SYSTEM AND METHOD FOR DIGITAL TRANSACTION

TECHNICAL FIELD

The present invention generally relates to the field of digital transaction, and particularly to a system, a method, and a machine readable device comprising a non-transitory machine-readable storage medium having machine-readable instructions stored thereon, the machine-readable instructions being executable by computing hardware, for transaction of digital data (e.g., bitcoin, digital currency, virtual currency, electronic money, cryptocurrency, or the like), addressing both security and speed issues.

BACKGROUND

Conventional architectures and processes in the field of digital transaction account individually for security or speed, but do not meet requirements of both security and speed.

Existing centralized systems (for example, a central bank that has a single control of financial-related activities) are popular in terms of security since each of these systems is constantly being monitored by a corresponding authority. However, manual or complicated processes performed on these system architectures compromise systems' speed, and hence delay execution of the activities.

On the other hand, existing decentralized systems or peer-to-peer networks rely on a host of computers to complete a specific activity on each system or network. An example of this is the Bitcoin system (which uses "bitcoin" as digital currency, virtual currency, electronic money, or cryptocurrency) that requires computer servers operable to validate financial transactions, in order to record a copy of the transaction to a

common ledger which broadcasts or allows access of data to all the computer servers. In other words, these systems do not require a single authority to manage or control data. These system architectures are at risk of thefts, attacks, or malwares capable of performing unauthorized transactions. These architectures, though relatively speedier compared to the existing centralized platforms, still need improvements in terms of security.

US9967238B1 teaches computer network systems and computer-implemented methods for cryptographically-secured distributed data management that place a focus on security.

US 20170344979 A1 as well disclosed a method and system for processing payment during an electronic commerce transaction.

To date, conventional architectures and processes, e.g., prior inventions as above regarding the existing centralized and decentralized systems continue to suffer from this trade-off between speed and security. For other systems or processes for digital transaction that are built to have unwavering security, the speed thereof is compromised. Alternatively, in systems or processes of digital transaction designed for speed, securities thereof are susceptible to unauthorized third parties.

BRIEF SUMMARY

The present invention provides a solution to the above trade-off issues of the conventional architectures and processes. More specifically, the present invention provides systems and methods and a machine readable device comprising a non-transitory machine-readable storage medium having machine-readable instructions stored thereon, the machine-readable instructions being executable by computing hardware, having the technical advantage of having security and speed at the same time.

According to an embodiment of the present invention, a system for digital transaction is provided, comprising at least one external data storage device for storing digital data of at least one user; a digital data storage application for a machine-readable device for transferring the digital data; and a queue book for arranging at least one smart contract or for verification or filtering of the at least one smart contract for at least one original blockchain for a peer-to-peer transaction; wherein the system further comprises: a digital data storage for receiving the digital data; a trade exchange connected to the digital data storage; the at least one smart contract from the trade exchange; and a plurality of proxies comprising proxy digital data, and wherein the proxy digital data are reusable. The proxy digital data can be used again for other proxy trade orders, even when a trade execution has not been completed. The transacted proxy digital data through at least one proxy blockchain can be reused immediately for other proxy trade orders.

In some embodiments of the present invention, the system comprises a plurality of proxies having a proxy digital data storage for duplicating the digital data from the digital data storage; a proxy order book for receiving a plurality of proxy trade orders from the trade exchange; a proxy matching system for matching the plurality of proxy trade orders; at least one proxy smart contract created from matching the plurality of proxy trade orders; and at least one proxy blockchain for verification of the at least one smart contract or for verification of the at least one proxy smart contract for proxy peer-to-peer transaction. These embodiments offer an advantage in that the time of transaction of digital data of trades can be significantly reduced, for example, being reduced from 10 minutes (i.e., at the speed of the existing platforms), to 10 seconds for the digital data (e.g., bitcoin, digital currency, virtual currency, electronic money, cryptocurrency, or the like) trade at the speed of some embodiments of the present invention.

In some embodiments of the present invention, the proxy digital data storage is connected to the digital data storage; or the proxy digital data storage and the digital data storage are linked to the digital data storage application. This provides security to the digital data.

