Zero-Knowledge for Privacy, Succinct for Rollups

Adrià Torralba-Agell[1, 3]
atorralbaag@uoc.edu

Ghazaleh Keshavarz[2, 3]
ghazaleh.keshavarzkalhori@uab.cat

Cristina Pérez-Solà[2, 3]
cperezsola@uoc.edu

David Megías[1, 3]
dmegias@uoc.edu

[1]Universitat Oberta de Catalunya
K-riptography and Information Security for Open Networks (KISON) Research Group

[2]Universitat Autònoma de Barcelona
SENDA - Security of Networks and Distributed Applications

[3]Cybercat - Center for Cybersecurity Research of Catalonia

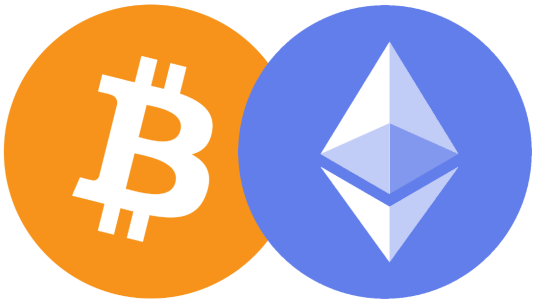
April 24th, 2024

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Digitalización e Inteligencia Artificial
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

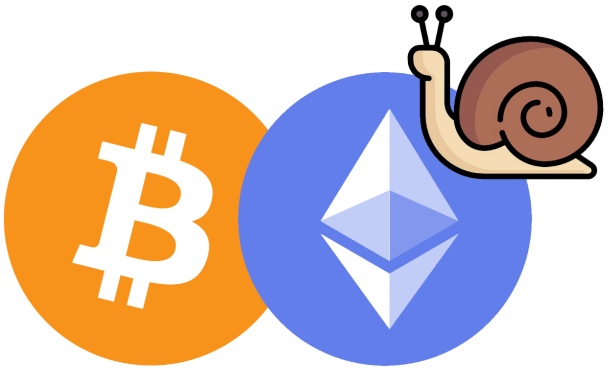
Table of Contents

Table of Contents

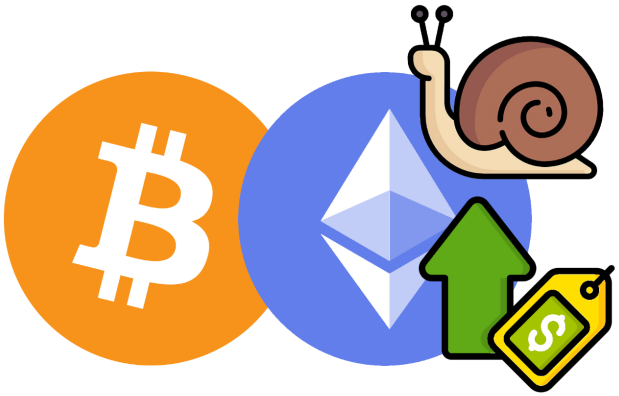
Bitcoin and Ethereum do not scale



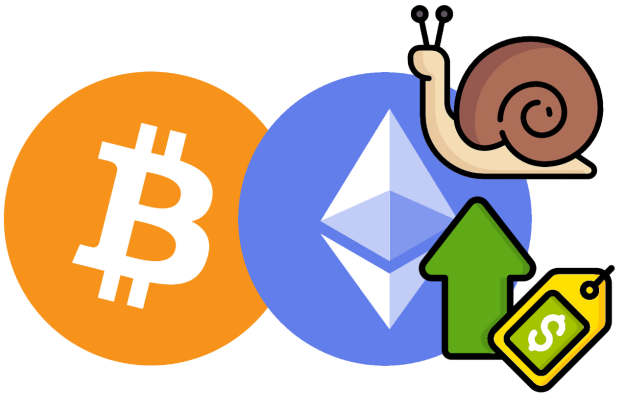
Slow

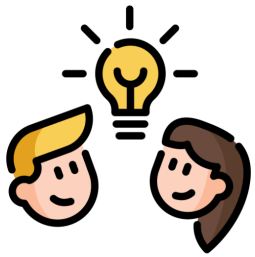


Expensive

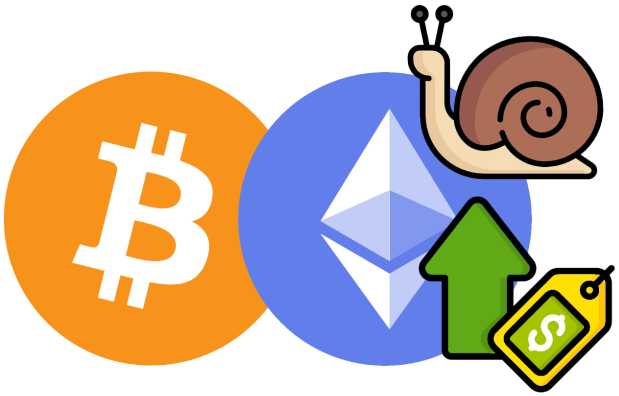


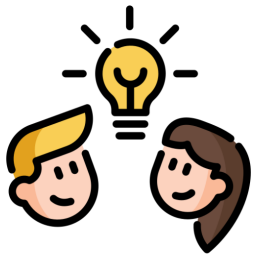
But people have ideas... Layer 2!

