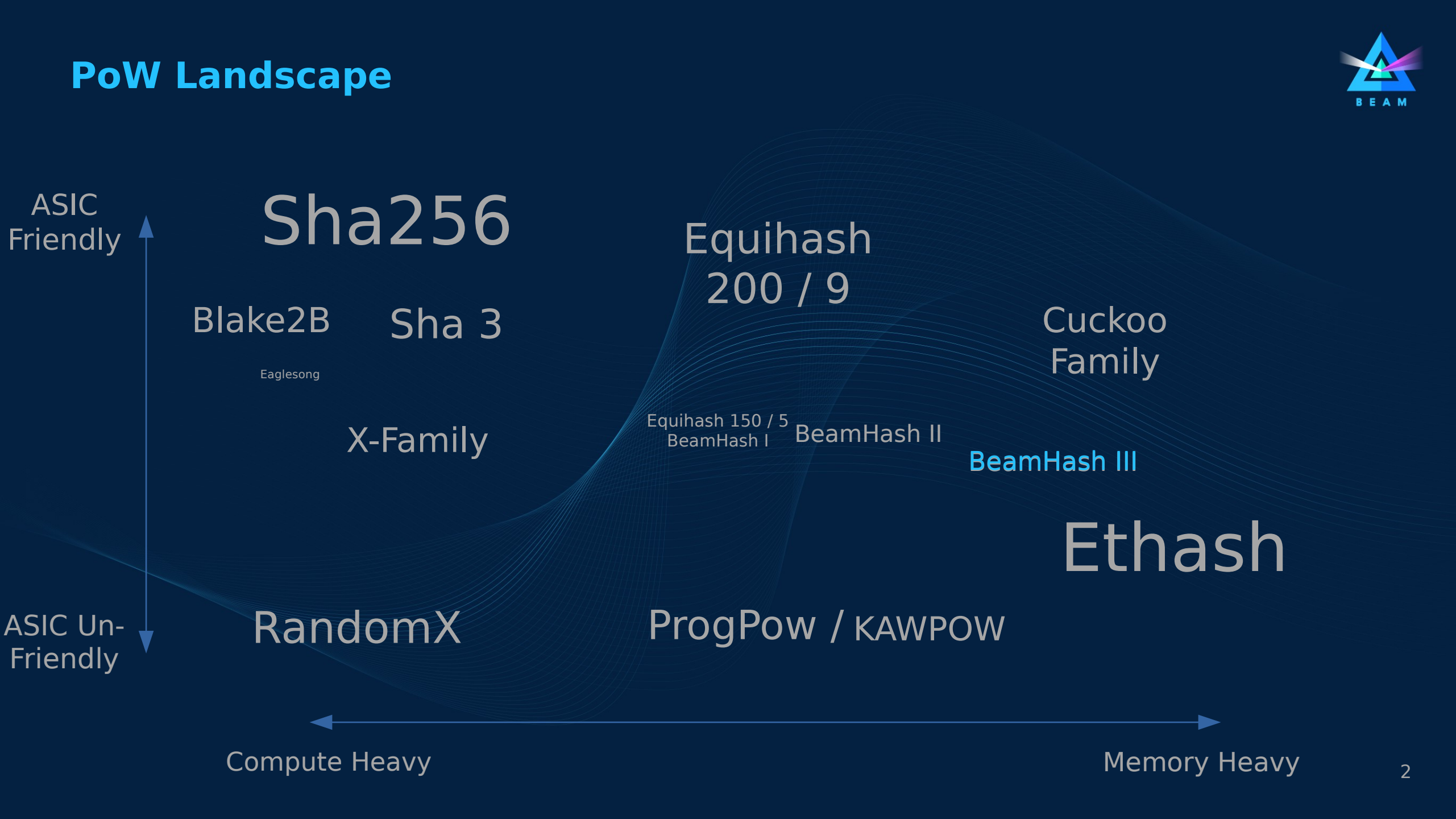
Introduction to Beam Hash III

Wilke Trei

PoW Landscape



Aspects of ASIC friendliness

Multiple different aspects to consider

- Benefit of ASIC over common hardware
- Development effort
- Expected chip size
- Stability of PoW

Not one Type of ASIC

- Single chip ASICs
  - Often much quicker
  - Larger chip size

- Multi chip ASICs
  - Smaller chips with distinguished function
  - Cheaper, but slower

