Sweden

(12) Patent specification (10) SE 542 329 C2

(21) Patent application number:	1750684-1	(51) Int.Cl.:	
(45) Grant of patent:	2020-04-14	***G06Q 30/06***	(2012.01)
(41) Available to the public:	2018-12-01		
(22) Filing date:	2017-05-31		
(24) Effective date:	2017-05-31		
(30) Priority data:	---		

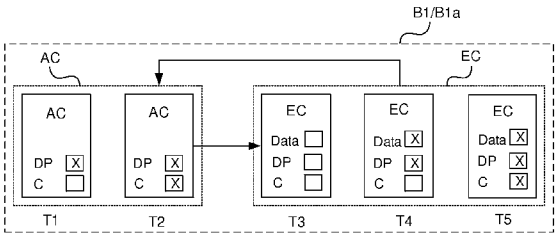
(73) Patentee: Scania CV AB, , 151 87 Södertälje SE
(72) Inventor: Marcus Löf, Stockholm SE
Jim Lindberg, Stockholm SE
(74) Agent: Scania CV AB, , 151 87, Södertälje SE

(54) Title: Method and system for performing data transactions in exchange for assets on a network

(56) Cited documents: US 2016260171 A1 · US 2017011460 A1

(57) Abstract:

The present invention relates to a method for performing data transactions in exchange for assets on a network. An agreement contract (AC) intended to be digitally signed by a network member acting as a data provider (DP) is provided. Said AC is intended to be digitally signed by at least one other network member acting as an asset committer (C) and to be made available for network members as signed. Said AC specifies rules for obtaining data to be provided. Upon signing of said AC by said data provider and said at least one other network member an enforcement contract (EC) intended to be digitally signed by said DP is provided. Said EC points back to the AC and is intended to comprise, in encrypted form, said data to be provided. Said EC is intended to be signed by said at least one asset C.



The present invention relates to a method for performing data transactions in exchange for assets on a network. An agreement contract (AC) intended to be digitally signed by a network member acting as a data provider (DP) is provided. Said AC is intended to be digitally signed by at least one other network member acting as an asset committer (C) and to be made available for network members as signed. Said AC specifies rules for obtaining data to be provided. Upon signing of said AC by said data provider and said at least one other network member an enforcement contract (EC) intended to be digitally signed by said DP is provided. Said EC points back to the AC and is intended to comprise, in encrypted form, said data to be provided. Said EC is intended to be signed by said at least one asset C.

METHOD AND SYSTEM FOR PERFORMING DATA TRANSACTIONS IN EXCHANGE FOR ASSETS ON A NETWORK

TECHNICAL FIELD

The invention relates to a method for performing data transactions in exchange for assets on a network according to the preamble of claim 1. The invention also relates to a system for performing data transactions in exchange for assets on a network. The invention in addition relates to a computer program and a computer readable medium.

BACKGROUND ART

Performance of data transactions on a network employing blockchain technology is common for e.g. bitcoin transactions. Performing other types of data transactions in exchange for assets on a network such as a blockchain network is also known. Such a blockchain network may comprise a family of network members having communication and processing means for communicating and processing said data transactions within said blockchain network.

It is also known to use so called smart contracts, i.e. an executable piece of code within the blockchain technology. For example US2017011460 discloses a method for performing transactions of securities based on smart contracts.

Such a smart contract may be utilized in various use cases when exchanging assets on the blockchain. In particular a smart contract can be used to perform atomic swaps, wherein a party X inputs assets to be swapped with assets inputted by party Y. When both parties committed their assets and

digitally signed the smart contract, the atomic swap is performed on the blockchain.

To make atomic swaps between arbitrary data and assets on a blockchain, initiated by the data provider by utilizing a smart contract the asset committer may simply obtain the contract and locally commit the funds and sign it without broadcasting the actions to the network. Thus the data can be obtained without publicly committing any assets.

There is thus a need for facilitating performance of data transactions in exchange for assets on a network.

OBJECTS OF THE INVENTION

An object of the present invention is to provide a method for performing data transactions in exchange for assets on a network which facilitate fair trade.

Another object of the present invention is to provide a system for performing data transactions in exchange for assets on a network which facilitate fair trade.

SUMMARY OF THE INVENTION

These and other objects, apparent from the following description, are achieved by a method, a system, a computer program and a computer readable medium, as set out in the appended independent claims. Preferred embodiments of the method and the system are defined in appended dependent claims.

Specifically an object of the invention is achieved by a method for performing data transactions in exchange for assets on a network. Said network comprises a family of network members having communication and

processing means for communicating and processing said data transactions within said network. The method comprises the step of providing an agreement contract intended to be digitally signed by a network member acting as a data provider, said agreement contract being intended to be digitally signed by at least one other network member acting as an asset committer and to be made available for network members as signed, said agreement contract specifying rules for obtaining data to be provided. The method further comprises the step of, upon signing of said agreement contract by said data provider and said at least one other network member, providing an enforcement contract intended to be digitally signed by said data provider, said enforcement contract pointing back to the previously signed agreement contract and is intended to comprise, in encrypted form, said data to be provided, said enforcement contract being intended to be signed by said at least one asset committer.

Hereby fair trade for performing data transactions in exchange for assets on a network is facilitated in that other network members of the family of network members has seen the agreement contract signed by the network member acting asset committer.

Thus, each network member comprises communication means for communicating data transactions within said network and processing means for processing said data transactions within said network.

According to an embodiment one or more network members may comprise recording means for recording data within said network.

According to an embodiment one or more network member may comprise storing means for storing data within said network.

Each network member may comprise any suitable computer device, server device, processing unit, control unit or the like.

The step of providing an agreement contract digitally signed by a network member acting as a data provider is performed by means for providing an agreement contract. The step of providing an agreement contract comprises the step of generating an agreement contract and digitally signing said generated agreement contract by said data provider.

The method thus comprises the step of making said signed agreement contract available for network members, preferably all network members. According to an embodiment said agreement contract is made available to network members when it has been provided. For a blockchain network said agreement contract is made available to all network members when it has been provided.

According to an embodiment the method comprises the step of determining whether said asset committer has digitally signed said agreement contract. The step of determining whether said asset committer has digitally signed said agreement contract is performed by determining means.

The step of providing an enforcement contract comprises according to an embodiment the step of providing an empty enforcement contract which may be digitally signed by data provider and asset committer and be provided, in encrypted form, with said data to be provided to said asset committer.

The step of providing an enforcement contract comprises the step of generating an enforcement contract and digitally signing said generated enforcement contract. The step of generating an enforcement contract is performed by means of enforcement contract generation means. Said enforcement contract is thus configured to be generated by means of enforcement contract generation means.

The step of providing an enforcement contract is based on information of whether said agreement contract has been digitally signed by said asset committer. The enforcement contract is thus configured to be generated

when said agreement contract has been digitally signed by said asset committer.

Said enforcement contract is configured to point back to the previously signed agreement contract. Said enforcement contract is thus configured to be connected to the previously signed agreement contract.

According to an embodiment the method comprises the step of making said signed enforcement contract available for network members, preferably all network members. According to an embodiment said enforcement contract is made available to network members when it has been provided. For a blockchain network said enforcement contract is made available to all network members when it has been provided.

According to an embodiment the method comprises the steps of: determining by determining means if said enforcement contract has been signed by said at least one asset committer within a predetermined time limit, if said enforcement contract has been signed by said data provider within a predetermined time limit, and if said enforcement contract comprised said data to be provided within a predetermined time limit; and if it is determined that said at least one asset committer and said data provider have signed said enforcement contract and said data was comprised in said enforcement contract said transaction is determined to be completed, and if it is determined that said at least one asset committer has not signed said enforcement contract penalties for said asset committer specified in said rules for obtaining data to be provided are enforced, and if it is determined that said data provider has not signed said enforcement contract and/or said data was not provided penalties for said data provider specified in said rules for obtaining data to be provided are enforced. Hereby efficient control of said transaction is facilitated for securing fair trade and proper compensation/penalty is facilitated if asset committer or data provider does not commit to the signed agreement. According to an embodiment of the method said agreement contract and said enforcement contract pointing back

to said agreement contract constitute a two-phase smart contract constellation. Hereby a kind of efficient electronic handshake of the agreement is facilitated for said fair trade.

