bitfwd

Privacy Fundamentals

t.me/bitfwd

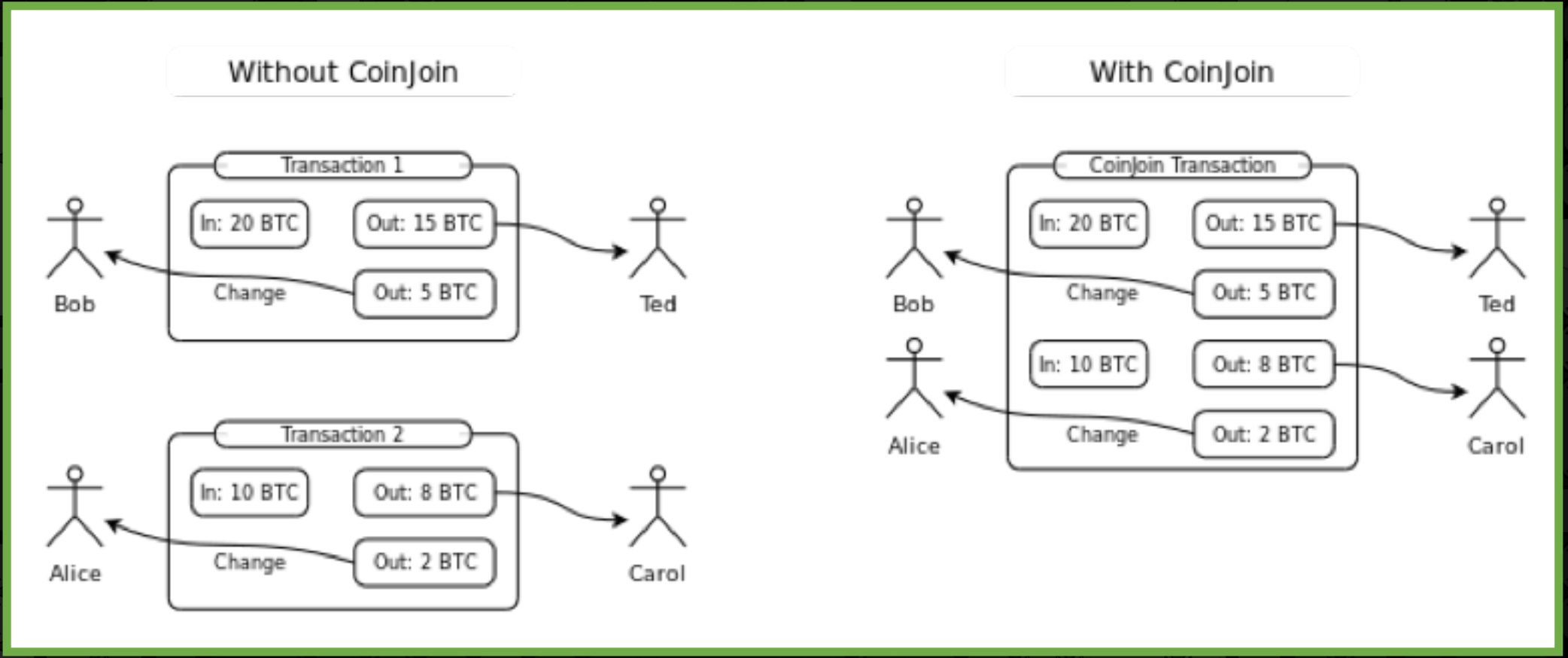
Tumblers

How do tumblers work?

- Users put funds into a giant pot.
- Coins (UTXO's) are mixed around.
- User takes same amount of money they put in.

bitfwd

How do they work?



Cons

- Centralised
- Limited Anonymity
- Requires participants to be online.

Pros

- Flexible
- Simple to implement
- Lightweight

bitfwd

Cryptonote & Ring Signatures

How do Ring Signatures work?

- Proves someone signed a transaction from a group of people without revealing who it was.

How does CN use Ring Sigs?

- User makes transaction.
- User takes outputs of similar transactions that are already on the blockchain to use as inputs to RS tx.
- Unclear who the transaction is for.
- All users are participants.
- RingCT hides amounts.