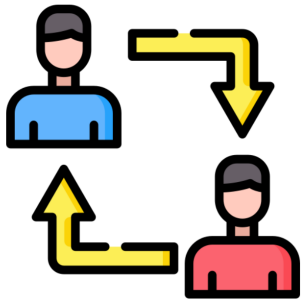




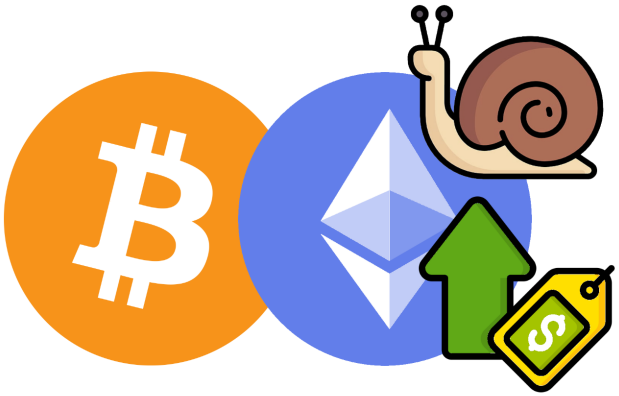
Payment Channel Networks

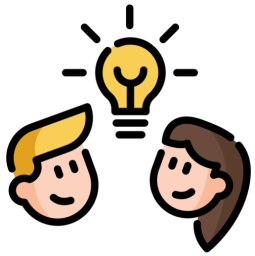


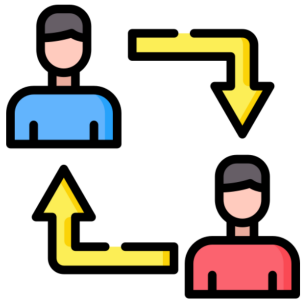


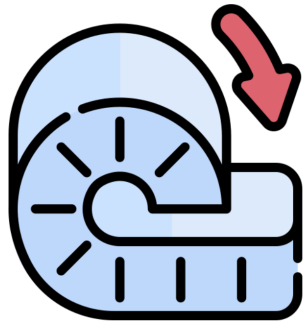


Rollups

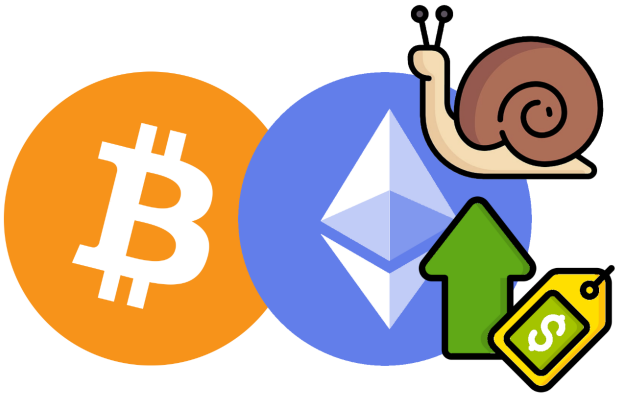


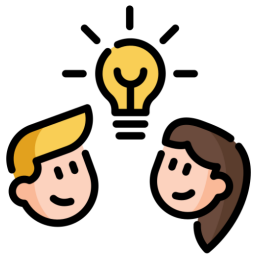


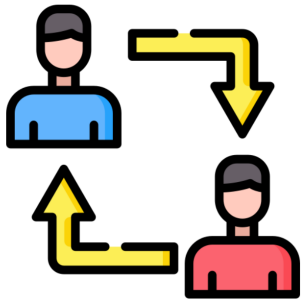


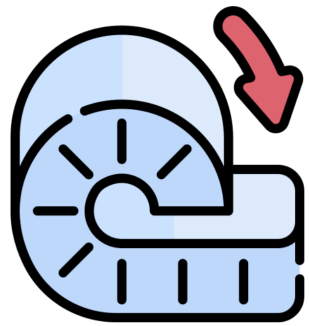


Bridges to enable interoperability

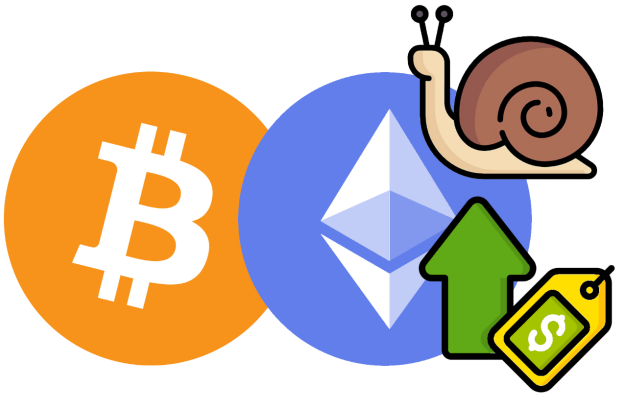


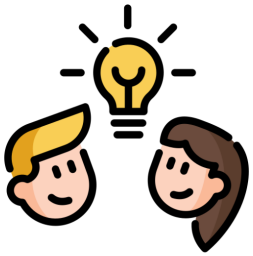


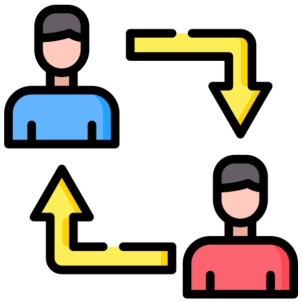




We are interested on rollups







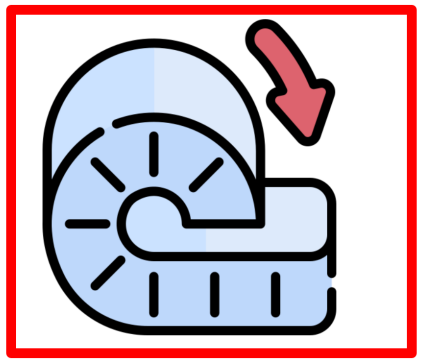
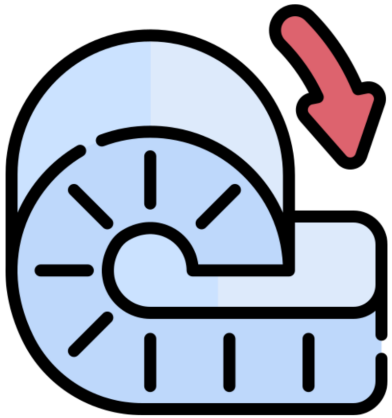
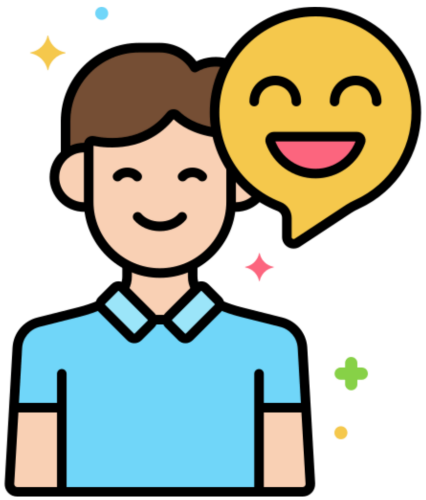