According to an embodiment of the method said network is configured as a blockchain network employing blockchain technology. By applying a blockchain network employing blockchain technology for performing said data transactions in exchange for assets by means of said agreement contract and said enforcement contract pointing back to said agreement contract said transactions may be efficiently performed by network members not necessarily trusting each other, the blockchain technology facilitating efficient and reliable control of the time of said transactions.

According to an embodiment of the method the step of providing an enforcement contract is performed automatically. The step of automatically providing an enforcement contract is based on information whether the asset committer has signed the agreement contract. The enforcement contract is thus configured to be automatically generated when said agreement contract has been digitally signed by said asset committer and said data provider.

Specifically an object of the invention is achieved by a system for performing data transactions in exchange for assets on a network. Said network comprises a family of network members having communication and processing means for communicating and processing said data transactions within said network. The system comprises means for providing an agreement contract intended to be digitally signed by a network member acting as a data provider, said agreement contract being intended to be digitally signed by at least one other network member acting as an asset committer and to be made available for network members as signed, said agreement contract specifying rules for obtaining data to be provided. The system further comprises means for providing an enforcement contract intended to be digitally signed by said data provider upon signing of said agreement contract by said data provider and said at least one other network

member, said enforcement contract being arranged to point back to the previously signed agreement contract and is intended to comprise, in encrypted form, said data to be provided, said enforcement contract being intended to be signed by said at least one asset committer.

According to an embodiment the system comprises means for determining if said enforcement contract has been signed by said at least one asset committer within a predetermined time limit, if said enforcement contract has been signed by said data provider within a predetermined time limit, and if said enforcement contract comprised said data to be provided within a predetermined time limit; and means for determining said transaction to be completed if it is determined that said at least one asset committer and said data provider have signed said enforcement contract and said data to be provided was comprised in said enforcement contract, and means for enforcing said enforcement contract penalties for said asset committer specified in said rules for obtaining data to be provided if it is determined that said at least one asset committer has not signed said enforcement contract; and means for enforcing said enforcement contract penalties for said data provider specified in said rules for obtaining data to be provided if it is determined that said data provider has not signed said enforcement contract and/or said data was not provided.

According to an embodiment of the system said agreement contract and said enforcement contract pointing back to said agreement contract constitute a two-phase smart contract constellation.

According to an embodiment of the system said network is configured as a blockchain network employing blockchain technology.

According to an embodiment of the system the means for providing an enforcement contract arranged to be performed automatically.

The system for performing data transactions in exchange for assets on a network is adapted to perform the method as set out herein.

The system according to the invention has the advantages according to the corresponding method.

Specifically an object of the invention is achieved by a computer program for performing data transactions in exchange for assets on a network, said computer program comprising program code which, when run on an electronic control unit or another computer connected to the electronic control unit, causes the electronic control unit to perform methods as set out herein.

Specifically an object of the invention is achieved by computer readable medium comprising instructions which, when executed by a computer, cause the computer to carry out the method as set out herein.

BRIEF DESCRIPTION OF THE DRAWINGS

For a better understanding of the present invention reference is made to the following detailed description when read in conjunction with the accompanying drawings, wherein like reference characters refer to like parts throughout the several views, and in which:

Fig. 1 schematically illustrates a network comprising a family of network members having communication and processing means for communicating and processing data transactions within said network according to an embodiment of the present invention;

Fig. 2 schematically illustrates performance of a data transaction in exchange for assets according to an embodiment of the present invention;

Fig. 3 schematically illustrates a block diagram of a system for performing data transactions in exchange for assets on a network according to an embodiment of the present invention;

Fig. 4 schematically illustrates a block diagram of a method for performing data transactions in exchange for assets on a network according to an embodiment of the present invention; and

Fig. 5 schematically illustrates a computer according to an embodiment of the present invention.

DETAILED DESCRIPTION

Hereinafter the term “link” refers to a communication link which may be a physical connector, such as an optoelectronic communication wire, or a non-physical connector such as a wireless connection, for example a radio or microwave link.

Hereinafter the term “blockchain” refers to a distributed database that maintains a continuously growing list of records referred to as blocks herein. Each block contains a timestamp and a link to a previous block.

A blockchain is a data structure that, together with a defined protocol of rules, enables entities that do not trust each other, to share database, without requiring a central trusted administrator.

Hereinafter the term “data provider” refers to any network member of a network configured to provide data in said network to one or more other network members of said network in which data transactions in exchange for assets are performed.

Hereinafter the term “asset committer” refers to any network member of a network configured to commit to assets in said network from one or more other network members of said network in which data transactions in exchange for assets are performed.

Hereinafter performance of data transactions in exchange for assets on a network may refer to any suitable data transaction and assets may refer to any suitable assets.

The term “data transaction” may refer to a data transaction between different automotive industry manufacturer of commercial vehicles, each automotive industry manufacturer being network members of a network in which data transactions in exchange for assets are performed. Said data transaction may here refer to information from one of the automotive industry manufacturers of e.g. road conditions which may be of value for one or more other automotive industry manufacturer of said network.

Hereinafter the term “enforcement contract penalties” refers to penalties for not fulfilling rules regarding an enforcement contract pointing back to said agreement contract, said rules being specified in said agreement contract. Said rules, specified in said agreement contract, comprises rules for a data provider to sign said enforcement contract within a predetermined time limit, rules for said data provider to include data to be provided in said data transaction within a predetermined time limit and rule, and rules for an asset committer to sign said enforcement contract within a predetermined time limit. Said rules, specified in said agreement contract, further specifies penalties for said data provider if said data provider has not signed said enforcement contract and/or said data was not provided within said specified time limits. Said rules, specified in said agreement contract, further specifies penalties for said asset committer if said asset committer has not signed said enforcement contract within said specified time limits.

Fig. 1 schematically illustrates a network N comprising a family of network members M1, M2, M3, M4 having communication and processing means for communicating and processing data transactions within said network according to an embodiment of the present invention.

Said network N thus comprises a family of network members M1, M2, M3, M4. Each network member M1, M2, M3, M4 comprises communication and processing means for communicating and processing said data transactions within said network. Thus, each network member M1, M2, M3, M4 comprises communication means for communicating data transactions within said network and processing means for processing said data transactions within said network.

According to an embodiment one or more network members M1, M2, M3, M4 may comprise recording means for recording data within said network N.

According to an embodiment one or more network members M1, M2, M3, M4 may comprise storing means for storing data within said network N.

Each network member M1, M2, M3, M4 may comprise any suitable computer device, server device, processing unit, control unit or the like.

One or more network members M1, M2, M3, M4 may comprise a computer in accordance with the computer described with reference to fig. 5.

Said network N is configured as a blockchain network N employing blockchain technology utilizing a blockchain. Each network member M1, M2, M3, M4 comprises a blockchain B1, B2, B3, B4 comprising blocks. Each network member M1, M2, M3, M4 has its own copy of a blockchain B1, B2, B3, B4 of said blockchain network N. Thus, each blockchain B1, B2, B3, B4 are intended to correspond to the other blockchains of said blockchain network N.

In the example in fig. 1 the blockchain network N comprises four network member M1, M2, M3, M4, a first network member M1, a second network member M2, a third network member M3 and a fourth network member M4.

The first network member M1 comprises a first blockchain B1 having blocks B1a, B1b, B1c. The second network member M1 comprises a second blockchain B2 having blocks B2a, B2b, B2c. The third network member M1

comprises a third blockchain B3 having blocks B3a, B3b, B3c. The fourth network member M1 comprises a fourth blockchain B4 having blocks B4a, B4b, B4c.

Each block contains a timestamp and a link to a previous block.

The blockchain network N may also be denoted peer-to-peer network. The blockchain network N comprises according to an embodiment a chronological timestamping server for autonomously managing a blockchain database, i.e. the respective blockchain in the blockchain network.

