

Claims

Claim 1

A method to enhance blockchains comprising:

one or more values (421, 422) chained from the future towards the past;

a cryptographic one-way function (317) applied between adjacent blocks, such that the value of an earlier block can be fast calculated from the value of the next later block, while calculating the value of the next later block from an earlier block is cryptographically hard;

and a storage (303, 304) to hold one or more secrets.

Claim 2

A method according to claim 1, characterized in that, the blockchain does not need any "proof of work" function.

Claim 3

A method according to claim 1, characterized in that, the blockchain does not need to comprise multiple systems to provide trusted blocks.

Claim 4

A method according to claim 1, comprising: a back-step seal value (418);

a mathematical function, such that the back-step seal value is mathematically combined (411) with the hash value of the previous block (208);

a cryptographic one-way function (412), whereby the result is protected against reverse calculation;

an insertion of such calculated result in a field of the block, to enable further detection of manipulations of the blockchain.

Claim 5

A method according to claim 1, characterized in that, a defined fixed number of blocks can be calculated, such that the chain has a predefined end.

Claim 6

A method according to claim 1, comprising:

one or more one-way functions (317, 318);

a set of multiplexers (311,312,323,324); and

a control logic (308), such that back chained values can be pre-calculated.

Claim 7

A method according to claim 1, comprising: a non-volatile storage holding intermediate checkpoint values;

a control logic to store and fetch these values, such that, required calculation of back-step and back-step seal values can start at values that are nearest to the required step.

Claim 8

A method according to claim 7, comprising:

one or more volatile cache storage layers;

a cache control logic;

a set of multiplexers, characterized in that, intermediate chain values can be precalculated and stored for fast access and use.

Claim 9

A method according to claim 8, wherein a second set of cache storage is provided, such that one cache is filled while the other cache is emptied.

Claim 10

A method according to claim 4, comprising:

an authentication function;

one or multiple authentication secrets;

a data protection function;

data protection secrets, such that,

an authenticated person, organization or process can request and receive back-step-seal values related to a requested block.

Claim 11

A method according to claim 1, characterized in that, the number of operations to generate a block is fixed resulting in a fixed response time for real time back-step blockchain applications.

Claim 12

A method according to claim 1, characterized in that, the embodiment is in one or multiple integrated circuits.

Claim 13

A method according to claim 1, characterized in that, the embodiment is integrated into a smartphone.

Claim 14

A method according to claim 1, characterized in that, the embodiment is integrated into an apparatus where data are sensed.

Claim 15

A method according to claim 1, characterized in that, the embodiment is integrated into an apparatus where data are recorded.

Claim 16

A method according to claim 1, characterized in that, the embodiment is integrated into an apparatus where instructions are executed.

Claim 17

A method according to claim 1, characterized in that, the embodiment is integrated into a data processing system.

Claim 18

A method according to claim 1, characterized in that, the embodiment is integrated into a data communication system.

Claim 19

A method according to claim 1, characterized in that, the embodiment is integrated into a legal identity document.

Claim 20

A method according to claim 1, characterized in that, the embodiment is integrated into a personalized payment device.