Beam PoW Strategy

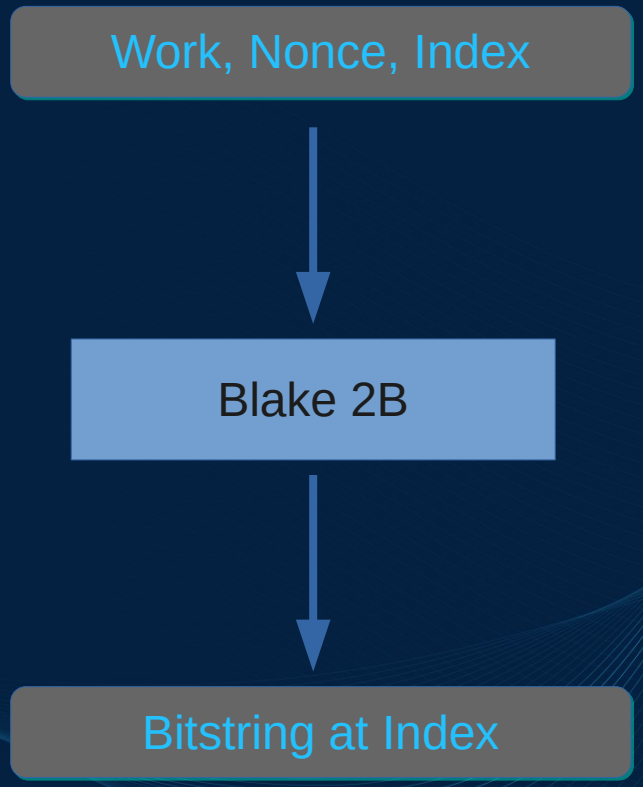
Why not change the PoW every 6 month?

- Avoid disruption of mining ecosystem
- Mining is important – but it is not everything
- Stable consensus is only path to mass adoption