Cons

- Large tx sizes (~13kb) with RingCT
- Privacy limited by ring size
- Not quantum proof
- No supply auditability (with RingCT)

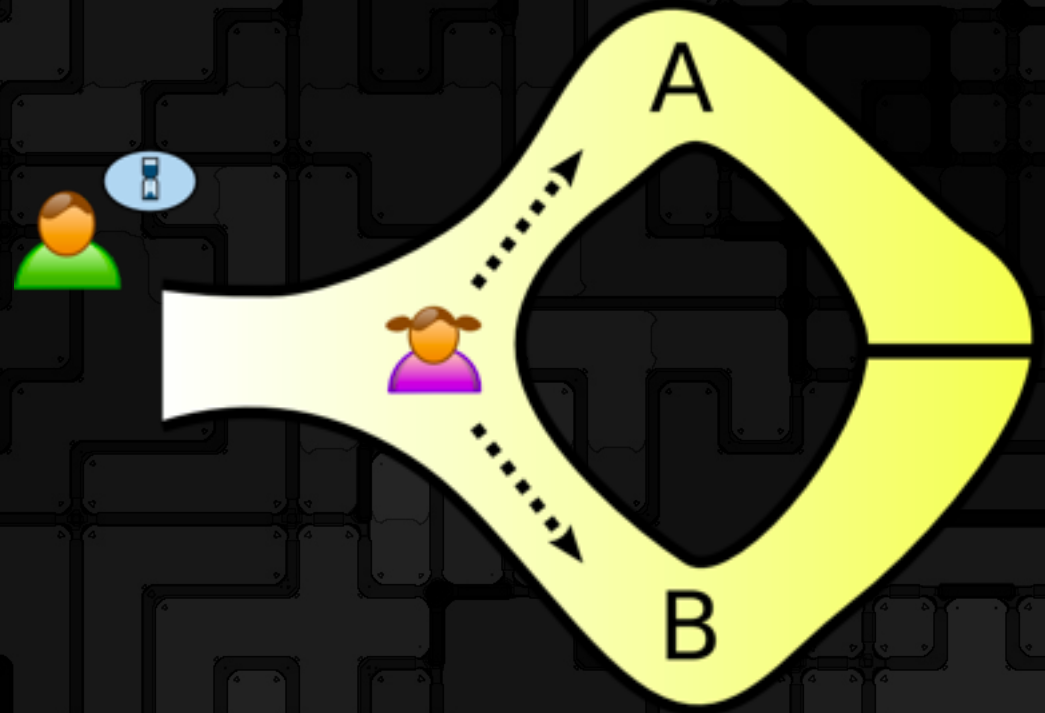
Pros

- No need for a mixer and mixing is done automatically.
- Anonymity set increases over time.
- Transaction amounts hidden.
- Well researched cryptography.

Zerocoin & Zcoin

bitfwd

What is a Zero Knowledge Proof?



How does Zerocoin work?