Each network member M1, M2, M3, M4 of the blockchain network N is linked to each other via links L1, L2, L3, L4, L5, L6 for facilitating communication comprising sharing of data. In a blockchain network the network members are linked, i.e. connected, to each other directly or indirectly. When network members are indirectly linked to each other, communication between these network members is performed via one or more other network members.

The first network member M1 and the second network member M2 are operably connected to each other via a link L1. The first network member M1 and the third network member M3 are operably connected to each other via a link L2. The second network member M2 and the third network member M3 are operably connected to each other via a link L3. The third network member M3 and the fourth network member M4 are operably connected to each other via a link L4. The first network member M1 and the fourth network member M4 are operably connected to each other via a link L5. The second network member M2 and the third network member M3 are operably connected to each other via a link L6.

Fig. 2 schematically illustrates performance of a data transaction in exchange for assets according to an embodiment of the present invention. The data transaction in exchange for assets is configured to be performed on a network such as e.g. a network of the type exemplified in fig. 1.

In a first action T1 an agreement contract AC is arranged to be digitally signed and provided to the network by a network member of said network, the network member acting as a data provider DP. The agreement contract AC is intended to be digitally signed by another network member acting as an asset committer C. In said example utilizing the blockchain network N in fig. 1 the first network member M1 may act as the data provider DP and the fourth network member M4 may act as the asset committer C. According to an embodiment the first action T1 constitutes a transaction.

The agreement contract AC is configured to be made available for network members as signed.

The agreement contract AC is in a second action T2, constituting a transaction, digitally signed by said asset committer C. The agreement contract AC signed by said asset committer C is configured to be made available for network members. In said example utilizing the blockchain network N in fig. 1 the agreement contract AC signed by said asset committer C is made available to second network member M2 and third network member M3 as a proof of said signature by said asset committer C.

Said agreement contract AC signed by said asset committer C specifies rules for obtaining data to be provided.

The action T1 and action T2 illustrates different stages of said agreement contract AC.

In a third action T3, upon signing of said agreement contract AC by said asset committer C and said data provider, an enforcement contract EC is configured to be provided. According to an embodiment said enforcement contract EC is configured to be automatically generated upon signing of said agreement contract AC by said asset committer C in said third action T3. According to an embodiment the third action T3 constitutes a transaction.

Said enforcement contract EC is configured to be pointing back to the previously signed agreement contract AC. Said enforcement contract EC comprises a reference to the previously signed agreement contract AC. Said enforcement contract EC comprises said data to be provided in encrypted form.

In a fourth action T4 said enforcement contract EC is digitally signed by said data provider DP and provided with said data to be provided in encrypted form. Thus, encrypted data to be provided to the asset committer is provided to said enforcement contract EC. According to an embodiment the fourth action T4 constitutes a transaction.

The enforcement contract EC is in a fifth action T5, constituting a transaction, digitally signed by said asset committer C. When said asset committer C has signed said enforcement contract EC said transaction between the data provider and the asset committer is determined to be completed.

All five actions T1-T5 are required in order to complete the transaction, i.e. in order to complete the full trade.

If it is determined that said asset committer C has not signed said enforcement contract EC within a predetermined time limit penalties specified in said rules for obtaining data to be provided are enforced.

If it is determined that said data provider DP has not signed said enforcement contract EC within a predetermined time limit and/or said data to be provided has not been included in the enforcement contract penalties specified in said rules for obtaining data to be provided are enforced.

Each block in a blockchain, e.g. the blockchain B1 in fig. 1, can contain one or more of said actions/transactions T1-T5. According to an embodiment, a single block such as the block B1a in fig. 1, contains all actions T1-T5. According to another embodiment each action T1-T5 is comprised in a separate block in a blockchain.

Fig. 3 schematically illustrates a block diagram of a system I for performing data transactions in exchange for assets on a network according to an embodiment of the present invention.

Said network comprises a family of network members having communication and processing means for communicating and processing said data transactions within said network.

Thus, each network member comprises communication means for communicating data transactions within said network and processing means for processing said data transactions within said network.

According to an embodiment one or more network members comprises recording means for recording data within said network.

According to an embodiment one or more network members comprises storing means for storing data within said network.

Each network member may comprise any suitable computer device, server device, processing unit, control unit or the like.

One or more network members may comprise a computer in accordance with the computer described with reference to fig. 5.

The network may be any suitable network such as e.g. a network of the type exemplified in fig. 1.

The system I comprises means 110 for providing an agreement contract AC intended to be digitally signed by a network member acting as a data provider DP. The means 110 for providing an agreement contract comprises means for generating an agreement contract and means for digitally signing said generated agreement contract by said data provider.

Said agreement contract AC is specifying rules for obtaining data to be provided. Said agreement contract AC comprises data specifying rules for obtaining data to be provided.

Said agreement contract AC is intended to be digitally signed by at least one other network member acting as an asset committer.

The system I comprises means 120 for making said signed agreement contract AC available for network members M1, M2, M3, M4. The means 120 for making said signed agreement contract AC available for network members is preferably arranged to make the agreement contract AC to all network members. According to an embodiment said agreement contract is arranged to be made available to network members when it has been provided. For a blockchain network said agreement contract is made available to all network members when it has been provided.

The system I further comprises means 130 for providing an enforcement contract EC intended to be digitally signed by said data provider upon signing of said agreement contract by said data provider and said at least one other network member. The means 130 for providing an enforcement contract EC comprises means for generating an enforcement contract EC and means for digitally signing said generated enforcement contract EC.

Said enforcement contract EC is arranged to point back to the previously signed agreement contract AC. Said enforcement contract EC is intended to comprise, in encrypted form, said data to be provided. Said enforcement contract is intended to be signed by said at least one asset committer.

According to an embodiment the means 130 for providing an enforcement contract EC comprises means 132 for determining whether said asset committer has digitally signed said agreement contract.

According to an embodiment the means 130 for providing an enforcement contract EC comprises means 134 for determining whether said data provider has digitally signed said agreement contract.

The means 130 for providing an enforcement contract is operably connected to said agreement contract AC via a link. The means 130 for providing an enforcement contract is via said link arranged to receive a signal representing information of whether the agreement contract AC has been signed by both said asset committer and said data provider.

The means 130 for providing an enforcement contract EC is arranged to generate said enforcement contract when said agreement contract AC has been digitally signed by said asset committer. The means 130 for providing an enforcement contract EC is arranged to be performed automatically.

The means 130 for providing an enforcement contract EC is according to an embodiment arranged to provide an empty enforcement contract and means for signing said enforcement contract and means for providing in encrypted form, said data to be provided to said asset committer.

Said enforcement contract EC is arranged to point back to the previously signed agreement contract AC. Said enforcement contract is thus configured to be connected to the previously signed agreement contract.

According to an embodiment the system I comprises means 140 for determining if said enforcement contract EC has been signed by said at least one asset committer within a predetermined time limit, if said enforcement contract has been signed by said data provider within a predetermined time limit, and if said enforcement contract comprised said data to be provided within a predetermined time limit.

The means 140 for determining if said enforcement contract EC has been signed by said at least one asset committer within a predetermined time limit, if said enforcement contract has been signed by said data provider within a

predetermined time limit, and if said enforcement contract comprised said data to be provided within a predetermined time limit is operably connected to said agreement contract AC via a link. Said means 140 is via said link arranged to receive a signal representing information of whether the enforcement contract EC has been signed.

According to an embodiment the system I comprises means 150 for determining said transaction to be completed if it is determined that said at least one asset committer and said data provider have signed said enforcement contract EC and said data was comprised in said enforcement contract. The means 150 for determining said transaction to be completed if it is determined that said at least one asset committer and said data provider have signed said enforcement contract EC and said data was comprised in said enforcement contract is operably connected to said means 140 via a link. The means 150 for determining said transaction to be completed is via said link arranged to receive a signal representing data about said enforcement contract EC having been digitally signed by said asset committer and said data provider and said data having been comprised in said enforcement contract.

The means 150 for determining said transaction to be completed if it is determined that said at least one asset committer and said data provider have signed said enforcement contract EC and said data was comprised in said enforcement contract is arranged to determine said transaction to be completed if said at least one asset committer and said data provider have signed said enforcement contract EC and said data was comprised in said enforcement contract within said predetermined time limits. Said time limits may be the same time limit or different time limits.

