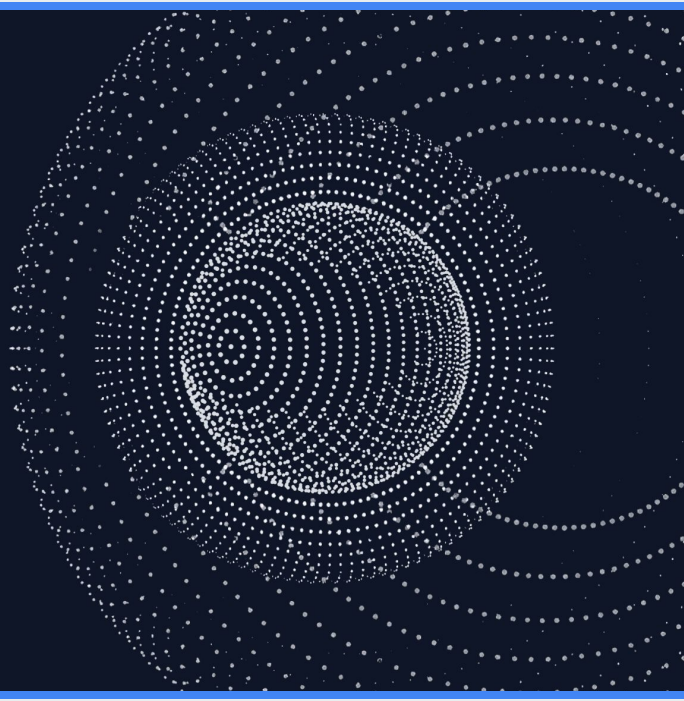
Fairgate

FLEX

Capital-Efficient Fraud-Proofs for Bitcoin Bridges



Sergio Demian Lerner | CTO, Fairgate Labs

Buenos Aires, SEP 2025

Estructura De Esta Presentación

1. Introducción
2. Descripción general del protocolo
3. Detalles
4. Variantes
5. Conclusiones

INTRODUCCIÓN

Fairgate

Protocolos de Computación Disputable y Depósitos de Seguridad

1. Hablaremos sobre el uso de bonos de seguridad en la familia de protocolos BitVM.
2. Puente como ejemplo de aplicación
3. Principalmente en el modelo de comité cerrado (permissioned model)
4. Suponiendo que solucionemos los problemas técnicos para implementar Garbled Circuits/MPC de manera eficiente y segura en Bitcoin.

El papel de los bonos de seguridad en los protocolos de Bitcoin

1. Compensación de las ganancias esperadas para un tramposo en un juego probabilístico repetible.
2. Reembolsar los costos de la disputa a las partes honestas (el tramposo paga)
3. Para desalentar los ataques de griefing (causar daño sin necesariamente un beneficio económico)

Los costos financieros de los depósitos de seguridad

1. Vinculado al coste de oportunidad
2. Crece exponencialmente con respecto al tiempo de bloqueo (interés compuesto)
3. Aumentará con el crecimiento del ecosistema DeFi de Bitcoin.

¿Por qué utilizamos depósitos estáticos?

1. Necesitamos algún tipo de depósito de seguridad.
2. Es más sencillo utilizar depósitos estáticos.
3. Los covenants emulados requieren que la fuente de fondos sea un UTXO conocido, y usa su identificador de transacción en la pre-firma

¿Qué tienen de malo los depósitos estáticos?

1. **Duración**: Los depósitos se mantienen durante el ciclo de vida del activo resguardado.
2. **Escalabilidad**: Los requisitos de los depósitos aumentan con el **cuadrado** del número de operadores
3. Mal balance: Si reducimos los depósitos, afectamos la seguridad, si los aumentamos, la **descentralización.**

Fraud-proof Trilemma

No se pueden tener las tres cosas a la vez en un sistema de disputas optimista:

- **Bajo costo** para los verificadores honestos (que chequear sea barato).
- **Seguridad** contra ataques de gasto de recursos (DoS)
- **Finalidad** rápida de las disputas.