In some embodiments of the present invention, the trade exchange comprises a plurality of trade orders having digital data, wherein the trade exchange is connected to an order book for receiving the plurality of trade orders, and to a matching system for matching the plurality of trade orders.

In some embodiments of the present invention, the digital data storage application includes a first security means; or the trade exchange comprises a second security means for initiating the plurality of trade orders.

In some embodiments of the present invention, the system comprises both centralized and decentralized digital data exchange parts. The centralized part comprises an order book, or a matching system. These can achieve increased speed of transaction of trades, as compared to trades of a conventional blockchain. The decentralized part comprises the at least one original blockchain, or the at least one proxy blockchain.

In another embodiment of the present invention, a method for digital transaction provides faster and more secure digital transactions. The method comprises steps of: depositing of digital data by at least one user to at least one external data storage device; transferring of the digital data to a digital data storage application by a first security means; receiving the digital data by a digital data storage; mirroring of the digital data from the digital data storage to a proxy digital data storage; initiating plurality of trade orders by a second security means to the digital data storage application; placing and matching the plurality of trade orders in a trade exchange; creating at least one smart contract from the plurality of trade orders which are

match; verifying of the at least one smart contract by at least one proxy blockchain; triggering a proxy trade execution by the at least one smart contract created from the trade exchange; arranging the at least one smart contract in a queue book; verifying, by the queue book, of the at least one smart contract in at least one original blockchain; performing a trade execution upon completion of the proxy trade execution; or transferring or exchanging of digital data to the digital data storage.

In some embodiments of the present invention, the step of above mentioned method for placing and matching the plurality of trade orders in a trade exchange, may comprise algorithmically matching the plurality of trade orders in an order book connected to the trade exchange.

BRIEF DESCRIPTION OF DRAWINGS

Fig. 1 illustrates a high-level system architecture addressing security and speed requirements in accordance to an embodiment of the present invention.

Fig. 2 illustrates a hybrid system in accordance to an embodiment of the present invention.

Fig. 3 illustrates an example of comparison of trade transaction in given time frame (t), between an embodiment of the present invention and a conventional blockchain.

Fig. 4 illustrates a system architecture of an exchange in accordance to an embodiment of the present invention.

Fig. 5 is a flow of a method for transaction in accordance to an embodiment of the present invention.

Fig. 6 illustrates a plurality of proxies coupled to a plurality of trade orders from the trade exchange in accordance to an embodiment of the present invention.

DETAILED DESCRIPTION

Embodiments of the present invention shall now be described in-depth and with greater detail.

Throughout the specification, the term "according to an embodiment", "in accordance to an embodiment", "in some embodiments", or "another embodiment" as used herein, should not be necessarily construed as limiting, as it may or may not refer to same embodiment(s).

It is noted that the figures are made for the purpose of illustration only as an aid to understanding, and not necessarily to scale the principles of the present invention. Additionally, it is noteworthy that structural and functional details shown or described herein must not be interpreted as limiting, but simply as an aid for a person skilled in the art to diversely exert the present invention.

Referring to Fig. 1, a high-level system architecture addressing security and speed requirements according to an embodiment of the present invention is shown. In an embodiment, there is provided a system **100** for digital transaction, the system **100** comprising at least one external data storage device **2** for storing digital data of at least one user; a digital data storage application **1a** for a machine-readable device **1** for transferring the digital data; a queue book **10** for arranging at least one smart contract **7** or for verification or filtering of the at least one smart contract **7** for at least one original blockchain **11** for a peer-to-peer transaction **12**; wherein the system further comprises: a digital data storage **3** for receiving the digital data; a trade exchange **5** connected to the digital data storage **3**; the at least

one smart contract **7** from the trade exchange **5**; or a plurality of proxies **120** comprising proxy digital data, and wherein the proxy digital data are reusable. As a result, multiple proxy trade orders are allowed to be transacted within a timeframe of one transaction. Additionally, the proxy digital data are securely encrypted, in such a manner that it is difficult to be decrypted. Therefore, the present invention is advantageous in terms of both speed and security.