According to an embodiment the system I comprises means 160 for enforcing said enforcement contract penalties for said asset committer specified in said rules for obtaining data to be provided if it is determined that said at least one asset committer has not signed said enforcement contract

EC. The means 160 for enforcing said enforcement contract penalties for said asset committer is operably connected to said means 140 via a link. The means 160 for enforcing said enforcement contract penalties for said asset committer is via said link arranged to receive a signal representing data about enforcing said enforcement contract penalties for said asset committer.

According to an embodiment the system I comprises means 170 for enforcing said enforcement contract penalties for said data provider specified in said rules for obtaining data to be provided if it is determined that said data provider has not signed said enforcement contract and/or said data was not provided. Said means 170 is operably connected to said means 140 via a link. Said means 170 is via said link arranged to receive a signal representing data about enforcing said enforcement contract penalties for said data provider.

The system I comprises means 180 for making said enforcement contract EC available for network members M1, M2, M3. The means 180 for making said enforcement contract EC available for network members is preferably arranged to make the enforcement contract EC available to all network members. According to an embodiment said enforcement contract EC is arranged to be made available to network members when it has been provided. For a blockchain network said enforcement contract EC is made available to all network members when it has been provided.

According to an embodiment of the system I said agreement contract AC and said enforcement contract EC pointing back to said agreement contract AC constitute a two-phase smart contract constellation.

According to an embodiment of the system I said network is configured as a blockchain network employing blockchain technology.

Fig. 4 schematically illustrates a block diagram of a method for performing data transactions in exchange for assets on a network according to an embodiment of the present invention.

Said network comprises a family of network members having communication and processing means for communicating and processing said data transactions within said network.

According to the embodiment the method for performing data transactions in exchange for assets on a network comprises a step S1. In this step an agreement contract intended to be digitally signed by a network member acting as a data provider is provided, said agreement contract being intended to be digitally signed by at least one other network member acting as an asset committer and to be made available for network members as signed, said agreement contract specifying rules for obtaining data to be provided.

According to the embodiment the method for performing data transactions in exchange for assets on a network comprises a step S2. In this step, upon signing of said agreement contract by said data provider and said at least one other network member, an enforcement contract intended to be digitally signed by said data provider is provided, said enforcement contract pointing back to the previously signed agreement contract and is intended to comprise, in encrypted form, said data to be provided, said enforcement contract being intended to be signed by said at least one asset committer.

The step of providing an agreement contract digitally signed by a network member acting as a data provider is performed by means for providing an agreement contract. The step of providing an agreement contract comprises the step of generating an agreement contract and digitally signing said generated agreement contract by said data provider.

The method thus comprises the step of making said signed agreement contract available for network members, preferably all network members. According to an embodiment said agreement contract is made available to network members when it has been provided. For a blockchain network said agreement contract is made available to all network members when it has been provided.

According to an embodiment the method comprises the step of determining whether said asset committer has digitally signed said agreement contract. The step of determining whether said asset committer has digitally signed said agreement contract is performed by determining means.

The step of providing an enforcement contract comprises according to an embodiment the step of providing an empty enforcement contract which may be digitally signed by data provider and asset committer and be provided, in encrypted form, with said data to be provided to said asset committer.

The step of providing an enforcement contract comprises the step of generating an enforcement contract and digitally signing said generated enforcement contract. The step of generating an enforcement contract is performed by means of enforcement contract generation means. Said enforcement contract is thus configured to be generated by means of enforcement contract generation means.

The step of providing an enforcement contract is based on information of whether said agreement contract has been digitally signed by said asset committer. The enforcement contract is thus configured to be generated when said agreement contract has been digitally signed by said asset committer.

Said enforcement contract is configured to point back to the previously signed agreement contract. Said enforcement contract is thus configured to be connected to the previously signed agreement contract.

According to an embodiment the method comprises the step of making said signed enforcement contract available for network members, preferably all network members. According to an embodiment said enforcement contract is made available to network members when it has been provided. For a blockchain network said enforcement contract is made available to all network members when it has been provided.

According to an embodiment the method comprises the steps of: determining by determining means if said enforcement contract has been signed by said at least one asset committer within a predetermined time limit, if said enforcement contract has been signed by said data provider within a predetermined time limit, and if said enforcement contract comprised said data to be provided within a predetermined time limit; and if it is determined that said at least one asset committer and said data provider have signed said enforcement contract and said data was comprised in said enforcement contract said transaction is determined to be completed, and if it is determined that said at least one asset committer has not signed said enforcement contract penalties for said asset committer specified in said rules for obtaining data to be provided are enforced, and if it is determined that said data provider has not signed said enforcement contract and/or said data was not provided penalties for said data provider specified in said rules for obtaining data to be provided are enforced. According to an embodiment of the method said agreement contract and said enforcement contract pointing back to said agreement contract constitute a two-phase smart contract constellation.

According to an embodiment of the method said network is configured as a blockchain network employing blockchain technology.

According to an embodiment of the method the step of providing an enforcement contract is performed automatically. The step of automatically providing an enforcement contract is based on information whether the asset committer has signed the agreement contract. The enforcement contract is thus configured to be automatically generated when said agreement contract has been digitally signed by said asset committer and said data provider. With reference to figure 4, a diagram of an apparatus 500 is shown. Apparatus 500 comprises a non-volatile memory 520, a data processing device 510 and a read/write memory 550. Non-volatile memory 520 has a first memory portion 530 wherein a computer program, such as an operating

system, is stored for controlling the function of apparatus 500. Further, apparatus 500 comprises a bus controller, a serial communication port, I/O-means, an A/D-converter, a time date entry and transmission unit, an event counter and an interrupt controller (not shown). Non-volatile memory 520 also has a second memory portion 540.

A computer program P is provided comprising routines for performing data transactions in exchange for assets on a network. Said network comprises a family of network members having communication and processing means for communicating and processing said data transactions within said network. The program P comprises routines for providing an agreement contract intended to be digitally signed by a network member acting as a data provider, said agreement contract being intended to be digitally signed by at least one other network member acting as an asset committer and to be made available for network members as signed, said agreement contract specifying rules for obtaining data to be provided. The program P comprises routines for, upon signing of said agreement contract by said data provider and said at least one other network member, providing an enforcement contract intended to be digitally signed by said data provider, said enforcement contract pointing back to the previously signed agreement contract and is intended to comprise, in encrypted form, said data to be provided, said enforcement contract being intended to be signed by said at least one asset committer. The program P comprises routines for determining by determining means if said enforcement contract has been signed by said at least one asset committer within a predetermined time limit, if said enforcement contract has been signed by said data provider within a predetermined time limit, and if said enforcement contract comprised said data to be provided within a predetermined time limit. The program P comprises routines for determining that said transaction is completed if it is determined that said at least one asset committer and said data provider have signed said enforcement contract and said data was comprised in said enforcement contract. The program P comprises routines for enforcing

penalties for said asset committer specified in said rules for obtaining data to be provided if it is determined that said at least one asset committer has not signed said enforcement contract. The program P comprises routines for enforcing penalties for said data provider specified in said rules for obtaining data to be provided are enforced if it is determined that said data provider has not signed said enforcement contract and/or said data was not provided. The computer program P may be stored in an executable manner or in a compressed condition in a separate memory 560 and/or in read/write memory 550.

When it is stated that data processing device 510 performs a certain function it should be understood that data processing device 510 performs a certain part of the program which is stored in separate memory 560, or a certain part of the program which is stored in read/write memory 550.

Data processing device 510 may communicate with a data communications port 599 by means of a data bus 516. Non-volatile memory 520 is adapted for communication with data processing device 510 via a data bus 513. Separate memory 560 is adapted for communication with data processing device 510 via a data bus 511. Read/write memory 550 is adapted for communication with data processing device 510 via a data bus 515. To the data communications port 599 e.g. the links connected to the control units 100 may be connected.