RESUMEN DEL PROTOCOLO

Fairgate

¿Qué es FLEX?

- Una familia de protocolos informáticos disputables y eficientes en capital con depósitos de seguridad a demanda.
- Esto significa:
  - La financiación de bonos de UTXO no se conoce durante la configuración.
  - Los depósitos de seguridad se utilizan durante el período de disputa entre los operadores y “torres de vigilancia” (watchtowers)

Roles

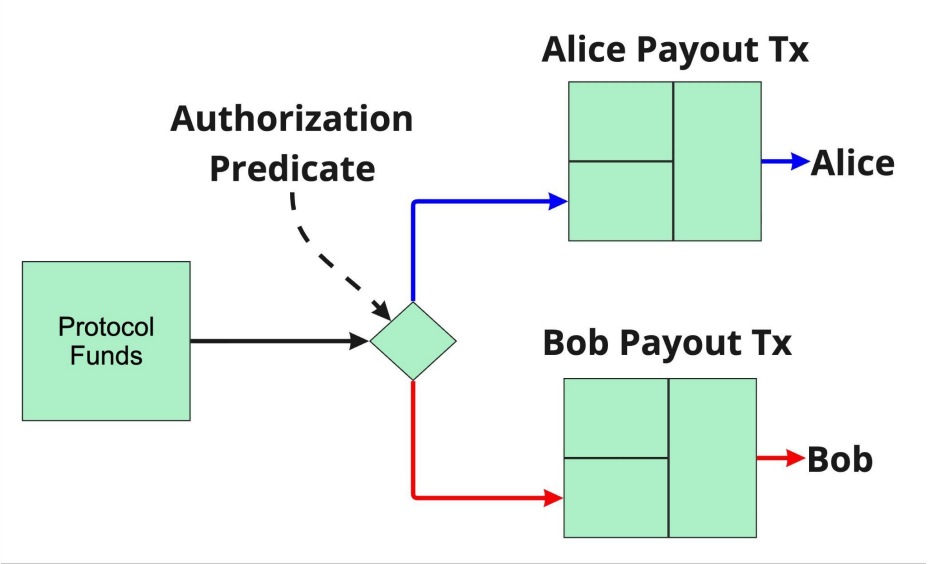
1. Flex es un protocolo de dos partes.
2. Alice: Prover
3. Bob: Verificador
4. En principio, sin otros protocolos, un sistema de n partes se convierte en n(n-1) instancias de FLEX.

DETALLES

Fairgate

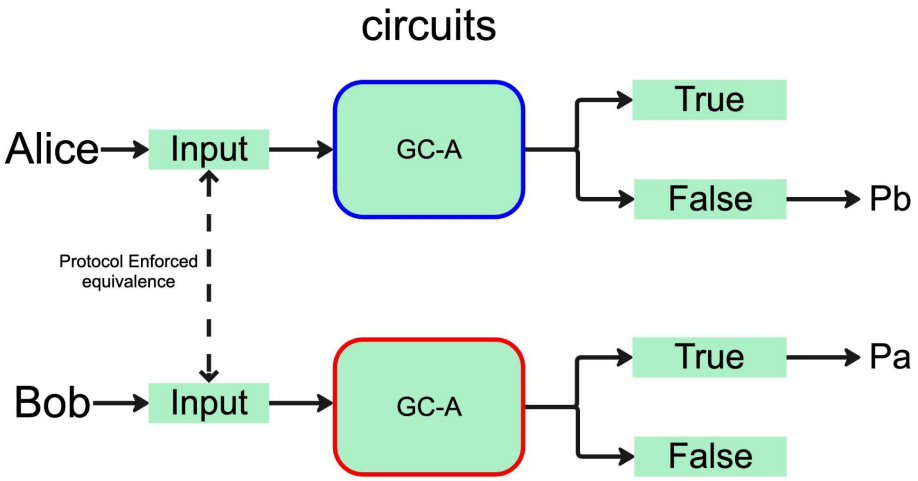
Conceptos Básicos

1. Hay un fondo de dinero que cuidan Alice y Bob
2. Alice o Bob pueden pedir retirar los fondos, si un predicado de autorización es verdadero
3. **Si hay disputa, ambos ponen un depósito de seguridad antes de disputar el predicado**