In some embodiments of the present invention, the digital data storage application **1**, at step 101, requires that the at least one user provides a first security means **1b** in order to facilitate transfer of the digital data from the at least one external data storage device **2**. The at least one user can, at step 102, deposit digital data from the at least one external data storage device **2** into their own digital data storage **3** through digital data storage application **1**. The digital data are converted at step 103, by mirroring or duplication, from the digital data storage **3** to the proxy digital data storage **4** in a back-end (not shown) to ensure processing compatibility with the at least one blockchain 8. Moreover, at step 104, a security means **5b** is applied to the digital data storage application **1** for initiating the plurality of trade orders **5a**. At step 105, the at least one user places the plurality of trade orders **5a** respectively in the trade exchange **5**. The plurality of trade orders **5a** is received by an order book **6**, and at step 106 being matched by a matching system **6a**. In some embodiments, the matching system **6a** can be an algorithm-based matching system. The plurality of trade orders **5a** that is matched, at step 107 creates the at least one smart contract **7**, and at step 108 the at least one blockchain **8** verifies the at least one smart contract **7**. At step 109a, a proxy trade execution is triggered by the at least one smart contract **7**. The plurality of proxies **120** facilitates the proxy trade execution. This is advantageous in that the time of transaction of digital data of trades can be significantly reduced, for example, being reduced from 10 minutes (at the speed of existing platforms), down to 10 seconds (at the speed of the system of some embodiments of

the present invention. Additionally, this is beneficial in that when transaction between users is completed within the blockchain, at step 109b, the proxy digital data in the proxy digital data storage **4** can be used again for new trade orders immediately, even when a trade execution has not been completed. The trade execution occurs upon completion of the proxy trade execution. Furthermore, the queue book **10** at step 110 arranges (e.g., chronologically) the at least one smart contract **7**, or at step 111 verifies or filters the at least one smart contract **7** in the at least one original blockchain **11**. At step 112 the trade execution takes place upon completion of the proxy trade execution, or thereafter, a peer-to-peer transaction **12**. Then, at step 113, the digital data are transferred or exchanged to corresponding digital data storage. The at least one user may withdraw digital data from their digital data storage into any external data storage device.

In some embodiments of the present invention, the proxy trade execution can take as little as 10 seconds. In contrast, conventional decentralized systems having a conventional blockchain generally have an execution time of at least 10 minutes. In addition, for example in Bitcoin transactions, execution of a transaction mainly depends on the speed of confirmation of users of plurality of computer servers, which may be located in any parts of the world, and execution can only be done after a consensus is established by these users. Also, these users have the option to determine which transaction to be processed first, and generally they prioritize those transactions that pay fees. Hence, delay or prolonged processing time for other transactions is inevitable. In contrast to the conventional decentralized system having a conventional blockchain, some embodiments of the present invention enable the proxy trade execution to have a minimum time of execution (for example, less than 10 seconds), thereby allowing faster verification and processing of digital data.

The above architectures, as evident above, expressly address both security and speed requirements.

In some embodiments of the present invention, the proxy digital data storage **4** is connected to the digital data storage **3**; or the proxy digital data storage **4** and the digital data storage **3** are linked to the digital data storage application **1a**. This provides security to the digital data. These features facilitate more secure transactions in the system.

In some embodiments of the present invention, the system comprises both a centralized and decentralized digital data exchange platform. The centralized part comprises the order book **6**, or the matching system **6a**. These can achieve increased speed of transaction of trades, as compared to trades of a conventional blockchain. The decentralized part comprises the at least one original blockchain **11**, or the at least one proxy blockchain **8**. This combination allows for faster and more secure digital data transaction.

The at least one external data storage device **2** may be implemented by a thumb drive, a flash drive, or any device capable of storing the digital data of the at least one user.

Referring to Fig. 2, a hybrid system of trade exchange is shown in accordance to an embodiment of the present invention. Then hybrid system comprises a centralized part 210 (may also be referred to as "off chain") comprising the order book 6, or the matching system **6a**. The hybrid system also comprises decentralized part 220 which comprises the original blockchain **11**, and the at least one blockchain **8**. At step 201,at least one incoming order is received from at least one user, and is recorded by the order book **6** in the blockchain **8** at step 202. A digital data storage (not shown) supplies security means to the blockchain **8** to decrypt orders. At step 203, digital data are sent to the matching system **6a**. At step 204, matching system **6a** sends at least one mirrored trade order to the blockchain **8**. At step 205, the at least one mirrored trade order is sent to the original blockchain **11**. At

step 206, digital data are then updated based on the history of matched trade.

