Desarrollo Blockchain Ethereum con Solidity

Módulo 7 - Sidechains

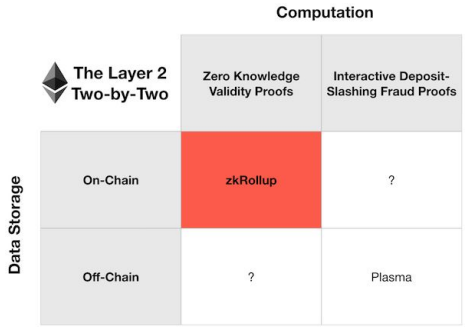
Sidechains

Rollups

- Son soluciones que realizan la ejecución de transacciones fuera de la cadena principal de Ethereum (capa 1) pero postea los datos de la transacción en la capa 1.
- Como los datos de las transacciones están en la capa 1, esto permite que los Rollups estén protegidos por la misma.
- Hereda las propiedades de seguridad de la capa 1 aunque la ejecución se realiza por fuera.
- En cierta forma “enrollan” varias transacciones en una, por eso el nombre.

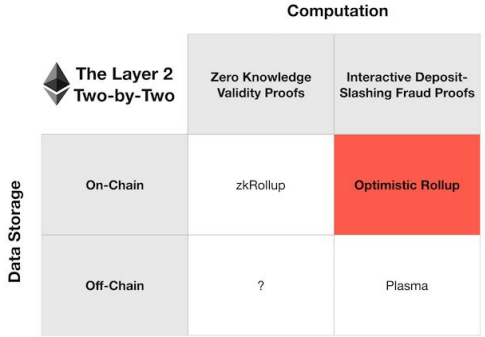
Zero Knowledge Rollups

- Conocidos también como **ZK-rollups.**
- Reúnen cientos de transacciones y se genera una prueba criptográfica conocida como SNARK.
- El SNARK generado se toma como prueba suficiente de validación y se postea en un contrato de la cadena principal (capa 1).
- El contrato de la cadena principal podrá decodificar la información de la transacción generada para verificar los cientos de operaciones que representa.
- El proceso de verificación es muy rápido.
- Es seguro y descentralizado pues el estado de las transacciones está en la cadena principal.
- Recién en 2021 se empezó a implementar soporte para contratos inteligentes.
- No vale la pena para aplicaciones con poca actividad ya que la verificación requiere de poder de cómputo.
- **Ejemplos:** Loopring, Starkware, zkTube.



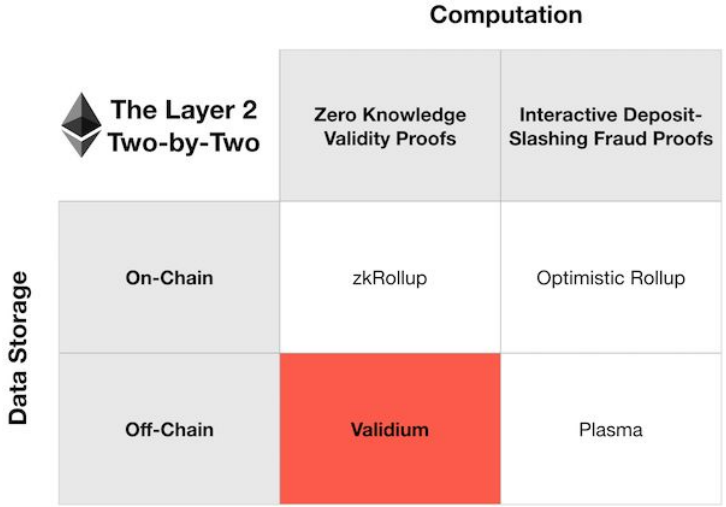
Optimistic Rollups

- No realiza cálculos computacionales por defecto si no que espera a que haya alguna sospecha de fraude, por ende funciona más rápido que la cadena principal.
- El contrato de la cadena principal no hace el chequeo como lo hace el ZK siempre si no que sólo cuando ocurre algo incorrecto, por eso es “optimista”.
- Depende de operadores o usuarios que marquen esa transacción como inválida.
- Soporta una funcionalidad similar al de la capa 1, por lo tanto soporta también contratos inteligentes.
- Obtiene todas las ventajas de descentralización y seguridad de la capa 1.
- Muchas veces se producen demoras en la registración de las transacciones en la capa 1 debido a la posibilidad de verificar fraudes.
- **Ejemplos:** Optimism, Fuel Network, Cartesi