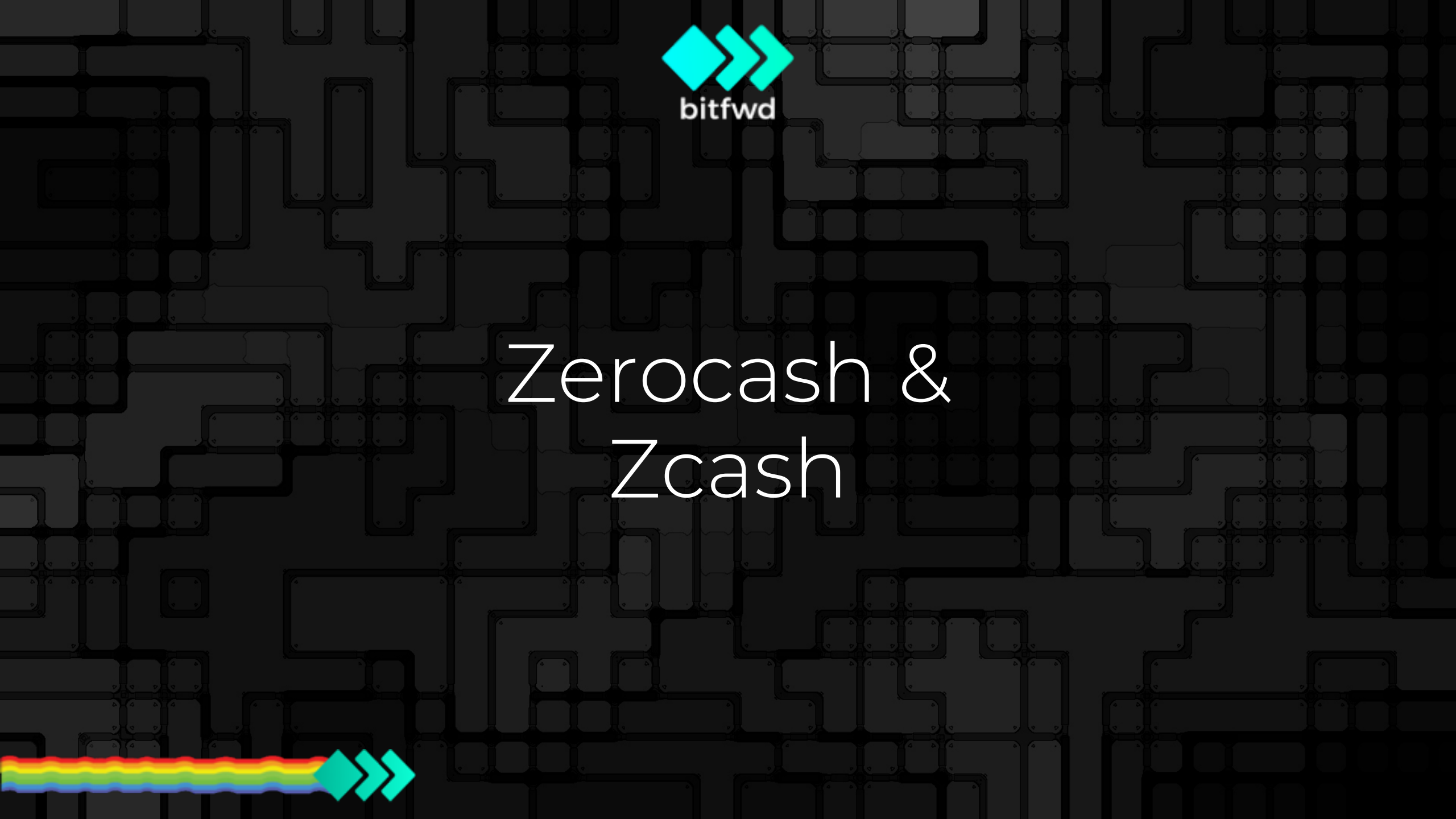
- Zerocoin uses ZKP to provide privacy
- Users can burn any number of coins (a Zerocoin mint)
- Users can then mint an equivalent number of brand new coins (a Zerocoin spend).

Cons

- Trusted one time setup
- Spend tx are huge (~25kb vs Monero's ~13kb)
- Spend tx are computationally intensive to verify (~0.5s)

Pros

- No need for mixing
- Breaks transaction links
- Larger anonymity set than Monero
- Maintains supply auditability
- Uses well researched cryptography



Zerocash & Zcash

How does Zcash work?

- Zcash uses zkSNARKs
- ZKP on steroids
- Allows you to prove some computational fact about data without revealing the data
- Zcash encrypts all the data

Cons

- Requires a trusted setup.
- No supply auditability.
- Bleeding edge technology.
- Generation of privacy tx takes a long time (~60s on a powerful computer)

Pros

- Largest anonymity set (includes all coins minted)
- Breaks transaction links
- Proof sizes are small (~1kb)
- Proofs are fast to verify, faster than Zcoin
- Hides transaction amounts

bitfwd

A Privacy Framework

Privacy

- Statistical obfuscation
- Breaking transaction links

Scalability

- Size of proof affects size of transaction.
- Smaller proofs ideal but can come with trade-offs.