When data is received on data port 599 it is temporarily stored in second memory portion 540. When the received input data has been temporarily stored, data processing device 510 is set up to perform execution of code in a manner described above. The signals received on data port 599 can be used by apparatus 500 providing an agreement contract intended to be digitally signed by a network member acting as a data provider, said agreement contract being intended to be digitally signed by at least one other network member acting as an asset committer and to be made available for network members as signed, said agreement contract specifying rules for

obtaining data to be provided. The signals received on data port 599 can be used by apparatus 500 for, upon signing of said agreement contract by said data provider and said at least one other network member, providing an enforcement contract intended to be digitally signed by said data provider, said enforcement contract pointing back to the previously signed agreement contract and is intended to comprise, in encrypted form, said data to be provided, said enforcement contract being intended to be signed by said at least one asset committer. The signals received on data port 599 can be used by apparatus 500 for determining by determining means if said enforcement contract has been signed by said at least one asset committer within a predetermined time limit, if said enforcement contract has been signed by said data provider within a predetermined time limit, and if said enforcement contract comprised said data to be provided within a predetermined time limit. The signals received on data port 599 can be used by apparatus 500 for determining that said transaction is completed if it is determined that said at least one asset committer and said data provider have signed said enforcement contract and said data was comprised in said enforcement contract. The signals received on data port 599 can be used by apparatus 500 for enforcing penalties for said asset committer specified in said rules for obtaining data to be provided if it is determined that said at least one asset committer has not signed said enforcement contract. The signals received on data port 599 can be used by apparatus 500 for enforcing penalties for said data provider specified in said rules for obtaining data to be provided if it is determined that said data provider has not signed said enforcement contract and/or said data was not provided.

Parts of the methods described herein can be performed by apparatus 500 by means of data processing device 510 running the program stored in separate memory 560 or read/write memory 550. When apparatus 500 runs the program, parts of the methods described herein are executed.

The foregoing description of the preferred embodiments of the present invention has been provided for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Obviously, many modifications and variations will be apparent to practitioners skilled in the art. The embodiments were chosen and described in order to best explain the principles of the invention and its practical applications, thereby enabling others skilled in the art to understand the invention for various embodiments and with the various modifications as are suited to the particular use contemplated.

CLAIMS

1. A computerized method for performing data transactions in exchange for assets on a network (N), said network comprising a family of network members (M1, M2, M3, M4) having communication and processing means for communicating and processing said data transactions within said network (N), **characterized by** the steps of: providing (S1) an agreement contract (AC) intended to be digitally signed by a network member acting as a data provider (DP), said agreement contract (AC) being intended to be digitally signed by at least one other network member acting as an asset committer (C) and to be made available for network members (M1, M2, M3, M4) as signed, said agreement contract (AC) specifying rules for obtaining data to be provided; and upon signing of said agreement contract (AC) by said data provider and said at least one other network member automatically generating and providing (S2) an enforcement contract (EC) intended to be digitally signed by said data provider (DP), said enforcement contract (EC) pointing back to the previously signed agreement contract (AC) and is intended to comprise, in encrypted form, said data to be provided, said enforcement contract (EC) being intended to be signed by said at least one asset committer (C).

2. A method according to claim 1, comprising the steps of: determining by determining means if said enforcement contract (EC) has been signed by said at least one asset committer (C) within a predetermined time limit, if said enforcement contract (EC) has been signed by said data provider (DP) within a predetermined time limit, and if said enforcement contract (EC) comprised said data to be provided within a predetermined time limit; and if it is determined that said at least one asset committer and said data provider have signed said enforcement contract (EC) and said data was comprised in said enforcement contract said transaction is determined to be completed, and if it is determined that said at least one asset committer (C) has not signed said enforcement contract (EC) penalties for said asset committer specified in said rules for obtaining data to be provided are enforced, and if it is determined that

said data provider (DP) has not signed said enforcement contract (EC) and/or said data was not provided penalties for said data provider specified in said rules for obtaining data to be provided are enforced.

3. A method according to claim 1 or 2, wherein said agreement contract (AC) and said enforcement contract (EC) pointing back to said agreement contract (AC) constitute a two-phase smart contract constellation.

4. A method according any of claims 1-3, wherein said network (N) is configured as a blockchain network employing blockchain technology.

5. A system for performing data transactions in exchange for assets on a network (N), said network comprising a family of network members (M1, M2, M3, M4) having communication and processing means for communicating and processing said data transactions within said network, **characterized by** means (110) for providing an agreement contract (AC) intended to be digitally signed by a network member acting as a data provider, said agreement contract (AC) being intended to be digitally signed by at least one other network member acting as an asset committer (C) and to be made available for network members as signed, said agreement contract (AC) specifying rules for obtaining data to be provided; and means (130) for automatically generating and providing an enforcement contract (EC) intended to be digitally signed by said data provider upon signing of said agreement contract (AC) by said data provider and said at least one other network member, said enforcement contract (EC) being arranged to point back to the previously signed agreement contract (AC) and is intended to comprise, in encrypted form, said data to be provided, said enforcement contract (EC) being intended to be signed by said at least one asset committer (C) to complete said transaction.

6. A system according to claim 5, comprising means (140) for determining if said enforcement contract (EC) has been signed by said at least one asset committer (C) within a predetermined time limit, if said enforcement contract

(EC) has been signed by said data provider (DP) within a predetermined time limit, and if said enforcement contract (EC) comprised said data to be provided within a predetermined time limit; and means (150) for determining said transaction to be completed if it is determined that said at least one asset committer (C) and said data provider have signed said enforcement contract and said data was comprised in said enforcement contract, and means (160) for enforcing said enforcement contract penalties for said asset committer specified in said rules for obtaining data to be provided if it is determined that said at least one asset committer (C) has not signed said enforcement contract (EC), and means (170) for enforcing said enforcement contract penalties for said data provider specified in said rules for obtaining data to be provided if it is determined that said data provider (DP) has not signed said enforcement contract (EC) and/or said data was not provided.

7. A system according to claim 5 or 6, wherein said agreement contract (AC) and said enforcement contract (EC) pointing back to said agreement contract (AC) constitute a two-phase smart contract constellation.

8. A system according any of claims 5-7, wherein said network is configured as a blockchain network employing blockchain technology.

9. A computer program (P) for performing data transactions in exchange for assets on a network, said computer program (P) comprising program code which, when run on an electronic control unit or another computer (500) connected to the electronic control unit, causes the electronic control unit to perform the steps according to claim 1-4.

10. A computer readable medium comprising instructions which, when executed by a computer, cause the computer to carry out the system according to anyone of claim 1-4.

I följande bilaga finns en översättning av patentkraven till svenska. Observera att det är patentkravens lydelse på engelska som gäller.

A Swedish translation of the patent claims is enclosed. Please note that only the English claims have legal effect.

PATENTKRAV

1. Datoriserat förfarande för utförande av datatransaktioner i utbyte mot tillgångar i ett nätverk (N), varvid nämnda nätverk omfattar en familj av nätverksmedlemmar (M1, M2, M3, M4) med kommunikations- och bearbetningsmedel för kommunikation och behandling av nämnda datatransaktioner inom nämnda nätverk (N), **kännetecknat av** stegen att: tillhandahålla (S1) ett avtalskontrakt (AC) avsett att undertecknas digitalt av en nätverksmedlem som agerar som dataleverantör (DP), varvid nämnda avtalskontrakt (AC) är avsett att undertecknas digitalt av minst en annan nätverksmedlem som agerar som tillgångsleverantör (C) samt att göras tillgängligt för nätverksmedlemmar (M1, M2, M3, M4) i undertecknat skick, varvid nämnda avtalskontrakt (AC) specificerar regler för erhållande av data som ska tillhandahållas; och efter undertecknandet av nämnda avtalskontrakt (AC) av nämnda dataleverantör och nämnda minst ena andra nätverksmedlem automatiskt generera och tillhandahålla (S2) ett verkställighetskontrakt (EC) avsett att undertecknas digitalt av nämnda dataleverantör (DP), varvid nämnda verkställighetskontrakt (EC) hänvisar tillbaka till det tidigare undertecknade avtalskontraktet (AC) och är avsett att omfatta, i krypterad form, nämnda data som ska tillhandahållas, varvid nämnda verkställighetskontrakt (EC) är avsett att undertecknas av nämnda minst ena tillgångsleverantör (C).