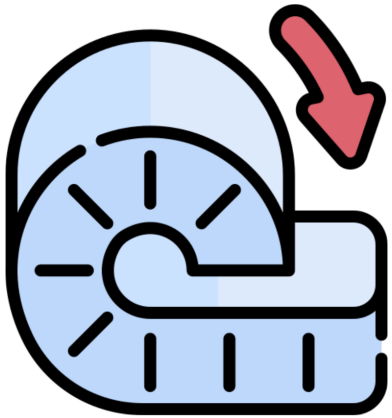
Table of Contents

Rollups

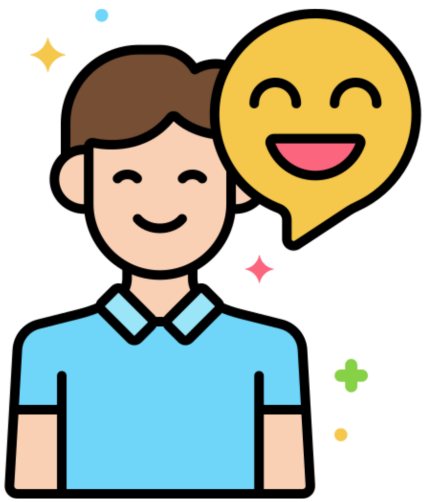


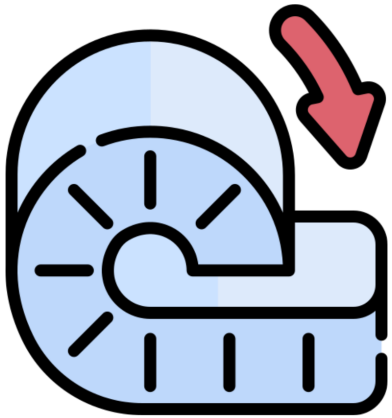
Optimistic Rollups

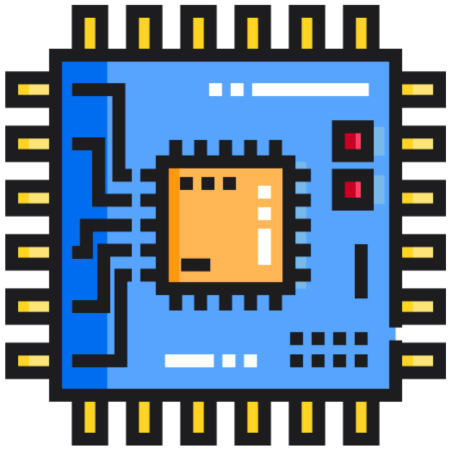