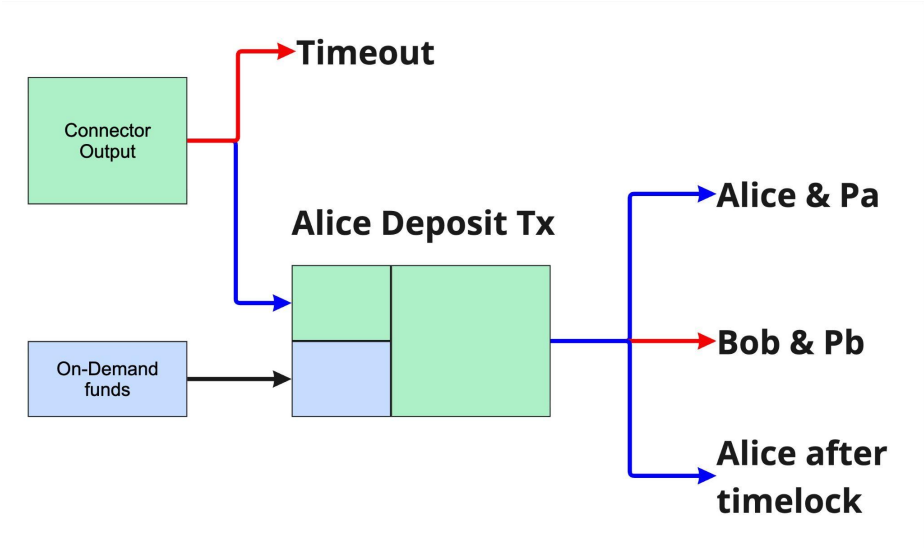
Modelo de circuito dual

- Se crean dos circuitos idénticos:
  - Alice construye **GC-A**
  - Bob construye **GC-B**
- **Entradas:**
  - Alice proporciona entradas a GC-A.
  - Bob proporciona entradas a GC-B.
- **Secretos revelados condicionalmente:**
  - GC-A revela **Pb** a Bob *si el predicado rechaza la entrada*
  - GC-B revela **Pa** a Alicia *si el predicado acepta la entrada*
- **Bob esta obligado a replicar la entrada de Alice**