2. Förfarande enligt krav 1, omfattande stegen att: fastställa medelst fastställelsemedel huruvida nämnda verkställighetskontrakt (EC) har undertecknats av nämnda minst ena tillgångsleverantör (C) inom en förutbestämd tidsbegränsning, huruvida nämnda verkställighetskontrakt (EC) har undertecknats av nämnda dataleverantör (DP) inom en förutbestämd tidsbegränsning och huruvida nämnda verkställighetskontrakt (EC) omfattade nämnda data som ska tillhandahållas inom en förutbestämd tidsbegränsning; och, om det fastställs att nämnda minst ena tillgångsleverantör och nämnda dataleverantör har undertecknat nämnda verkställighetskontrakt (EC) och nämnda data omfattades i nämnda verkställighetskontrakt, nämnda

transaktion fastställs som genomförd, och, om det fastställs att nämnda minst ena tillgångsleverantör (C) inte har undertecknat nämnda verkställighetskontrakts (EC), straff för nämnda tillgångsleverantör som specificeras i nämnda regler för erhållande av data som ska tillhandahållas verkställs, och, om det fastställs att nämnda dataleverantör (DP) inte har undertecknat nämnda verkställighetskontrakt (EC) och/eller nämnda data inte tillhandahölls, straff för nämnda dataleverantör som specificeras i nämnda regler för erhållande av data som ska tillhandahållas verkställs.

3. Förfarande enligt krav 1 eller 2, varvid nämnda avtalskontrakt (AC) och nämnda verkställighetskontrakt (EC) som hänvisar tillbaka till nämnda avtalsavtal (AC) utgör en tvåfasig smart kontraktkonstellation.

4. Förfarande enligt något av kraven 1-3, varvid nämnda nätverk (N) är konfigurerat som ett blockkedjenätverk användande blockkedjeteknik.

5. System för utförande av datatransaktioner i utbyte mot tillgångar i ett nätverk (N), varvid nämnda nätverk omfattar en familj av nätverksmedlemmar (M1, M2, M3, M4) med kommunikations- och bearbetningsmedel för kommunikation och behandling av nämnda datatransaktioner inom nämnda nätverk, **kännetecknat av** medel (110) för tillhandahållande av ett avtalskontrakt (AC) avsett att undertecknas digitalt av en nätverksmedlem som agerar som dataleverantör, varvid nämnda avtalskontrakt (AC) är avsett att undertecknas digitalt av minst en annan nätverksmedlem som agerar som tillgångsleverantör (C) samt att göras tillgängligt för nätverksmedlemmar i undertecknat skick, varvid nämnda avtalskontrakt (AC) specificerar regler för erhållande av data som ska tillhandahållas; och medel (130) för automatisk generering och tillhandahållande av ett verkställighetskontrakt (EC) avsett att undertecknas digitalt av nämnda dataleverantör efter undertecknandet av nämnda avtalskontrakt (AC) av nämnda dataleverantör och nämnda minst ena andra nätverksmedlem, varvid nämnda verkställighetskontrakt (EC) är anordnat för att hänvisa tillbaka till det tidigare undertecknade avtalskontraktet (AC) och är avsett att omfatta, i krypterad form, nämnda data som ska

tillhandahållas, varvid nämnda verkställighetskontrakt (EC) är avsett att undertecknas av nämnda minst ena tillgångsleverantör (C) för att genomföra nämnda transaktion.

6. System enligt krav 5, omfattande medel (140) för fastställande av huruvida nämnda verkställighetskontrakt (EC) har undertecknats av nämnda minst ena tillgångsleverantör (C) inom en förutbestämd tidsbegränsning, huruvida nämnda verkställighetskontrakt (EC) har undertecknats av nämnda dataleverantör (DP) inom en förutbestämd tidsbegränsning och huruvida nämnda verkställighetskontrakt (EC) omfattade nämnda data som ska tillhandahållas inom en förutbestämd tidsbegränsning; och medel (150) för fastställande av nämnda transaktion som ska genomföras om det fastställs att nämnda minst ena tillgångsleverantör (C) och nämnda dataleverantör har undertecknat nämnda verkställighetskontrakt och nämnda data omfattades i nämnda verkställighetskontrakt, och medel (160) för verkställande av nämnda verkställighetskontrakts straff för nämnda tillgångsleverantör som specificeras i nämnda regler för erhållande av data som ska tillhandahållas om det fastställs att nämnda minst ena tillgångsleverantör (C) inte har undertecknat nämnda verkställighetskontrakt (EC), och medel (170) för verkställande av nämnda verkställighetskontrakts straff för nämnda dataleverantör som specificeras i nämnda regler för erhållande av data som ska tillhandahållas och om det fastställs att nämnda dataleverantör (DP) inte har undertecknat nämnda verkställighetskontrakt (EC) och/eller nämnda data inte tillhandahölls.

7. System enligt krav 5 eller 6, varvid nämnda avtalskontrakt (AC) och nämnda verkställighetskontrakt (EC) som hänvisar tillbaka till nämnda avtalsavtal (AC) utgör en tvåfasig smart kontraktkonstellation.

8. System enligt något av kraven 5-7, varvid nämnda nätverk är konfigurerat som ett blockkedjenätverk användande blockkedjeteknik.

9. Datorprogram (P) för utförande av datatransaktioner i utbyte mot tillgångar på ett nätverk, varvid nämnda datorprogram (P) omfattar programkod som, när

den körs på en elektronisk styrenhet eller en annan dator (500) ansluten till den elektroniska styrenheten, bringar den elektroniska styrenheten att utföra stegen enligt krav 1-4.

10. Datorläsbart medium omfattande instruktioner som, när de exekveras av en dator, bringar datorn att utföra systemet enligt något av kraven 1-4.