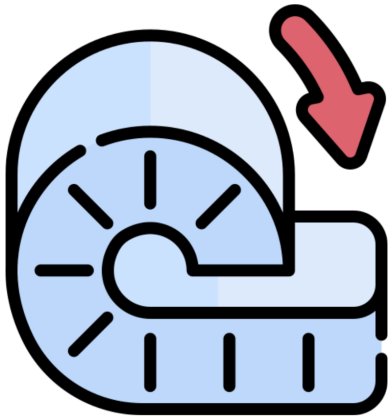
Zero-Knowledge Rollups

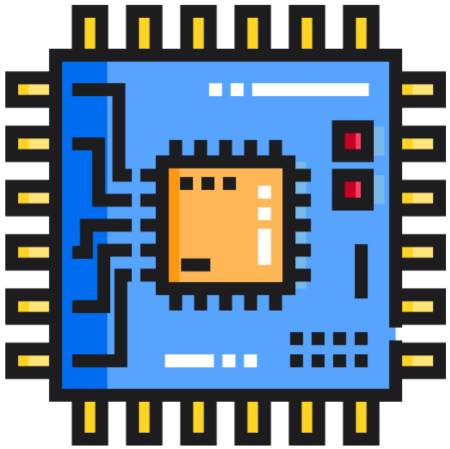




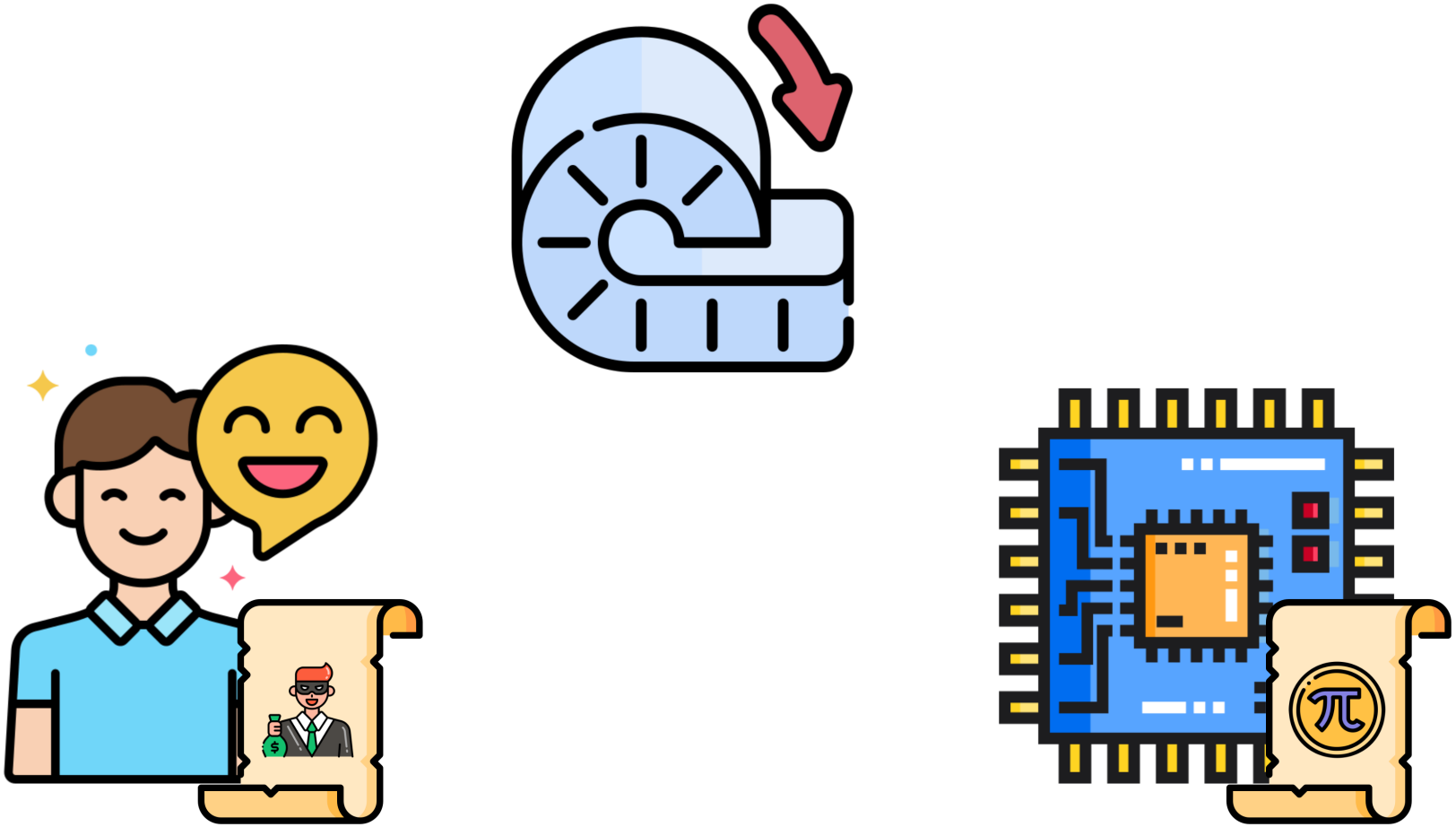


Optimistic Rollups - Fraud Proofs

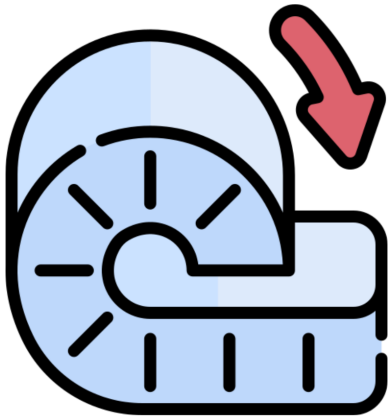