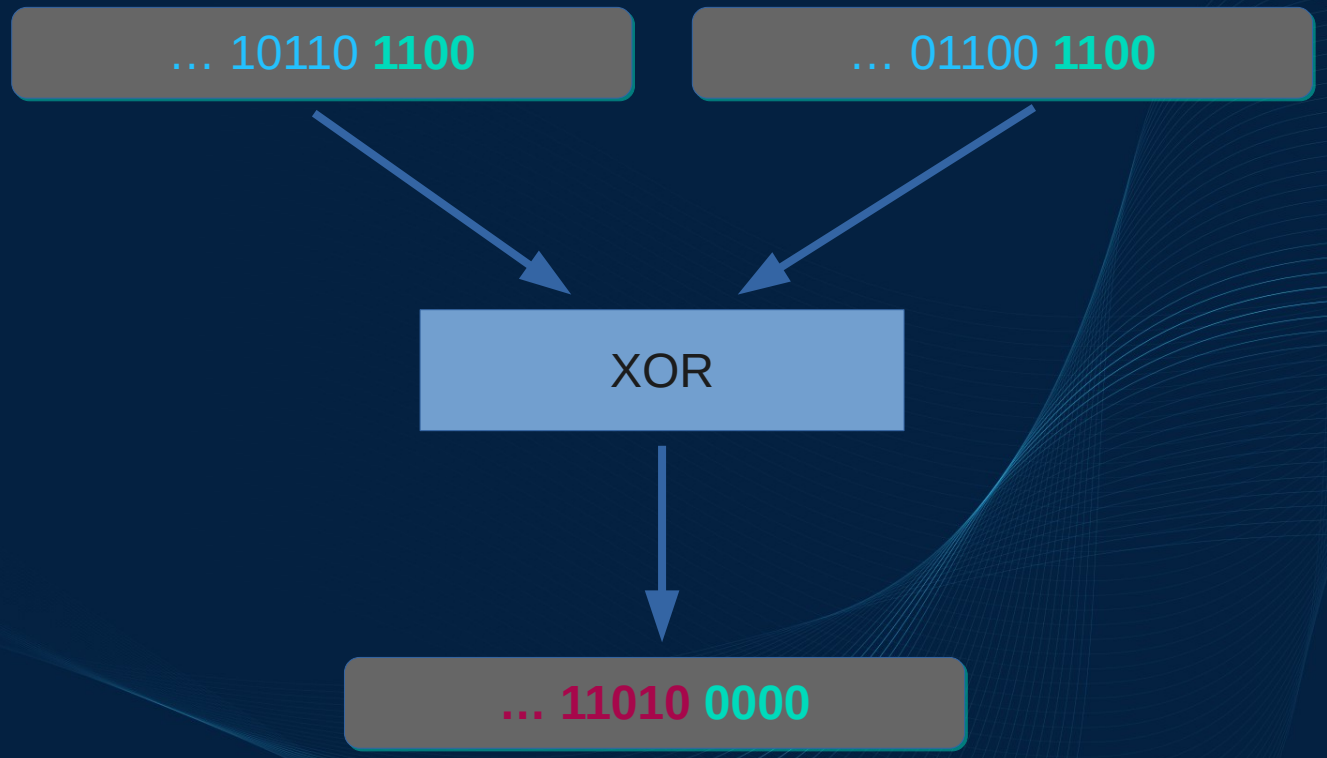
Beam PoW Stragegy

- Give GPU miners a head start
- Make mining as relaxing as possible
- When first ASICs come: make them “cheap”

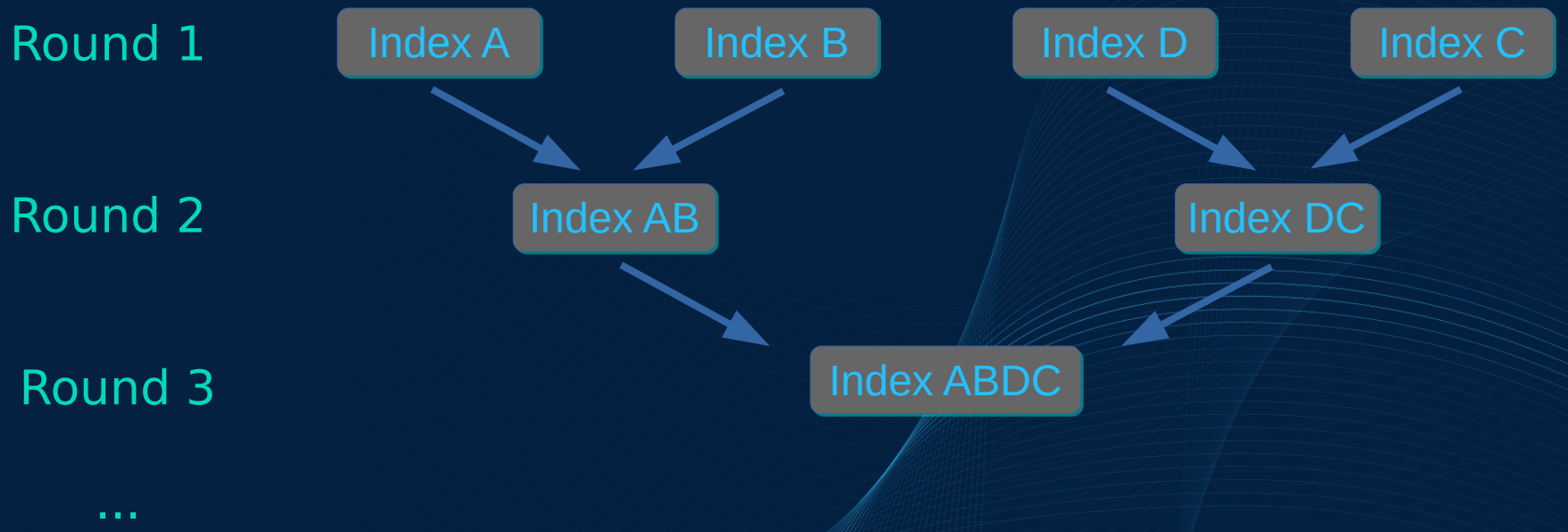
Some Equihash Basics - Generation



Some Equihash Basics - Matching



Some Equihash Basics – Growing Index Tree



For BeamHash I / II:

- We match 25 bits each rounds (50 in the last)
- 5 Rounds total – so 32 indexes that give a 0 xor

What could be better?