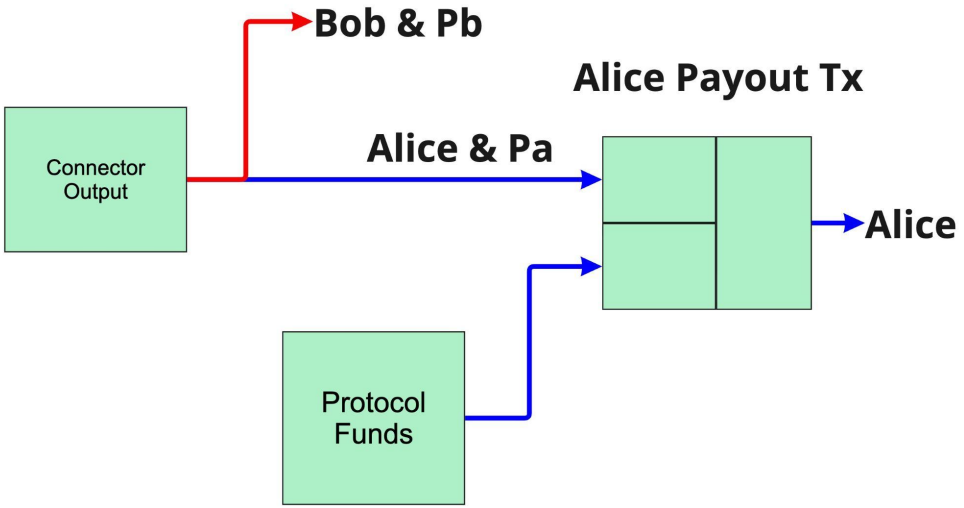
Manejo de depósitos de seguridad

1. Diseño simétrico para Alice y Bob
2. Financiado con UTXO externos mediante SIGHASH_ANYONECANPAY
3. **Los TXID no se conocen de antemano.**
4. El flujo del protocolo impone la publicación de la entrada del circuito correspondiente
5. 3 vías de gasto



Manejo de depósitos del Contrato

1. Alice pide el retiro
2. Alice puede retirar los fondos si gana la disputa (con Pa)
3. Bob puede impedir que Alice retire los fondos (con Pb)
4. Bob no puede retirar los fondos



Configuración

1. Alice y Bob intercambian
    2. Claves públicas de Lamport para entradas de circuitos
    3. Materiales de circuitos (garbled circuits)
    4. Pruebas de conocimiento cero sobre la corrección de los circuitos
5. Firman las transacciones que conforman un DAG para obtener covenants emulados
6. Firmar transacción de depósito de fondos que protege el contrato en cuestión

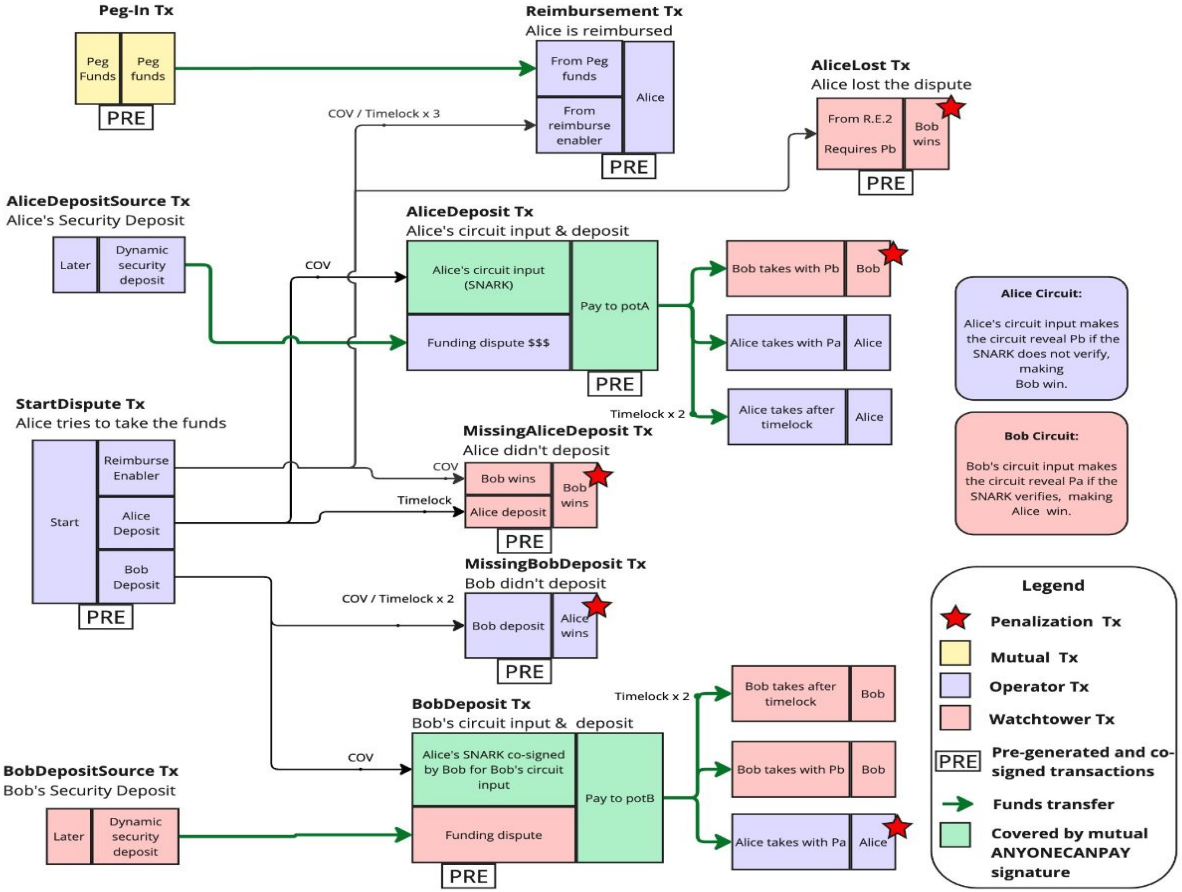
Uso en Bridges - Peg-out usando reembolsos