Zero-Knowledge Rollups - Validity Proofs



Zero-Knowledge Rollups



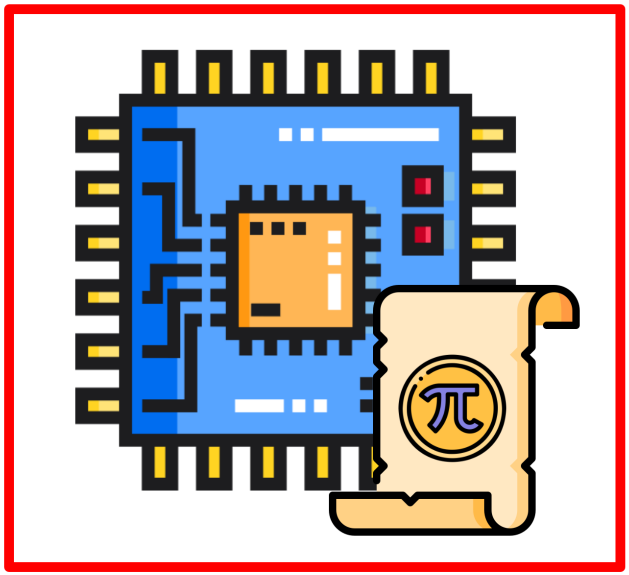
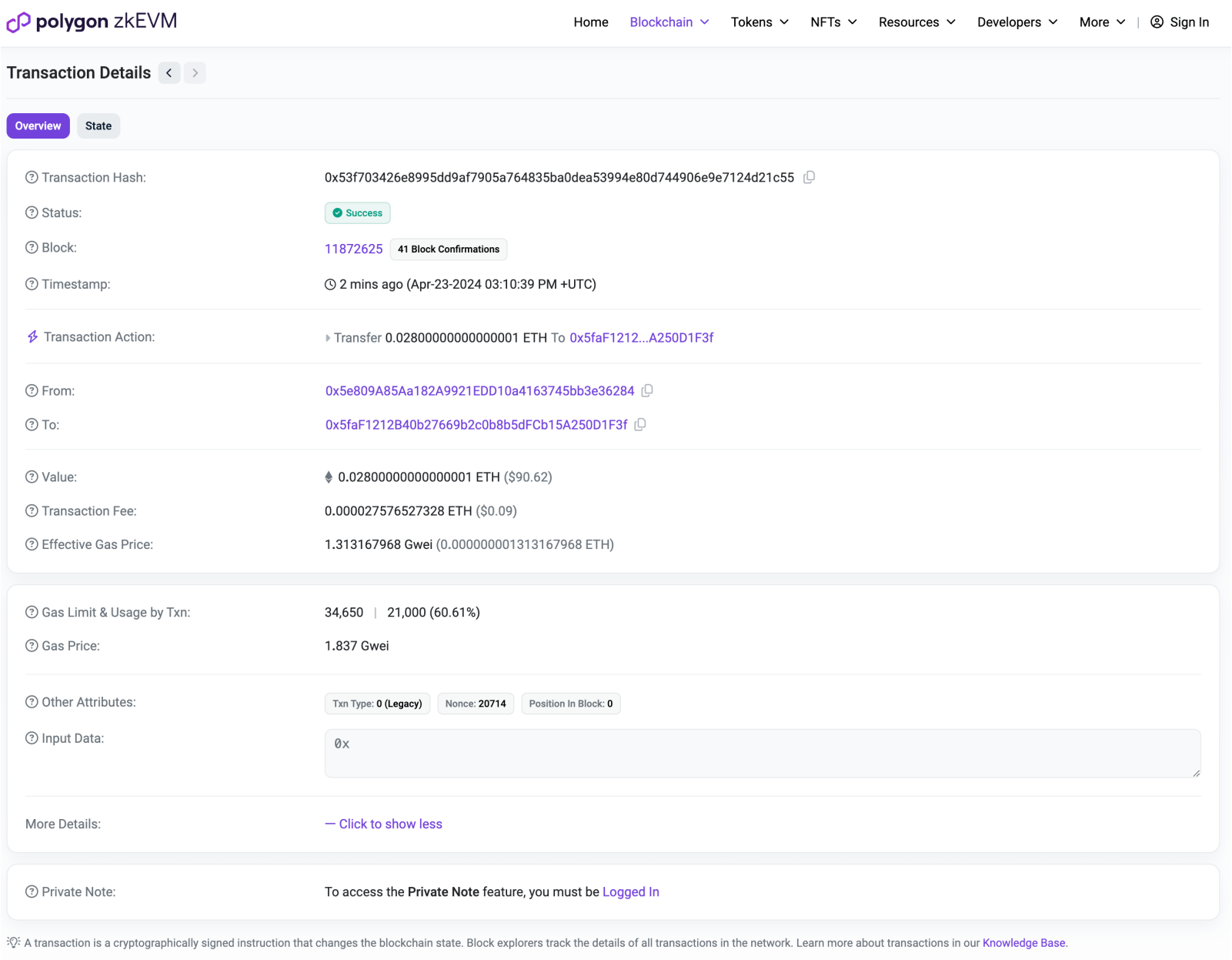
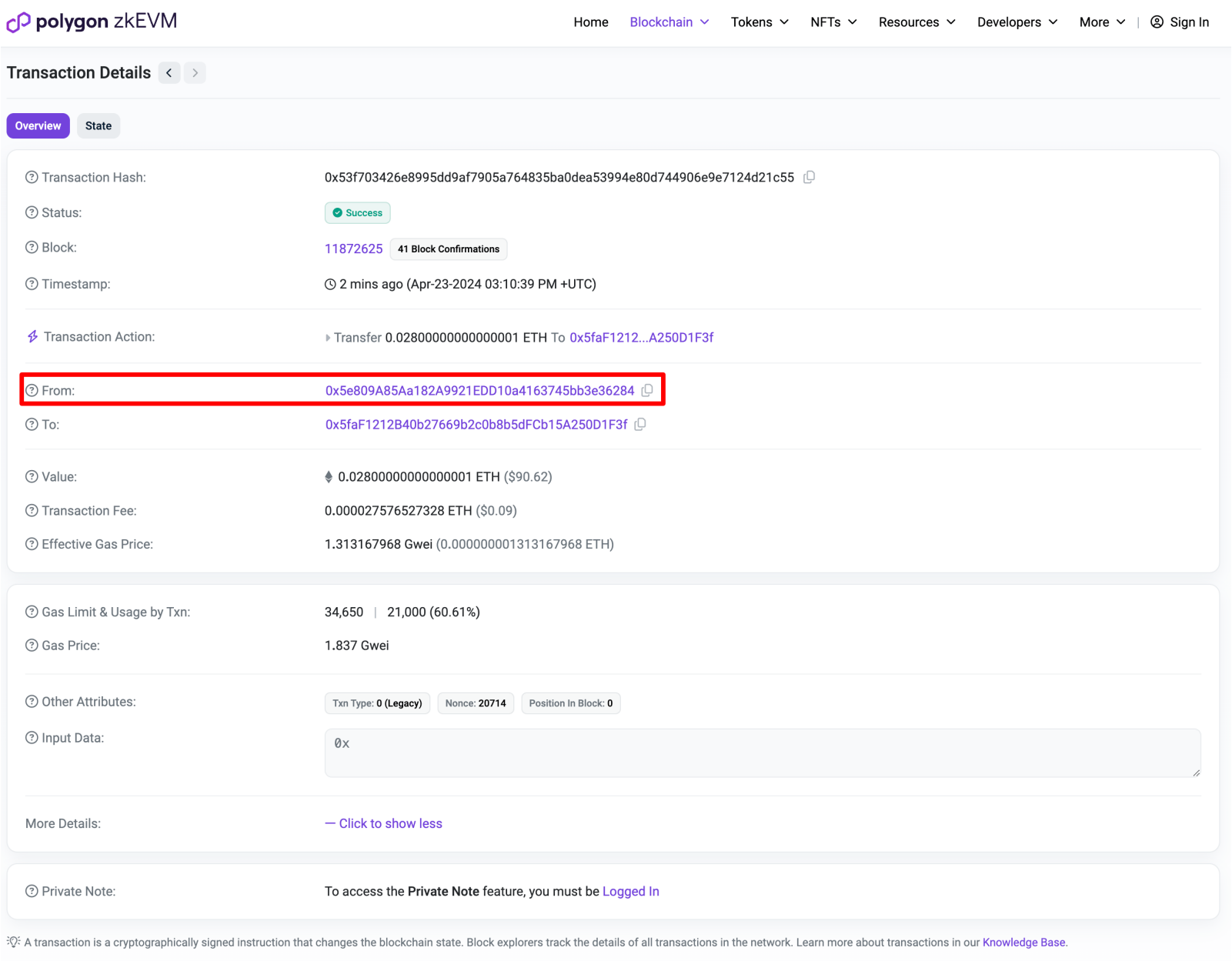