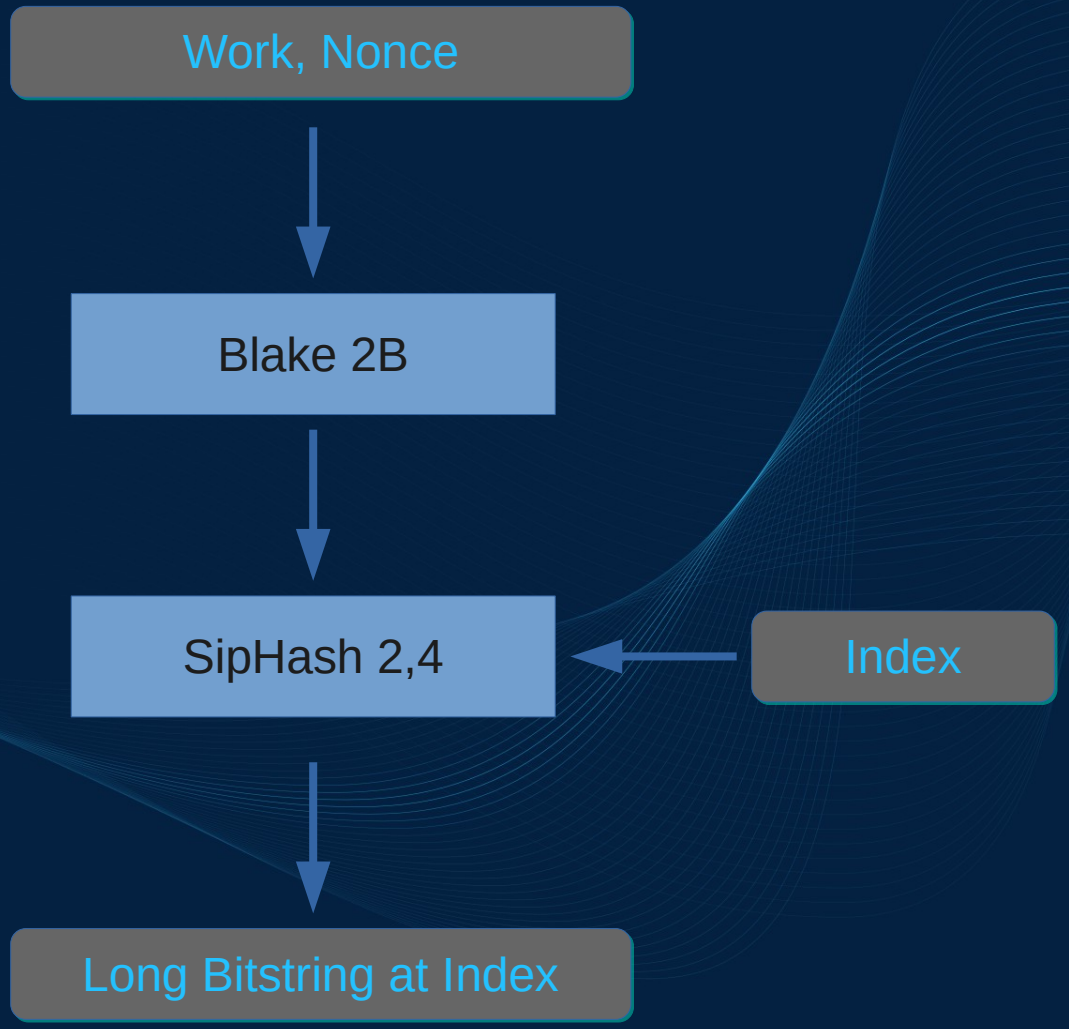
Implementation Aspects

- The number of bits moved changes every round
- The index tree is scattered
- Massive filtering of invalids required