1. Un usuario en una cadena lateral inicia el peg-out
2. Alice transfiere por adelantado los bitcoins al usuario (en la red Bitcoin)
3. Alice anuncia el adelanto de fondos
4. Si no hay oposición, el protocolo devuelve los fondos a Alice
5. Si hay oposición, Alice pone el depósito de seguridad y publica las etiquetas de entrada del circuito GC-A.
6. Bob pone depósito de seguridad y publica las etiquetas de entrada del circuito GC-B correspondientes

Resultados

- Camino super-feliz
  - Ambas partes están de acuerdo y Alice retira los fondos
- Camino feliz
  - Ambas partes participan y evalúan los circuitos → se revela un secreto.
  - Si Pa → Alice cobra su depósito + el de Bob y recibe el reembolso.
  - Si Pb → Bob cobra su depósito + el depósito de Alice y bloquea el reembolso.
- Liveness / Timeouts
  - Si Bob no participa → Alice recupera su depósito y completa el peg-out.
  - Si Alice no participa → Bob recupera su depósitos y detiene el peg-out.
  - Ambos pueden reclamar otras penalizaciones en la cadena lateral

Grafo de Transacciones



VARIANTES de FLEX

Fairgate

Lidiando con la asimetría

1. El sistema es mayoritariamente simétrico.
2. Pero Alice se adelanta → debe publicar las entradas antes de que Bob deposite.
3. Las funciones de depósito y entrada se fusionan para simplificar:
    - Tanto Alice como Bob utilizan una sola transacción cada uno para proporcionar el depósito de seguridad y las entradas del circuito.

Problema de publicación no reembolsable de la entrada del circuito

- Suponiendo que se pueda comprobar la validez del peg-out **sin las entradas completas.**
- Que pasa si Alice publica las entradas (con su depósito) pero Bob Bob no esté disponible.
    - **Alice aún paga el costo de entrada (aproximadamente 16 000 vbytes para Groth16).**
- Soluciones
    - Reembolso de un depósito de seguridad estático
    - Predepósito de Bob
    - Separación de Depósitos y Publicación de Entradas

CONCLUSIONES

Fairgate

Familia de protocolos FLEX

- Presentamos FLEX, un de resolución de disputas entre 2 partes con bonos de seguridad a demanda basado en GC para Bitcoin.
- Aplicaciones: puentes y otros sistemas optimistas que usan pruebas de fraude.
- Beneficios clave:
  - Resuelve las ineficiencias de capital asociadas con los diseños de bonos estáticos.
  - Reduce los gastos financieros generales.
  - Mejora la escalabilidad y la descentralización.

Gracias!

https://github.com/FairgateLabs

BitVMX

https://bitvmx.org