Table of Contents

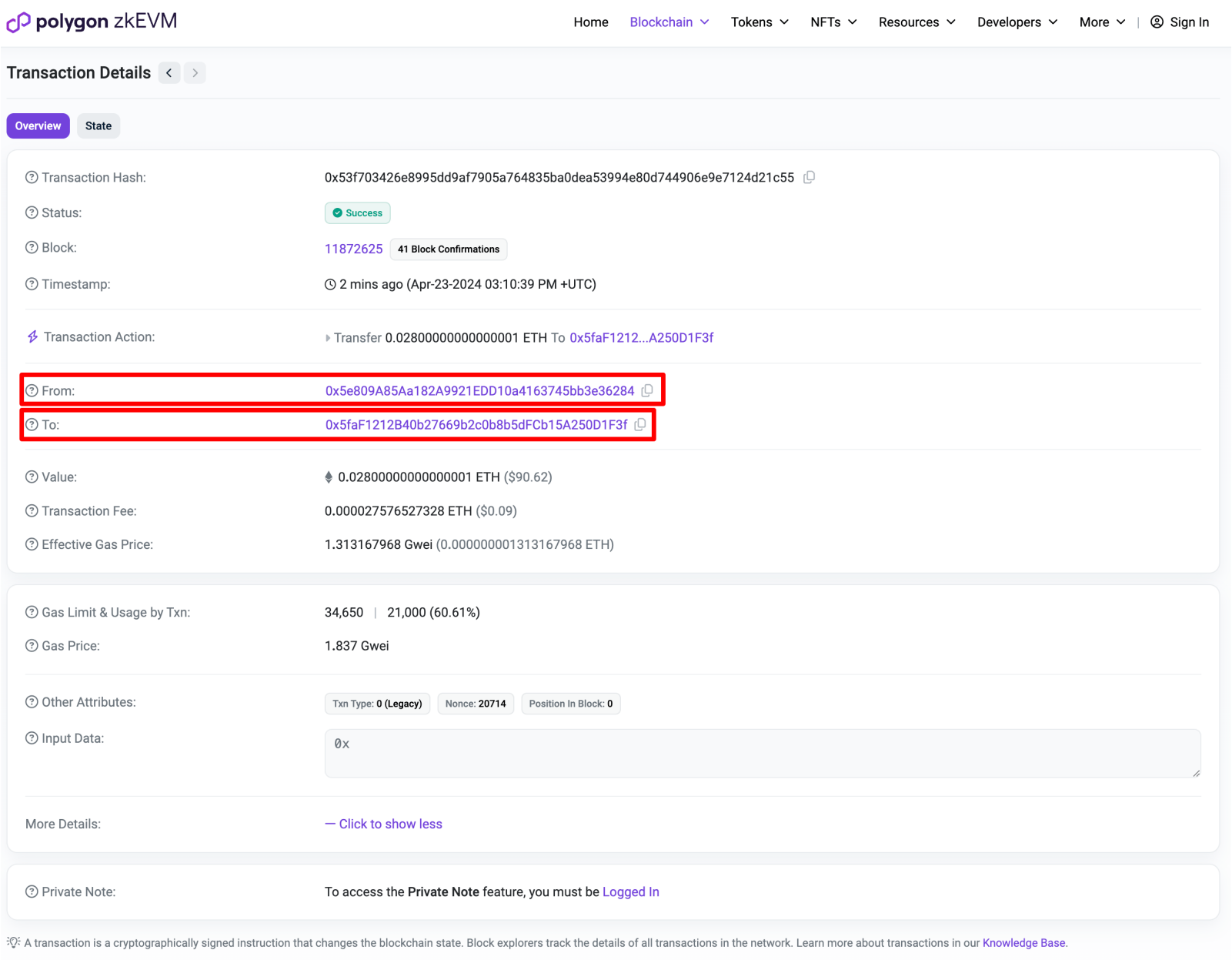
Exploring a zkRollup...



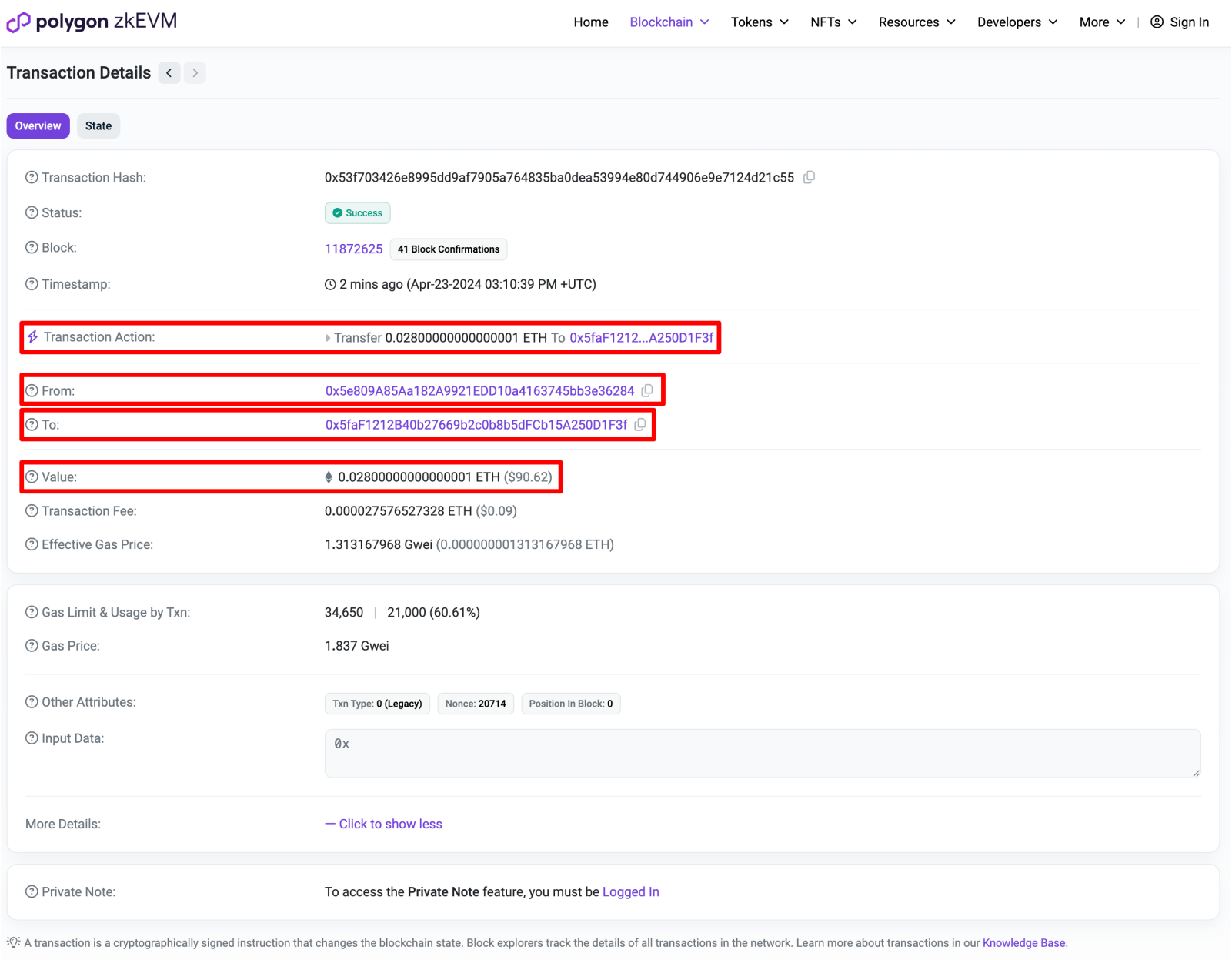
Exploring a zkRollup...



Exploring a zkRollup...



Exploring a zkRollup...



Exploring a zkRollup...