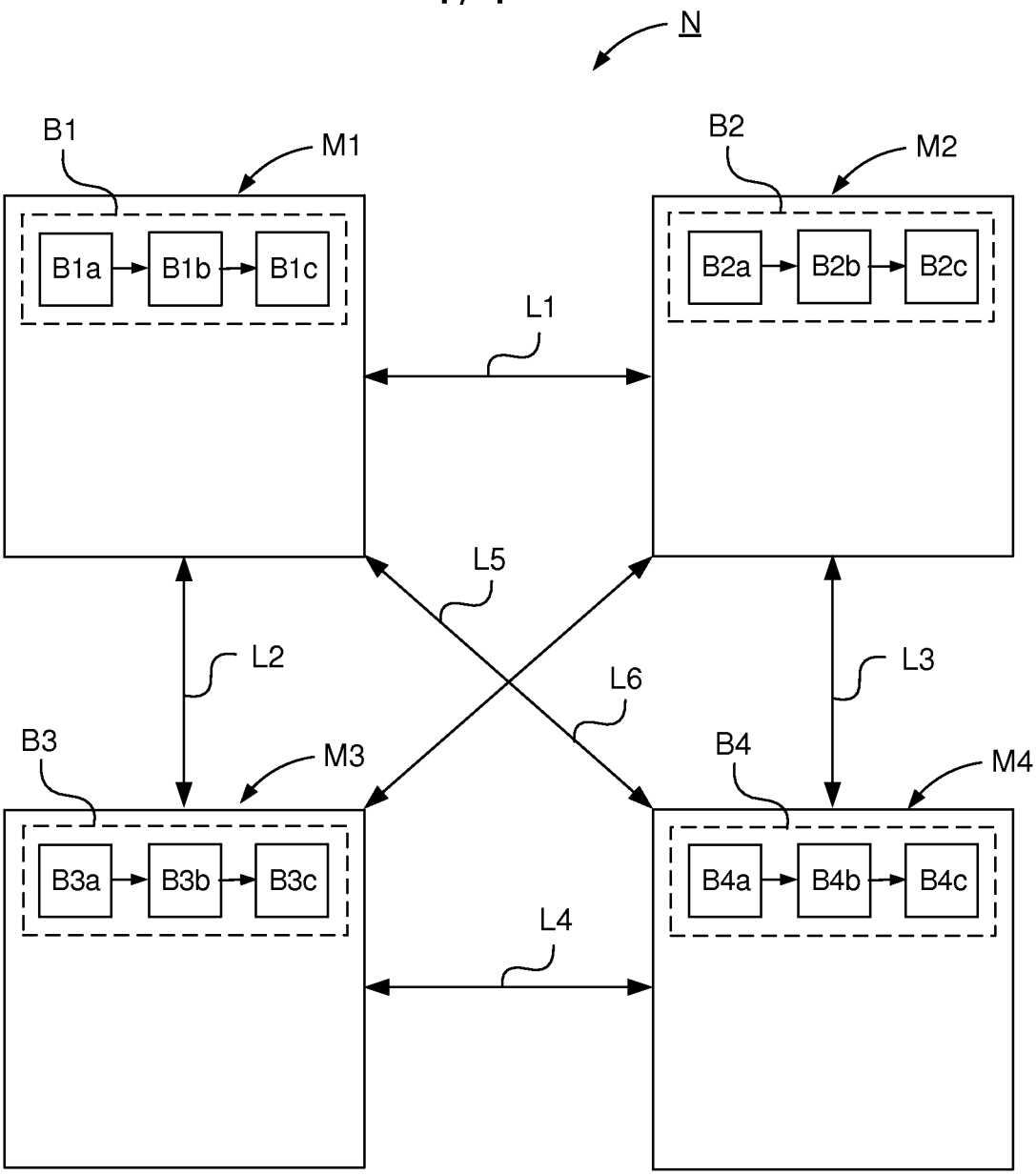

N
B1
M1
B2
M2
B1a
B1b
B1c
B2a
B2b
B2c
L1
L5
L2
L3
L6
B3
M3
B4
M4
B3a
B3b
B3c
B4a
B4b
B4c
L4

Fig. 1

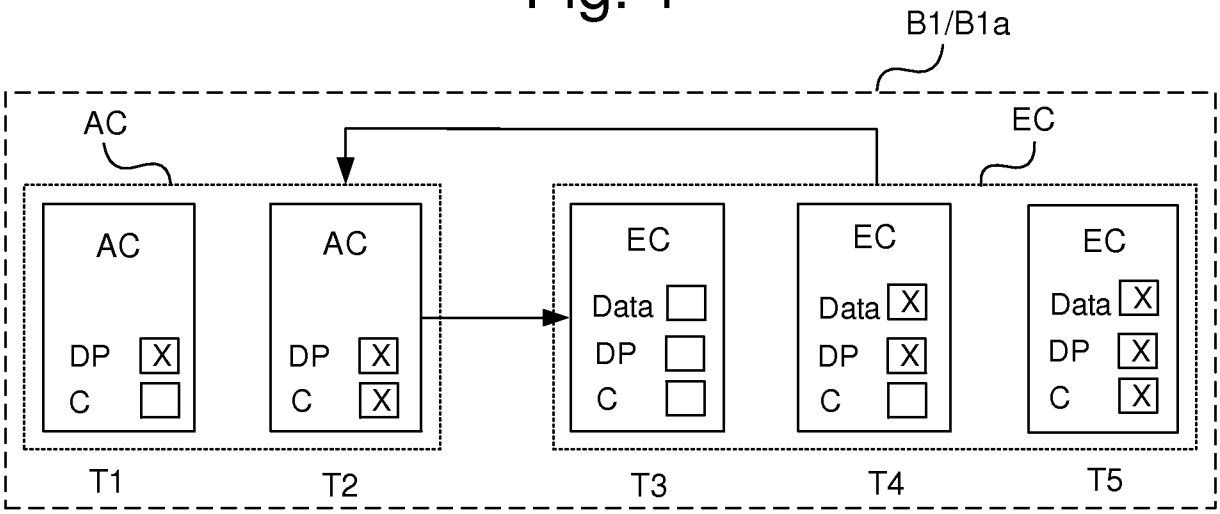

B1/B1a
AC
EC
AC
DP X
C
AC
DP X
C X
EC
Data
DP
C
EC
Data X
DP X
C
EC
Data X
DP X
C X
T1
T2
T3
T4
T5

Fig. 2

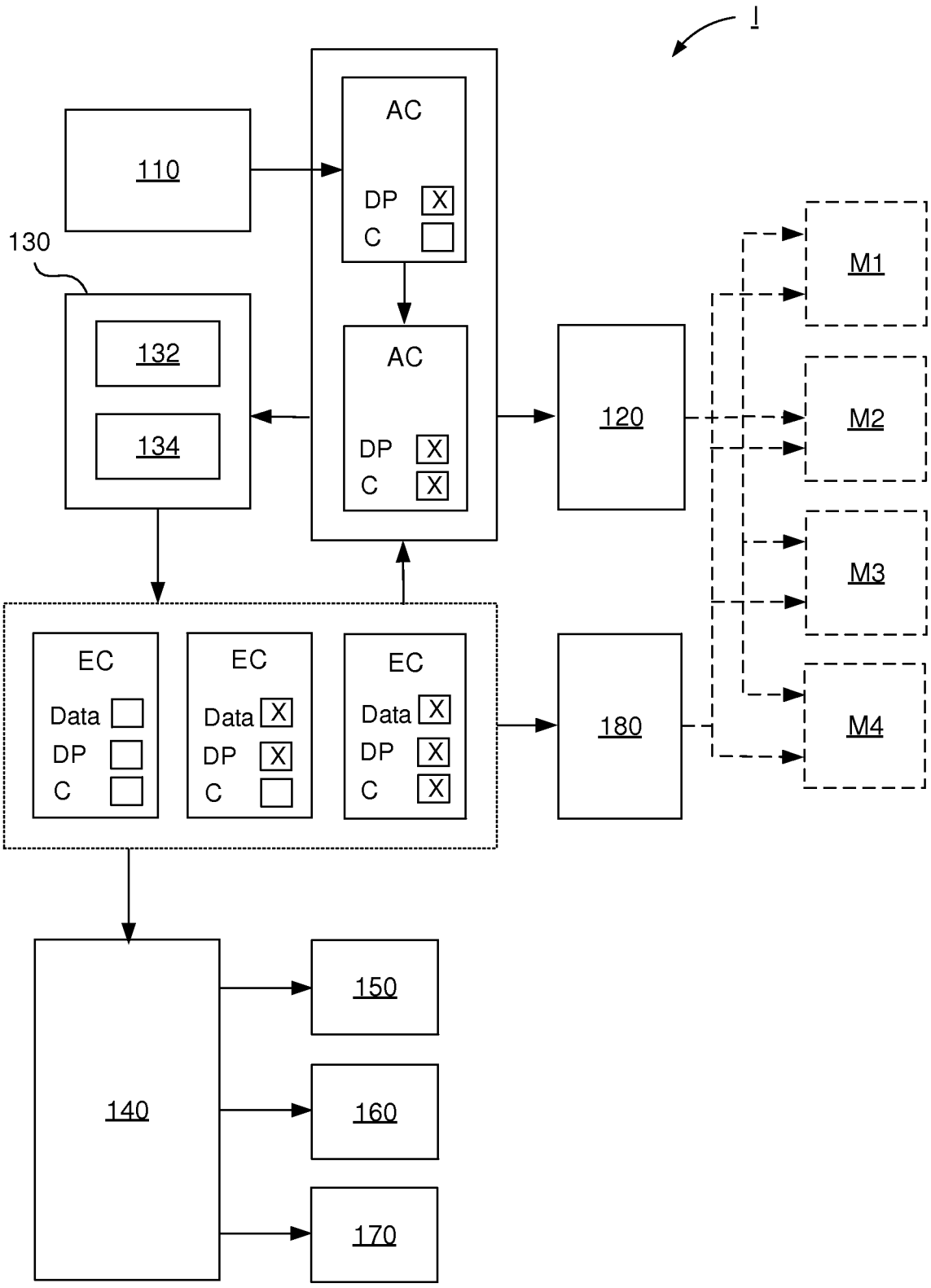

1
110
AC
DP X
C
130
132
134
AC
DP X
C X
120
M1
M2
M3
M4
EC
Data
DP
C
EC
Data X
DP X
C
EC
Data X
DP X
C X
180
140
150
160
170