Computational Difficulty

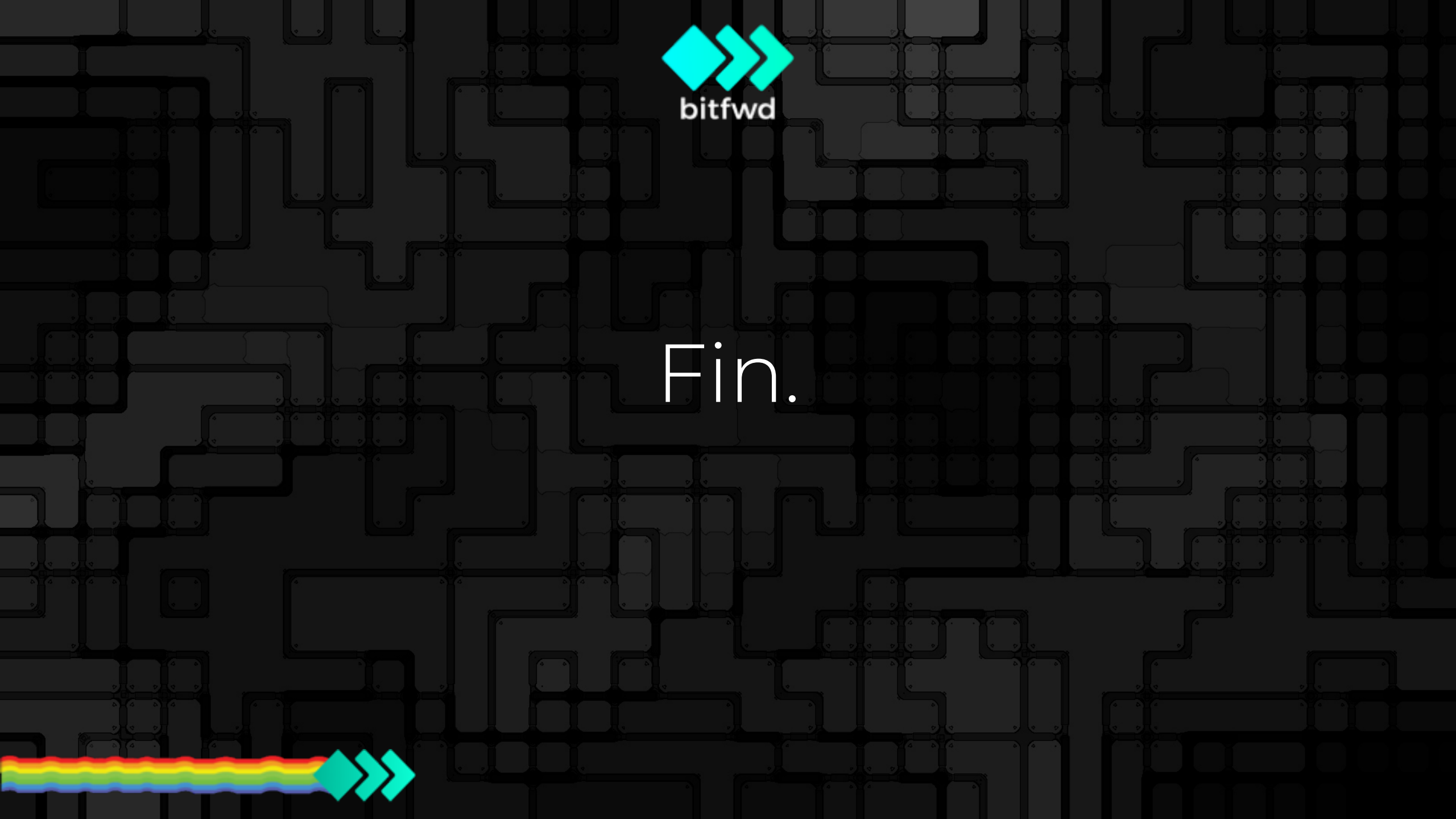
- Computation used at two different times: proof generation & validation
- Important to ensure that computational difficulty for validation is low.

Reliability

- Reliability or trustworthiness of underlying technology
- In general, the more time has passed and the more products use this service, the more reliable it is

Completeness Of Privacy

- Privacy is not limited to just the blockchain: can be leaked.



Fin.