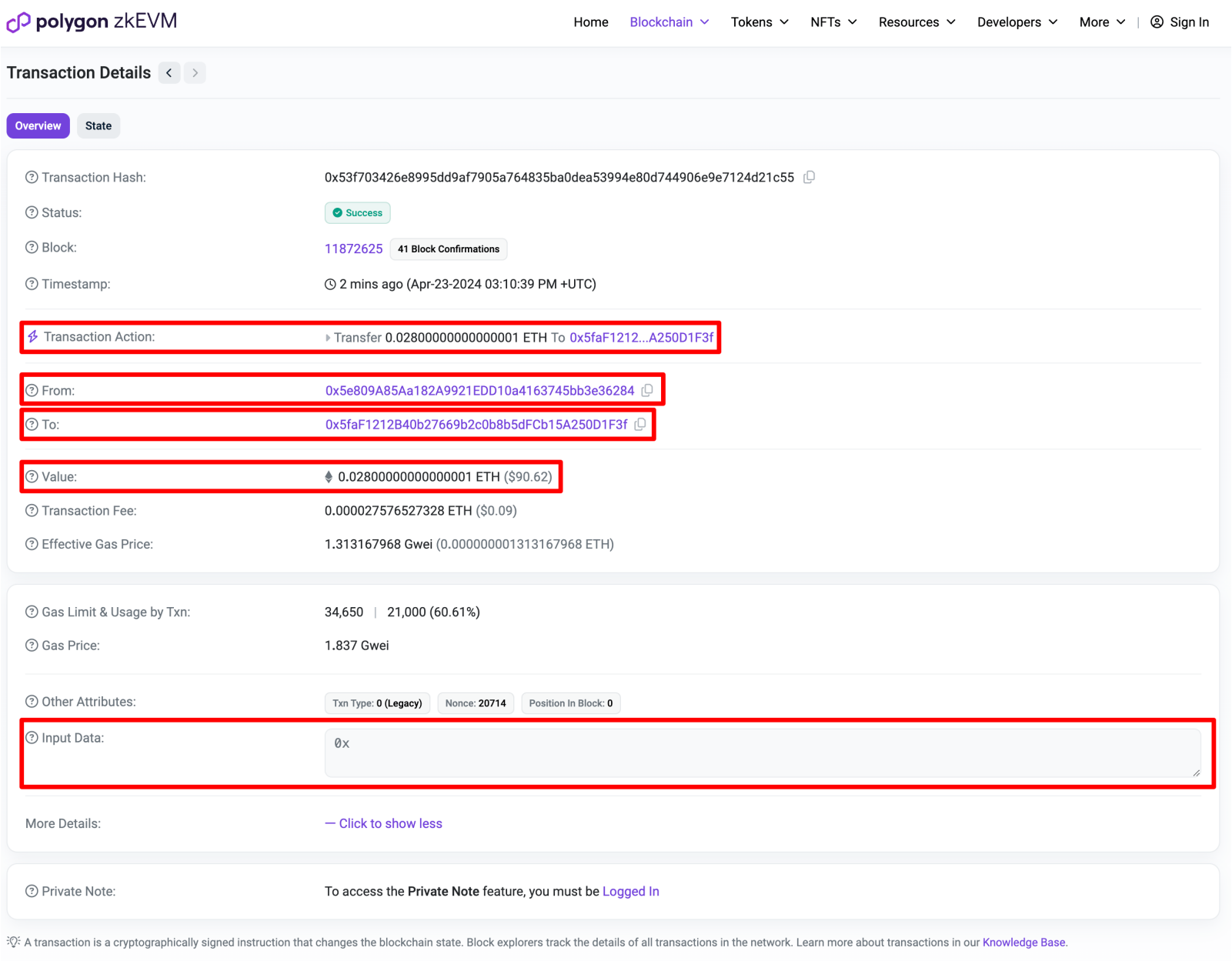


Table of Contents

SNARKs

SNARKs

- S Succinct

SNARKs

S Succinct: “means that the Proof is short.”

SNARKs

S Succinct: "means that the Proof is short."

N Non-interactive

SNARKs

S Succinct: "means that the Proof is short."

N Non-interactive: "means that the Proof is 'static', consisting of a single message from the Prover."

SNARKs

S Succinct: "means that the Proof is short."

N Non-interactive: "means that the Proof is 'static', consisting of a single message from the Prover."

AR ARguments

SNARKs

- **S** Succinct: "means that the Proof is short."
- **N** Non-interactive: "means that the Proof is 'static', consisting of a single message from the Prover."
- **AR** ARguments: "ensures protection for the Verifier against a computationally bounded Prover."

SNARKs

- **S** Succinct: "means that the Proof is short."
- **N** Non-interactive: "means that the Proof is 'static', consisting of a single message from the Prover."
- **AR** ARguments: "ensures protection for the Verifier against a computationally bounded Prover."
- **K** of Knowledge

SNARKs

- **S** Succinct: "means that the Proof is short."
- **N** Non-interactive: "means that the Proof is 'static', consisting of a single message from the Prover."
- **AR** ARguments: "ensures protection for the Verifier against a computationally bounded Prover."
- **K** of Knowledge: "means that the protocol establishes not only that the statement is true, but also that the Prover *knows* a 'witness'."

SNARKs

- **S** **Succinct**: "means that the Proof is short."
- N Non-interactive: "means that the Proof is 'static', consisting of a single message from the Prover."
- AR ARguments: "ensures protection for the Verifier against a computationally bounded Prover."
- K of Knowledge: "means that the protocol establishes not only that the statement is true, but also that the Prover *knows* a 'witness'."

Renaming zkRollups

sucRollup Succinct Rollup?

Renaming zkRollups

sucRollup Succinct Rollup?

ivcRollup IncrementallyVerifiableComputation Rollup?

Renaming zkRollups

sucRollup Succinct Rollup?

ivcRollup IncrementallyVerifiableComputation Rollup?

Or... Rollup + Privacy

Renaming zkRollups

sucRollup Succinct Rollup?