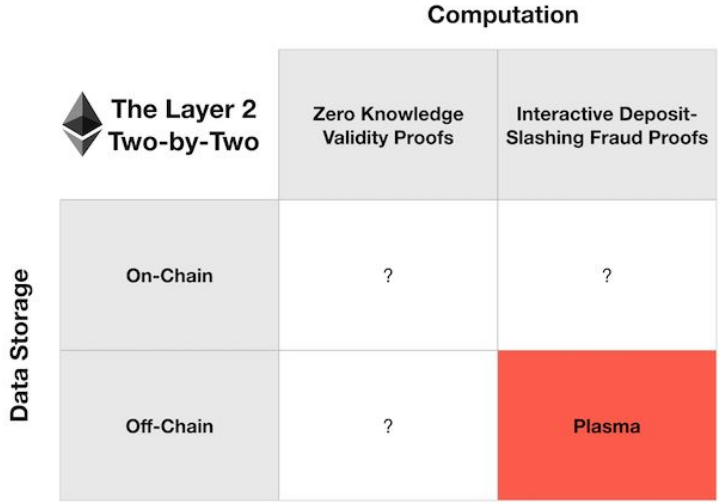
Validium

- Utiliza pruebas de validación como por ejemplo los ZK-rollups pero la información de las transacciones no se almacena en la cadena principal.
- Puede soportar hasta 10.000 TPS por cadena de validium.
- No tiene latencia en traspaso de cadenas, por lo tanto su eficiencia es muy buena.
- No tiene soporte total para contratos inteligentes.
- Se requiere de poder de cómputo para las validaciones de ZK.
- **Ejemplos:** Starkware, Loopring.



Plasma

- Es una blockchain separada que está anclada a la cadena principal y usa verificaciones de fraude al estilo rollups optimistas.
- Tienen alto volumen de transacciones y bajo costo.
- No soporta contratos complejos, sólo algunos escenarios de transacción de Tokens.
- Se debe chequear cada tanto el estado de la red principal para ver que los fondos no estén comprometidos.
- Depende de operadores que administren la información.
- Los retiros a la red principal pueden demorar días.