Fig. 3

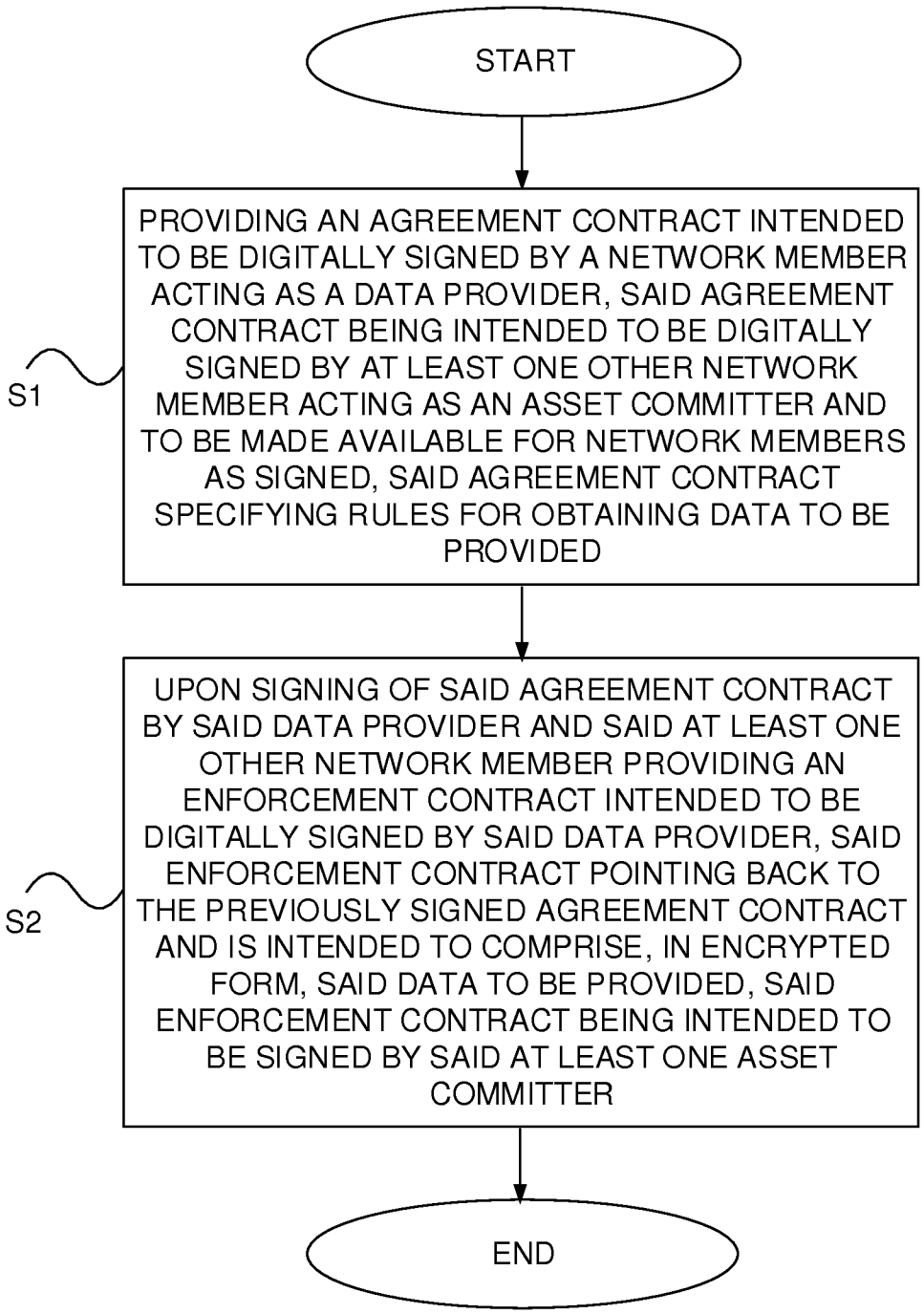

START
PROVIDING AN AGREEMENT CONTRACT INTENDED TO BE DIGITALLY SIGNED BY A NETWORK MEMBER ACTING AS A DATA PROVIDER, SAID AGREEMENT CONTRACT BEING INTENDED TO BE DIGITALLY SIGNED BY AT LEAST ONE OTHER NETWORK MEMBER ACTING AS AN ASSET COMMITTER AND TO BE MADE AVAILABLE FOR NETWORK MEMBERS AS SIGNED, SAID AGREEMENT CONTRACT SPECIFYING RULES FOR OBTAINING DATA TO BE PROVIDED
S1
UPON SIGNING OF SAID AGREEMENT CONTRACT BY SAID DATA PROVIDER AND SAID AT LEAST ONE OTHER NETWORK MEMBER PROVIDING AN ENFORCEMENT CONTRACT INTENDED TO BE DIGITALLY SIGNED BY SAID DATA PROVIDER, SAID ENFORCEMENT CONTRACT POINTING BACK TO THE PREVIOUSLY SIGNED AGREEMENT CONTRACT AND IS INTENDED TO COMPRISE, IN ENCRYPTED FORM, SAID DATA TO BE PROVIDED, SAID ENFORCEMENT CONTRACT BEING INTENDED TO BE SIGNED BY SAID AT LEAST ONE ASSET COMMITTER
S2
END

Fig. 4

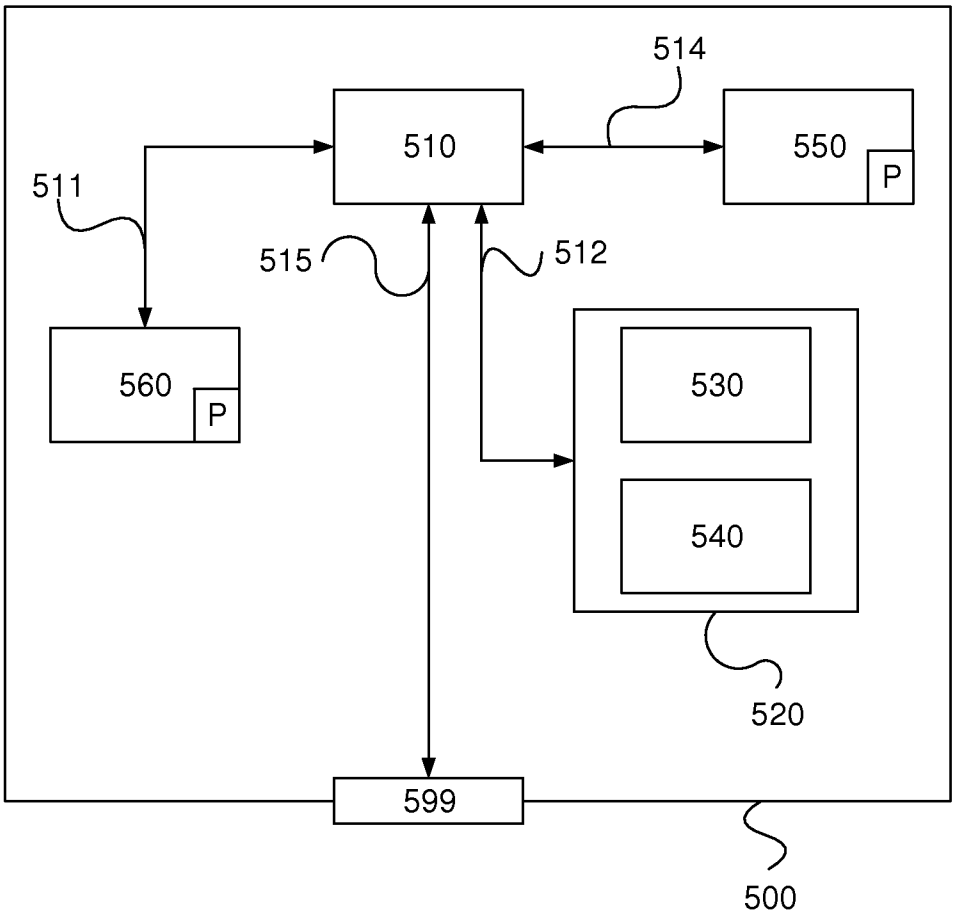


Fig. 5