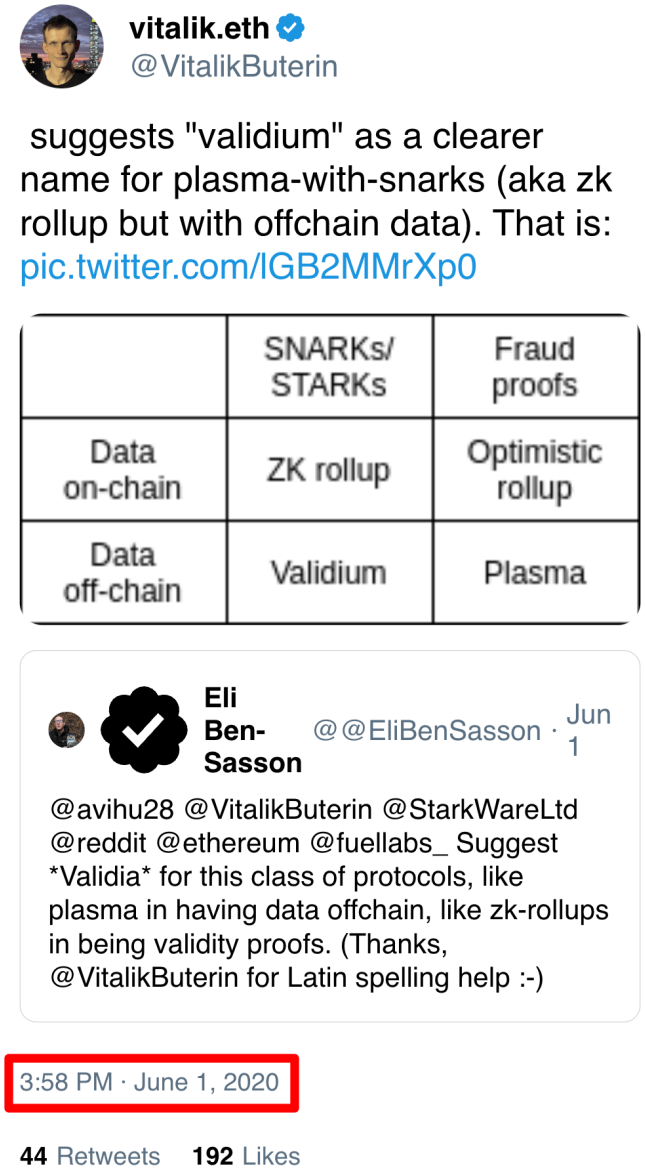
ivcRollup IncrementallyVerifiableComputation Rollup?

Or... Rollup + Privacy

zkzkRollup Zero-Knowledge(Zero-Knowledge Rollup)?

Table of Contents

Original classification



vitalik.eth ✓
@VitalikButerin

suggests "validium" as a clearer name for plasma-with-snarks (aka zk rollup but with offchain data). That is: pic.twitter.com/lGB2MMrXp0

	SNARKs/ STARKs	Fraud proofs
Data on-chain	ZK rollup	Optimistic rollup
Data off-chain	Validium	Plasma

Eli Ben-Sasson @@EliBenSasson · Jun 1

@avihu28 @VitalikButerin @StarkWareLtd @reddit @ethereum @fuellabs_ Suggest *Validia* for this class of protocols, like plasma in having data offchain, like zk-rollups in being validity proofs. (Thanks, @VitalikButerin for Latin spelling help :-)

3:58 PM · June 1, 2020

44 Retweets **192** Likes

New classification

cal (zk/acc)
@calummoore

sorry, but this is what the table should actually be
pic.twitter.com/w7Q64RQG40

	SNARKs/ STARKs	Fraud proofs
Data **Public**	~~ZK-rollup~~ **succinct rollup**	Optimistic rollup
Data **Private**	~~Validium~~ **zk-rollup**	~~Plasma~~ **impossible**

vitalik.eth @@VitalikButerin · Jun 1

@EliBenSasson suggests "validium" as a clearer name for plasma-with-snarks (aka zk rollup but with offchain data). That is:
pic.twitter.com/lGB2MMrXp0
x.com/EliBenSasson/s…

7:00 PM · April 18, 2024

1 Retweet **6** Likes

Table of Contents

SNARKs

S **Succinct**

N Non-interactive

AR ARguments

K of Knowledge

(zk)SNARKs

(zk) Zero-Knowledge $\Rightarrow$ as *a* way to enable Privacy

S **Succinct**

N Non-interactive

AR ARguments

K of Knowledge

Adding Privacy to Rollups

From Satybaldy et al. (2020)

Adding Privacy to Rollups

From Satybaldy et al. (2020)

- Zero-Knowledge Proofs (zkSNARK or zkSTARK)

Adding Privacy to Rollups

From Satybaldy et al. (2020)

- Zero-Knowledge Proofs (zkSNARK or zkSTARK)
- Secure Multi-party Computation

Adding Privacy to Rollups

From Satybaldy et al. (2020)

- Zero-Knowledge Proofs (zkSNARK or zkSTARK)
- Secure Multi-party Computation
- Homomorphic Encryption

Adding Privacy to Rollups

From Satybaldy et al. (2020)

- Zero-Knowledge Proofs (zkSNARK or zkSTARK)
- Secure Multi-party Computation
- Homomorphic Encryption
- Commitment Schemes

Adding Privacy to Rollups

From Satybaldy et al. (2020)

- Zero-Knowledge Proofs (zkSNARK or zkSTARK)
- Secure Multi-party Computation
- Homomorphic Encryption
- Commitment Schemes
- Mixing

Adding Privacy to Rollups

From Satybaldy et al. (2020)

- Zero-Knowledge Proofs (zkSNARK or zkSTARK)
- Secure Multi-party Computation
- Homomorphic Encryption
- Commitment Schemes
- Mixing
- Ring Signatures

Adding Privacy to Rollups

From Satybaldy et al. (2020)

- Zero-Knowledge Proofs (zkSNARK or zkSTARK)
- Secure Multi-party Computation
- Homomorphic Encryption
- Commitment Schemes
- Mixing
- Ring Signatures
- Differential Privacy

Adding Privacy to Rollups

From Satybaldy et al. (2020)

- **Zero-Knowledge Proofs (zkSNARK or zkSTARK)**
- Secure Multi-party Computation
- **Homomorphic Encryption**
- **Commitment Schemes**
- Mixing
- Ring Signatures
- Differential Privacy

Conclusions

- Next steps for zkRollups (after decentralisation)

Conclusions

- Next steps for zkRollups (after decentralisation)
- Currently some projects aiming to do that

Conclusions

- Next steps for zkRollups (after decentralisation)
- Currently some projects aiming to do that
  - Aztec: "Privacy-first L2 on Ethereum"

Conclusions

- Next steps for zkRollups (after decentralisation)
- Currently some projects aiming to do that
  - Aztec: "Privacy-first L2 on Ethereum"
  - Payy (but UTXO-based...)

Thank you for your attention!

@0xAdriaTorralba

0xAdriaTorralba

atorralbaag@uoc.edu

QR Code to my research