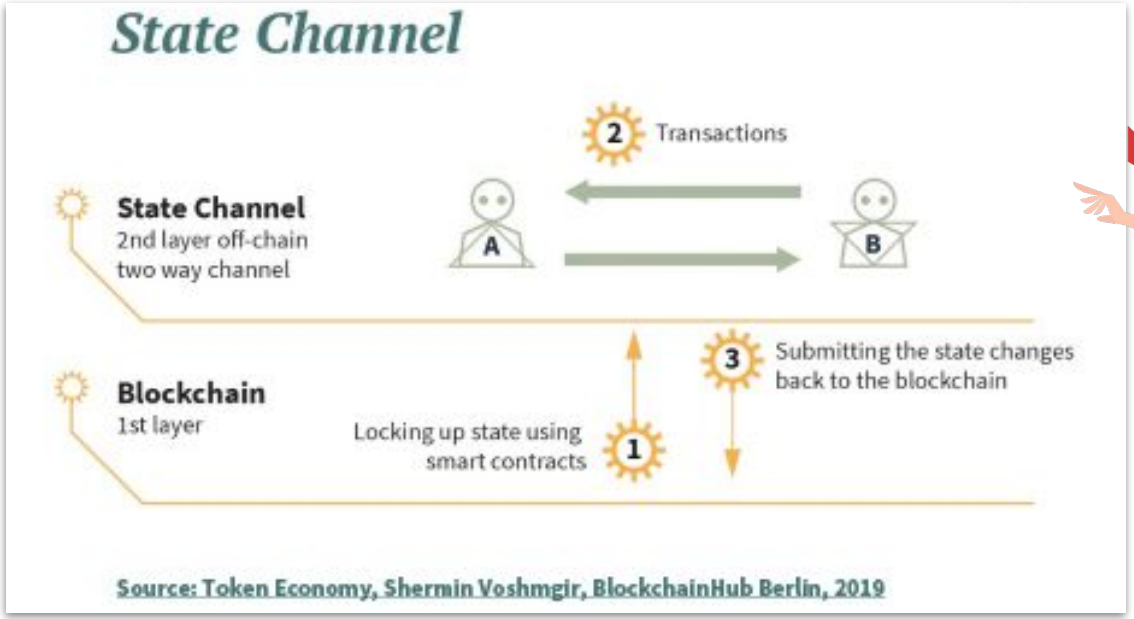


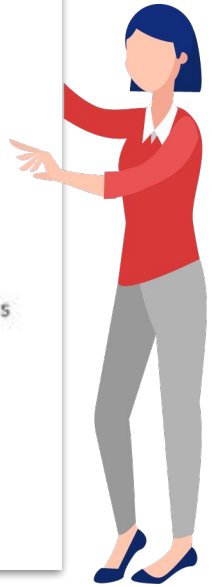
Canales

- Permite a los participantes a emitir una cierta cantidad de transacciones fuera de la cadena registrando en la cadena principal sólo dos transacciones.
- Las transacciones se realizan a gran velocidad y sin costo por transacción.
- Como primera instancia se bloquea un saldo en la red principal en un contrato/billetera multifirma.

- Es útil para:
  - Alto volumen de transacciones/cambios de estado.
  - Cuando se conoce la cantidad de participantes de antemano.
  - Participantes que están siempre disponibles.
- Existen dos tipos de canales:
  - Canales de pago.
  - Canales de estado.
- No es recomendado para transacciones ocasionales entre usuarios.
- **Ejemplos:** Connext, Perun, Raiden

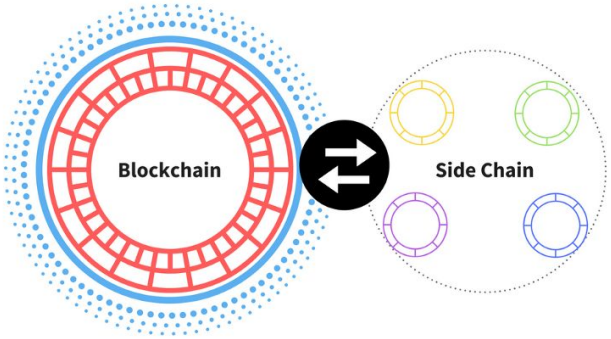
Canales


State Channel
2
Transactions
State Channel
2nd layer off-chain
two way channel
A
B
Blockchain
1st layer
Locking up state using
smart contracts
1
3
Submitting the state changes
back to the blockchain
Source: Token Economy, Shermin Voshmgir, BlockchainHub Berlin, 2019



Sidechains

- Blockchain separadas que funcionan en paralelo a la red principal de Ethereum.
- Tienen su propio protocolo se consenso (PoA, PoS, etc).
- Están conectadas a la red principal por un puente bilateral.
- Se basan en la EVM por lo tanto pueden ejecutar contratos inteligentes.
- En cierta forma son un “clon” de Ethereum ya que podemos hacer exactamente lo mismo: crear contratos, implementarlos, conectarlos con una dApp e interactuar por medio de Web3.



- En general son más centralizadas y además no aprovechan las ventajas del consenso de la red principal.
- Podría ocurrir un fraude si hay quorum en el consenso de la sidechain.
- **Ejemplos:** Skale, xDai, Polygon.

¡Muchas gracias!

¡Sigamos trabajando!