Referring to Fig. 3, an example of comparison of trade transaction with respect to execution time frame, between an embodiment of the present invention and a conventional block chain is shown. In a given time frame, t (for example, from t=0 minute to t=10 minutes), a trade transaction in a conventional blockchain **320** produces a single trade contract, whereas in a same given time frame, a trade transaction via the blockchain system **310** of an embodiment of the present invention produces multiple trade contracts (not limited to the number as illustrated).

Referring to Fig. 4, a system architecture of an exchange in accordance to an embodiment of the present invention is shown. The diagram illustrates a conceptual framework for implementing the embodiments of the system and method of the present invention. The system architecture of an exchange comprises an application layer 410, a web browser, mobile App, terminal emulator 420, an access layer 430, a web 440, an API 450, a router 460, a service 470, a matching server 480, a price server 490, a data server 495, a store age layer 496, and a MySQL 497.

Referring to Fig. 5, a method for transaction in accordance to an embodiment of the present invention is shown. The method comprises the steps of first, at step 510, depositing of digital data by at least one user to at least one external data storage device **2**; second, at step 520, transferring of the digital data to a digital data storage application **1a** by a first security means **1b**; third, at step 530, receiving the digital data by a digital data storage **3**; then at step 540, mirroring of the digital data from the digital data storage **3** to a proxy digital data storage **4**; subsequently, at step 550, initiating plurality of trade orders **5a** by a second security means **5b** to the digital data storage application **1a**; at step 560, placing and matching thereafter the plurality of trade orders **5a** in a trade exchange **5**; then at step 570, creating at least one smart contract **7** from the plurality of

trade orders **5a** which are match; at step 580, verifying thereafter, of the at least one smart contract **7** by at least one proxy blockchain **8**; after which, at step 581, triggering a proxy trade execution by the at least one smart contract **7** created from the trade exchange **5**; then at step 583, arranging the at least one smart contract **7** in a queue book **10**; further, at step 584, verifying by the queue book **10**, of the at least one smart contract **7** in at least one original blockchain **11**; thereafter, at step 585, performing a trade execution upon completion of the proxy trade execution; or consequently, at step 586, transferring or exchanging of digital data to the digital data storage **3**.

In some embodiments of the present invention, the method facilitates multiple trade execution, wherein at step 582, the proxy digital data in the corresponding proxy digital data storage **4** can be used again for new trade orders, even when an actual trade execution has not been completed.

In some embodiments of the present invention, the step 560 of placing and matching the plurality of trade orders **5a** in a trade exchange **5** can comprise: algorithmically matching the plurality of trade orders **5a** in an order book **6** connected to the trade exchange **5**.

The abovementioned method possesses same benefits/advantages of providing more secure and speedy transaction as the system disclosed herein.

Referring to Fig. 6, the plurality of proxies **120** is shown. The plurality of proxies **120** is designed for duplicating the digital data from the digital data storage, and facilitates the proxy trade execution. The plurality of proxies **120** is triggered by the plurality of trade orders **5a** from the trade exchange **5**. The plurality of proxies **120** comprises the proxy order book **9a** for receiving the plurality of proxy trade orders **9b** from the trade

exchange **5**; the proxy matching system **9c** for matching the plurality of proxy trade orders **9b**; the at least one proxy smart contract **9d** created from matching the plurality of proxy trade orders **9b**; and the at least one proxy blockchain **8** for verification of the at least one smart contract **7** or for verification of the at least one proxy smart contract **9d** for proxy peer-to-peer transaction **9e**. The plurality of proxies **120** provides faster transaction speed to the users.

It should be noted that "at least one smart contract" is different with "at least one proxy smart contract". The "at least one smart contract" is created from the trade exchange from the plurality of trade orders which are match, or the "at least one smart contract" triggers a proxy trade execution. The "at least one proxy smart contract" is created from matching the plurality of proxy trade orders, or is suitable for proxy peer-to-peer transaction.