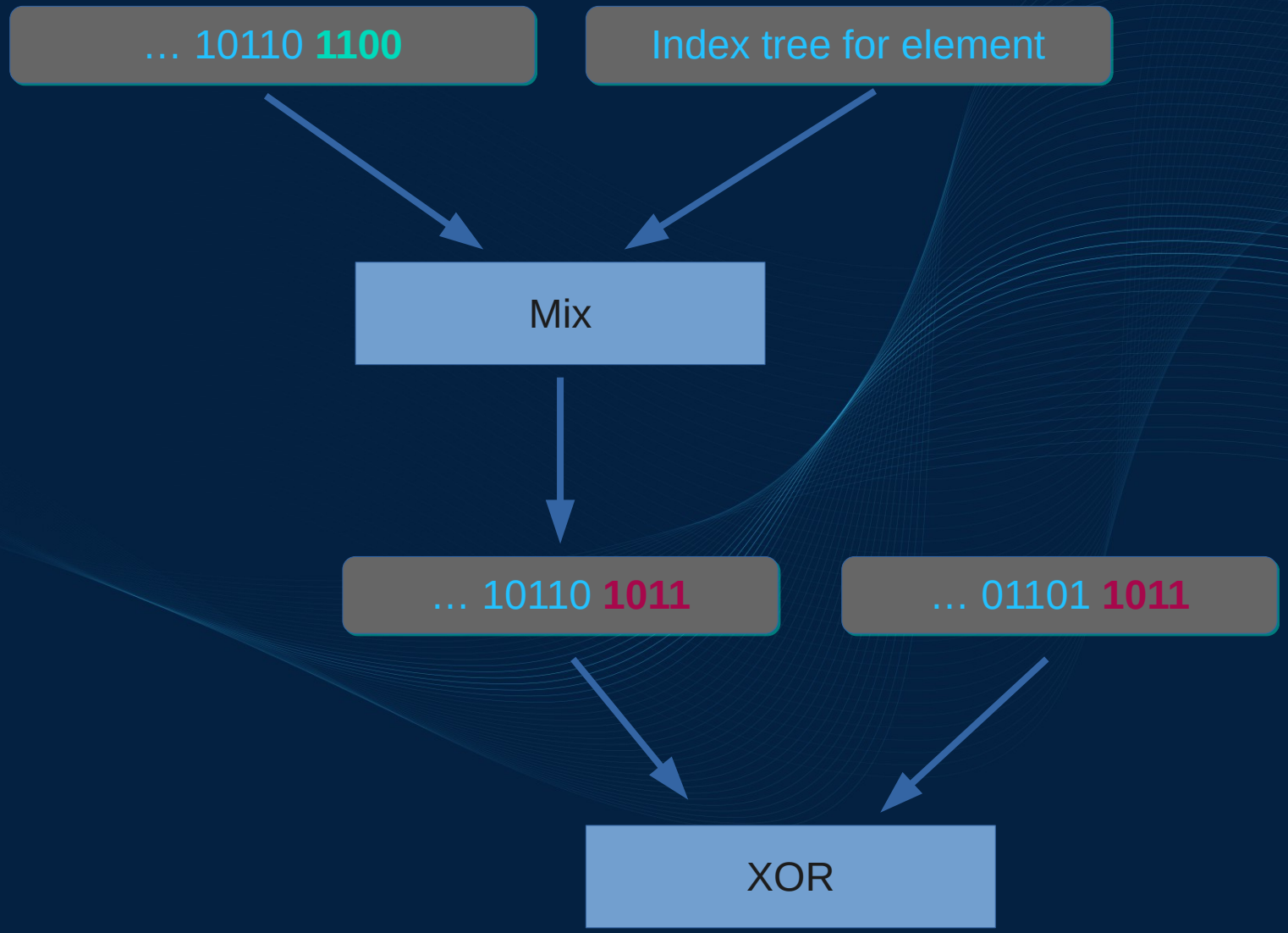
Algorithmic Aspects

- Blake2B is quite compute heavy
- The elements to be load / stored are rather small

BeamHash III Basics - Generation



BeamHash III Basics – Mixing before Round



Beam Hash III Basic Properties

Implementation Aspects

- We start with 448 bit element length and decrease this so the total number of element bits + index tree fits 64 byte
- The index tree is part of mix and is no longer scattered
  → This gives a very simple memory layout
- No more filtering of invalids midway

Algorithmic Aspects

- The generation is much less compute heavy
- Each load / store is 64 byte and fits well the L2 cache architecture of currently state of the art GPUs

Conclusion

Beam Hash III ...

- ... is easier to implement then Beam Hash I / II
- ... fits well into 5G memory (4G and 3G are possible)
- ... is made to utilize the memory bandwidth of all current GPUs better then any other Equihash
- ... is single chip ASIC “resistant” for the next years
- ... allows affordable multi chip ASIC designs

... is a good PoW for Beam to go with