchange descentralizad

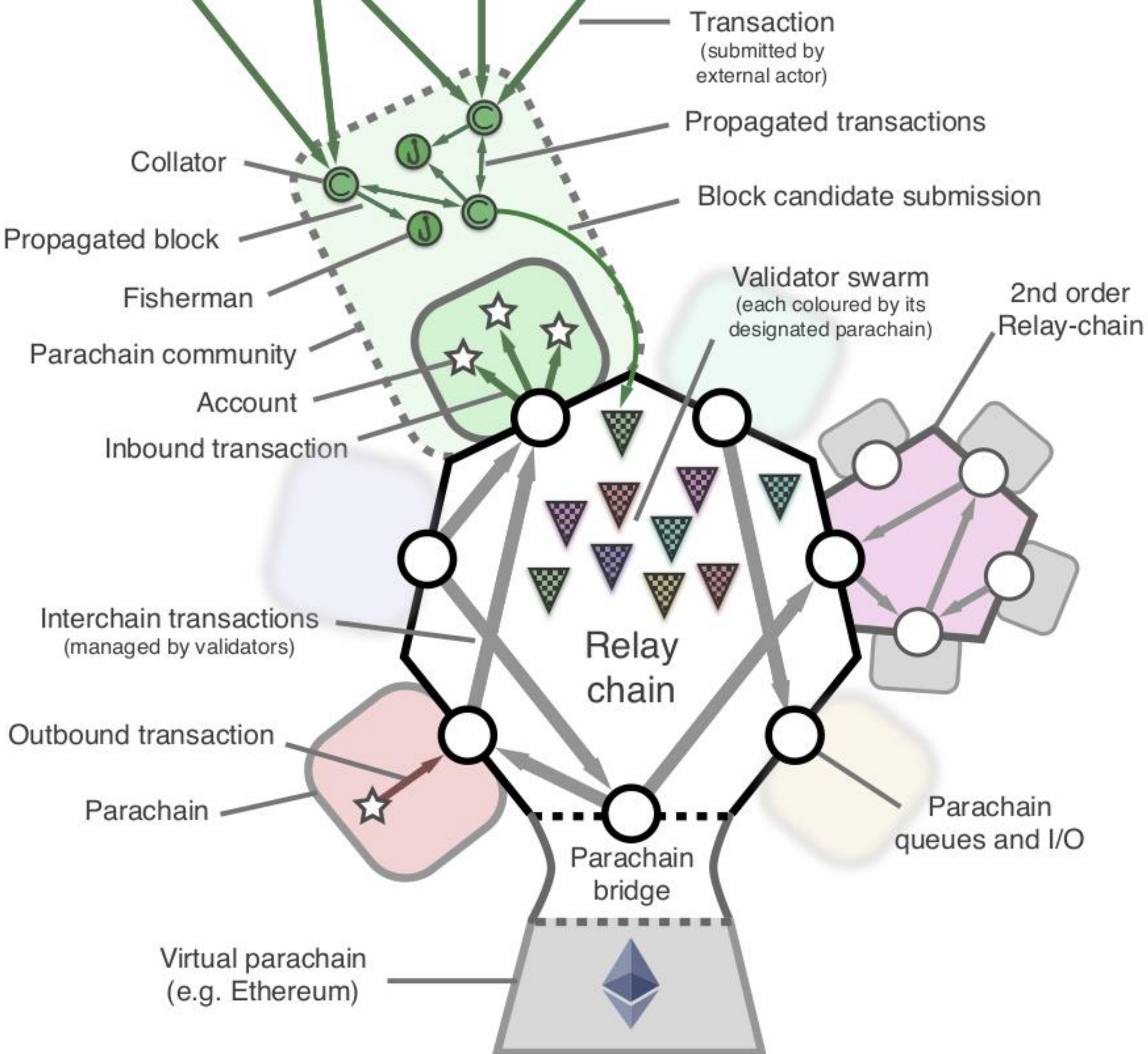


DOT

- Gobierno sobre la red
  - Los poseedores de DOT tienen control total sobre el protocolo.

- Operación
  - La teoría de juegos incentiva a los poseedores de *tokens* a comportarse de forma honesta.

- Vinculación y pago
  - Se agregan nuevas *parachains* mediante *tokens* a modo de fianza. Es una forma de *Proof of Stake* (PoS).


Transaction
(submitted by
external actor)
Propagated transactions
Collator
Block candidate submission
Propagated block
Fisherman
Validator swarm
(each coloured by its
designated parachain)
2nd order
Relay-chain
Parachain community
Account
Inbound transaction
Interchain transactions
(managed by validators)
Relay
chain
Outbound transaction
Parachain
Parachain
queues and I/O
Parachain
bridge
Virtual parachain
(e.g. Ethereum)

Diseño general - Consensus

- Consenso sobre un conjunto de bloques acordados mutuamente.
  - *Tendermint*
  - *HoneyBadgerBFT*

- Polkadot necesita un medio para determinar un conjunto de validadores e incentivarlos a ser honestos → PoS.

Diseño general
Demostrando la participación

- Medios para controlar la participación.
- Validadores seleccionados mediante NPoS.
- Incentivación a partir de expandir la base de *tokens* (pensada actualmente ~10%).
- Las recompensas a los validadores no se ejecutan al instante (planteado un periodo de 3 meses)

Diseño general
Comunicación entre cadenas

- Comunicación tan simple como puede ser.
- Al igual que en las *blockchains* actuales, las transacciones externas son asíncronas.
- La Relay chain mueve las transacciones en la cola de salida de una *parachain* a la cola de entrada de la cadena de destino.

Tipo-Ethereum & Polkadot

- Objetivo crítico del proyecto.
- Estándar de interoperabilidad.
- *Smart contracts*
  - *Break-in*
  - *Break-out*
- Bajo coste económico a partir de aplicar estrategias de almacenamiento en buffer y empaquetamiento de transacciones.

Tipo-Bitcoin & Polkadot

- Es necesario un número de validadores mayor al actual que proporciona Bitcoin.
- Protocolo más limitado y difícil de coordinar una actualización a través de *hard forks*.
- Es posible que tenga lugar después de la interoperabilidad directa de Ethereum.

Tipo-IOTA - Polkadot

- Proyecto que no depende de bloques ni de cadenas.
- No hay estados ni transacciones.
- La solución pasa por mantener un árbol de Merkle separado de todas las transacciones a partir de una cierta profundidad del DAG.
- Tratar ese raíz de Merkle como un estado global.

Tipo-Cosmos & Polkadot

- Intercambio de *tokens* (Cosmos) vs llamadas a métodos de *smart contracts* remotos (Polkadot).
- El bloque que especifica la transición puede ser verificado en relación a un hash padre (usando un cliente ligero).
- Protocolo interconexión de cadenas *tendermint*.

Tech

- Specs:
  - https://github.com/w3f/polkadot-spec/blob/master/spec.md
- Paper:
  - https://github.com/polkadot-io/polkadot-white-paper/raw/master/PolkaDotPaper.pdf