

CLAIMS

1. A communication network node for providing data to a distributed ledger, wherein the node comprises circuitry configured to perform at least one of:
 - provide verification of input data which is used as input to a smart contract,
 - provide verification whether output data, which is based on an output from a smart contract, is correctly received at a predetermined device.
2. The communication network node of claim 1, wherein the input data are verified based on sensor data, the sensor data identifying a user.
3. The communication network node of claim 2, wherein the sensor data are provided by at least one sensor included in a mobile terminal of the user.
4. The communication network node of claim 2, wherein the sensor data are provided by at least one sensor detecting a user.
5. The communication network node of claim 2, wherein the circuitry is further configured to provide a certification of the sensor providing the sensor data.
6. The communication network node of claim 2, wherein the sensor data include location data or biometric data.
7. The communication network node of claim 6, wherein the location data are transmitted to a location server for verification.
8. The communication network node of claim 6, wherein the biometric data are transmitted to a biometric data server for verification.
9. The communication network node of claim 1, wherein the circuitry is further configured to receive or transmit data based on a data integrity functionality.

10. The communication network node of claim 9, wherein the data integrity functionality is based on at least one of: hash function, digital signature, block stream algorithm.
11. The communication network node of claim 1, wherein the circuitry is further configured to transmit a trigger for causing execution of the smart contract.
12. The communication network node of claim 1, wherein the circuitry is further configured to perform binding between a user based identification and a mobile terminal based identification.
13. The communication network node of claim 12, wherein the verification involves verification of the binding.
14. The communication network node of claim 12, wherein the mobile terminal based identification includes at least one of cellular international mobile subscriber identity, cellular international mobile station equipment identity.
15. The communication network node of claim 1, wherein circuitry is further configured to verify the authentication of a connected device.
16. The communication network node of claim 1, wherein the distributed ledger includes a blockchain.
17. The communication network node of claim 1, wherein the distributed ledger includes data for mobility as a service.
18. A method for operating a smart contract, wherein the smart contract has at least two different states, the method comprising:
changing a state of the smart contract in response to receiving a trigger.
19. The method of claim 18, wherein the trigger is received from a trusted network communication node.
20. The method of claim 18, wherein the trigger is received from a trusted sensor.