

soon as possible. In particular, a fast data synchronisation of the data stored in the peer-to-peer application and on the node with the error and the data stored in the peer-to-peer application and on the further nodes of the peer-to-peer network is required.

5

Therefore, embodiments of the present disclosure seek to provide a peer-to-peer network having at least two nodes, which enables a tamper-proof storing of data in a peer-to-peer application and, in particular, which allows the restoration of a full functionality of the node after occurrence of operation error within a short period of time.

10

According to a first aspect of the present disclosure, there is provided a peer-to-peer network according to claim 1. The peer-to-peer network comprises at least one first node comprising at least one first clock module. The first node comprises at least a part of at least one peer-to-peer application. The peer-to-peer network comprises at least one second node comprising at least one second clock module. The second node comprises at least a part of the peer-to-peer application. The peer-to-peer network comprises at least one establishable communication connection between the first node and the second node. The first node comprises at least one first synchronization clock module. The second node comprises at least one second synchronization clock module. At least the first synchronization clock module is configured to transmit at least one first synchronization clock message to the second synchronization clock module via the communication connection. The second synchronization clock module is configured to synchronize the clock signal of the second clock module to the clock signal of the first clock module based on synchronization information included in the first synchronization clock message. The first node comprises a first signing module configured to sign the first synchronization clock message with a signature. The signature of the first synchronization clock message is validated by two or more nodes of the nodes of the peer-to-peer network.

15

20

25

30

In contrast to the prior art, the peer-to-peer network according to the present inventions enables to store data in a peer-to-peer application in a tamper-proof way

by providing an improved (time) synchronization mechanism. Clock offsets between a clock signal of the first node and a clock signal of a second node are at least reduced by transmitting first synchronization clock message(s) from the first node to the second node, wherein the at least one message comprises synchronization information

These block chains are connected via frameworks, such as sidechains or smart contracts.

Financial values can be (instantaneously) exchanged with a transaction via a
5 cryptocurrency. In a further embodiment, micropayment channels are used for a
constant payment stream that can be handled party off-chain to reduce the amount of
on-chain transactions. In a further embodiment so called state channels or state
networks (e.g. Raiden Network) may be used to exchange digital tokens off-chain in a
secure way. Opening and/or closing of state channels may be registered on the block
10 chain. This means that individual transactions may not be stored on the block chain in
order to improve scalability and avoid movement tracking of pseudonyms on the
block chain. According to the present invention, a man-in-the-middle is not necessary.
Fully automated processes from authentication to charging and billing can be
provided.

15 A further aspect of the present disclosure is a method for operating at least one peer-
to-peer network, in particular, a previously described peer-to peer network. The peer-
to peer network comprises at least one first node comprising at least one first clock
module and at least a part of at least one peer-to-peer application and at least one
20 second node comprising at least one second clock module and at least a part of the
peer-to-peer application. The method comprises:

- transmitting at least one first synchronization clock message from a first
synchronization clock module of the first node to a second synchronization
clock module of the second node via a communication connection between
25 the first node and the second node,
- synchronizing the clock signal of the second clock module to the clock signal
of the first clock module based on synchronization information included in
the received first synchronization clock message,
- signing the first synchronization clock message with a signature by the first
30 node, and
- validating the signature of the first synchronization clock message by two or
more nodes of the nodes of the peer-to-peer network.

Another aspect of the present disclosure is a first node of a peer-to-peer network, in particular, a previously described peer-to peer network. The first node comprises at least one first clock module. The first node comprises at least a part of at least one peer-to-peer application. The first node comprises at least one first communication
5 module configured to establish at least one communication connection to at least one communication module of at least one second node of the peer-to-peer network. The first node comprises at least one first synchronization clock module configured to generate at least one first synchronization clock message. The communication module is configured to transmit the first synchronization clock message to the
10 communication module of the second node. The first synchronization clock message comprises synchronization information configured to synchronize a clock signal of a second clock module of the second node to the clock signal of a first clock module of the first node.

15 A further aspect of the present disclosure is a second node of a peer-to-peer network, in particular, a previously described peer-to peer network. The second node comprises at least one second clock module. The second node comprises at least a part of at least one peer-to-peer application. The second node comprises at least one communication module configured to receive at least one first synchronization clock
20 message from a first node of the peer-to peer network. The second node comprises at least one second synchronization clock module configured to synchronize the clock signal of the second clock module to the clock signal of a first clock module of the first node based on synchronization information included in the received first synchronization clock message. The first synchronization clock message is processed
25 only in case the signature of the first synchronization clock message is valid, wherein the signature of the first synchronization clock message is validated by two or more nodes of the nodes of the peer-to-peer network.

A still further aspect of the invention is a node of a peer-to-peer network, in particular,
30 a previously described peer-to peer network. The node comprises at least a part of at least one peer-to-peer application. The node comprises at least one communication module configured to communicate with at least one further node of the peer-to peer

network. The node comprises at least one controlling module comprising at least one detecting means configured to detect at least one operation error of the node. The controlling module comprises at least one evaluating means configured to evaluate whether the detected operation error requires a data synchronization of the data
5 stored in the peer-to-peer application of the node. The controlling module comprises