Schnitzeljagd - a signature chain consensus algorithm

Author: Alexander Klassen

This is more of a concept paper rather than a full specification and should be treated as such.

Idea

Schnitzeljagd is a consensus algorithm that aims to enable and encourage cooperative block mining.

It does so by establishing a chain of signatures as proof of work, where every address in this signature chain is rewarded once the block is mined.

Each entry in the signature chain is restricted by the previous, making it the objective to find an address fittinig for the next position.

How it works

In order for a block to be mined it needs to have a signature chain of a given length P

.

Each entry in this signature chain is a pair of address and signature.

position

CLUE

ADDR

CLUE_KEY

SGN

0

BLOCK_HASH

ADDR_0

hash(ADDR_0 + BLOCK_HASH)

signature(ADDR_0, BLOCK_HASH + CLUE_0)

1

hash(SGN_0)

ADDR_1

hash(ADDR_1 + BLOCK_HASH)

signature(ADDR_1, BLOCK_HASH + CLUE_1)

n

hash(SGN_${n-1})

ADDR_n

hash(ADDR_2 + BLOCK_HASH)

signature(ADDR_2, BLOCK_HASH + CLUE_n)

CLUE_0 = BLOCK_HASH

CLUE_n = hash(SGN_${n-1})

CLUE_KEY = hash(ADDR + BLOCK_HASH)

Only the address and the signature are stored in the chain as CLUE and CLUE_KEY can be deduced.

address restriction

ADDR fits in position n if the first y

bits of CLUE_KEY

and CLUE_n

are the same.

Routes

When a specific block is being mined multiple CLUE_KEYs can be found for the same CLUE. Because different CLUE_KEYs create different signatures and thereby different next CLUEs, the signature chain kind of branches out, creating multiple possible routes. This looks similar to how lightning strikes find their path through the air: https://youtu.be/qQKhIK4pvYo?t=298

More routes make it easier for leverage the same CLUE_KEY while mining a block, as it can be tried out on every route.

Difficulty Parameters: y

& P

Schnitzeljagd difficulty can be adjusted by the two parameters:

- y - the numbers of bits have to match when comparing CLUE and CLUE_KEY
- P - the target length of the signature chain.

While both of them directly effect the difficulty, they can also be used to alter the network behaviour when searching for CLUEs.

For example would it be a good idea to set the y of the exit position higher to decrease the risk of two simultaneously mined blocks.

Setting a higher P and lowering y could result in a same difficulty while further diversifying rewards.

Rewarding

Every address in the signature chain will get rewarded once the block is mined. Whether the reward should be distributed equally or somehow dependent on the difficulty of each position is to be determined.

Possible Modifications

The algorithm can be further modified, depending on the needs.

Special Objectives

The parameter y could is a signed integer. Positive values define difficulty as before, negative values are identifiers for special objectives.

A special objective could be any restriction defined by the protocol.

Idea 1:

A special objective could be that the address, signing at this position, is in some way trusted, making it impossible to mine a block in solitude.

Idea 2:

The first position objective could be that the signature is given by some trusted network member, thereby controlling the number of candidate blocks.

Idea 3:

In a permissioned blockchain the restriction could be, that some positions needs to be signed by a specific group of addresses, for example a department, acknowledging the block.

CLUE_KEY not position agnostic

The CLUE_KEY may be computed for a specific CLUE, making the mining harder and precluding the reuse of CLUE_KEYs on different routes.

CLUE_KEY_n = hash(ADDR + BLOCK_HASH + CLUE_${n-1})

Lucky keys

A CLUE_KEY can match more than the expected y bits of the CLUE, making it a lucky key. Lucky keys reduce the difficulty of the resulting CLUE by the half of the overmatched bits.

This results in more desired routes with lucky keys, making them more preferable even if they have short signature chains.

A lucky key should not reduce the difficulty of the exit position, as this would increase the risk of simultaneously mined blocks.

The Schnitzel

The signature of the last position is called Schnitzel

.

This is a rough idea and I would like to get some feedback.