BitVM1

– Construindo Ethereum no Bitcoin

vinteum

Qual a importância?

- Escalabilidade
- Computador baseado no Bitcoin
- Capacidades semelhantes ao smart contracts do Ethereum
- Turing Completeness
- 1-of-N setting
- Optimistic RollUp

vinteum

Ideia Central

Objetivo: escalar o uso de Bitcoin... mas se quiser dá pra jogar xadrez

- Representação de qualquer programa em circuitos binários
- Cada porta binária é codificada em uma folha
- Bit Commitments
- Revogar de maneira simples

Críticas

- Complexidade
- Grandes transações on-chain
- SuperTestnet thinks not having Turing Completeness on Bitcoin is good to protect the program. By implementing BitVM you keep the base layer unchanged and just puts the program on the tap tree, so you don't need to verify the program, just to verify the false part of the program.

Conclusão V1.0

- A ideia central é criar um sistema de confiança usando a camada base do Bitcoin, onde há um verificador e um “atestador” mas com computação otimista.
- Reduz a pegada on-chain mas aumenta off-chain
- Possibilita fazer esquemas laterais

BitVM2

- Uma ponte mais leve...

Qual o problema com BitVM1?

- Necessário membros específicos para contestar uma transação
- Protocolo de auditoria razoavelmente longo

Melhorias

- Auditoria em dois ciclos
- Qualquer um pode contestar
- Uso de SNARK (ZKP mais rápido e não iterativo) ao invés de portas lógicas

BitVM

- Resumo (agora vai)

Paradigma

- Optimistic Computation
- SNARK verifier
- Disprove faulty assertion

A ponte

- Vai fazer a ponte para qualquer outro sistema
- Raramente utilizada
- Usuário final nem saberia que está usando
- Quantidade fixa de operadores, mas qualquer um pode auditar

vinteum

Garantias

- É uma federação, mas somente um membro é necessário para garantir a segurança
- Qualquer um pode ser membro (você pode auditar)
- Se todos operadores desonestos mas um membro honesto, o desonesto ainda não consegue retirar dinheiro desonestamente

SNARK

- Um verificador SNARK pode ter gbs
- Fazer 1000 commits de 4MB = 1 programa de 4GB

Conclusão

- Complexo complexo complexo
- Uso possível: ponte com maior desconfiança em terceiros
- Não necessita de modificar a camada base

Referências

1. What is BitVM? with Robin Linus and Super Testnet (SLP520)
2. MIT Bitcoin Expo 2024: Scaling Up - BitVM (Robin Linus)
3. BitVM - by José
4. How Viable Are BitVM Based Pegs? - Bitcoin Magazine
5. BitVM 2: Opening Up The Playing Field - Bitcoin Magazine
6. The Big Deal with BitVM: Arbitrary Computation Now Possible on Bitcoin Without a Fork
7. Some Intuitions on Zero-Knowledge Proofs