While various embodiments are presented by the present invention, it should be noted that these embodiments are illustrative only, and not restrictive. Modification to the embodiments herein describes are possible to those skilled in the art, without departing from the principles of the present invention. Further, various steps in the method may be done (e.g., desired steps may be added, manipulated, or deleted) in any order sought. Throughout the description and claims, expressions such as "including", "have", "having", "comprising", shall be construed in a non-exclusive manner, allowing other features, components, elements, or steps, not explicitly described to be also present. Moreover, references to singular, may also relate to plural.

CLAIMS

1. A system **(100)** for digital transaction, the system **(100)** comprising:

at least one external data storage device **(2)** for storing digital data of at least one user;

a digital data storage application **(1a)** for a machine-readable device **(1)** for transferring the digital data;

a queue book **(10)** for arranging at least one smart contract **(7)**, or for verification or filtering of the at least one smart contract **(7)** for at least one original blockchain **(11)** for a peer-to-peer transaction **(12)**;

a digital data storage **(3)** for receiving the digital data;

a trade exchange **(5)** connected to the digital data storage **(3)**;

the at least one smart contract **(7)** from the trade exchange **(5)**; and

a plurality of proxies comprising proxy digital data.

2. The system of claim 1, wherein the plurality of proxies further comprises:

at least one proxy digital data storage **(4)** for duplicating the digital data from the digital data storage **(3);**

at least one proxy order book **(9a)** for receiving plurality of proxy trade orders **(9b)** from the trade exchange **(5);**

at least one proxy matching system **(9c)** for matching the plurality of proxy trade orders **(9b);**

at least one proxy smart contract **(9d)** created from matching the plurality of proxy trade orders **(9b);** or

at least one proxy blockchain **(8)** for verification of the at least one smart contract **(7),** or for verification of the at least one proxy smart contract **(9d)** for proxy peer-to-peer transaction **(9e).**

3. The system of claim 1, wherein the proxy digital data is reusable.

4. The system of claim 1 or 2, wherein the proxy digital data storage **(4)** is connected to the digital data storage **(3);** and

wherein the proxy digital data storage **(4)** and the digital data storage **(3)** are linked to the digital data storage application **(1a).**

5. The system of claim 1, wherein the trade exchange **(5)** further comprises a plurality of trade orders **(5a)** having digital data, the trade exchange **(5)** is connected to an order book **(6)** for receiving the plurality of trade orders **(5a)**, and to a matching system **(6a)** for matching the plurality of trade orders **(5a)**.

6. The system of claim 1, wherein the digital data storage application **(1a)** requires a first security means **(1b)**.

7. The system of claim 1, wherein the trade exchange **(5)** comprises a second security means **(5b)** for initiating the plurality of trade orders **(5a)**.

8. A method for digital transaction, comprising steps of:

(a) depositing digital data from at least one user to at least one external data storage device **(2)**;

(b) transferring the digital data to a digital data storage application **(1a)** by a first security means **(1b)**;

(c) receiving the digital data by a digital data storage **(3)**;

(d) mirroring the digital data from the digital data storage **(3)** to a proxy digital data storage **(4)**;

(e) initiating a plurality of trade orders **(5a)** by a second security means **(5b)** to the digital data storage application **(1a);**

(f) placing and matching the plurality of trade orders **(5a)** in a trade exchange **(5);**

(g) creating at least one smart contract **(7)** from the plurality of trade orders **(5a)** which are matched;

(h) verifying the at least one smart contract **(7)** by at least one proxy blockchain **(8);**

(i) triggering a proxy trade execution by the at least one smart contract **(7)** created from the trade exchange **(5);**

(j) arranging the at least one smart contract **(7)** in a queue book **(10);**

(k) verifying, by the queue book **(10),** of the at least one smart contract **(7)** in at least one original blockchain **(11);**

(l) performing a trade execution upon completion of the proxy trade execution; or

(m) transferring or exchanging digital data to the digital data storage **(3).**

9. The method of claim 8, wherein placing and matching the plurality of trade orders **(5a)** in a trade exchange **(5),** further comprises:

algorithmically matching the plurality of trade orders **(5a)** in an order book **(6)** connected to the trade exchange **(5).**