

METHOD OF DELIVERY-VERSUS-PAYMENT (DvP) AND SYSTEM THEREOF

Field of Invention

[0001] The invention relates to delivery-versus-payment (**DvP**) settlement process in relation to financial instruments and various aspects of implementing DvP, including generation of a temporary password for facilitating secured DvP.

Background

Distributed Ledger Technology (DLT)

[0002] Blockchains are essentially implementations of Distributed Ledger Technology (**DLT**). A DLT is way for recording the transactions of assets in multiple places at the same time, it also relies on principles of consensus to achieve accurate entries of transactions into the distributed databases. In other words, it is a network built on contracts that consistently and coherently define the rights and obligations of its participants. In doing so, it may replace the need for a centralised authority to enforce rules, disseminate information and make decisions. Instead, DLT participants – each represented by a computer (**node**) on the network – simultaneously share, update, verify, and reach consensus on transactions.

[0003] In addition, data involved in these activities is protected by cryptography, and is immutable, hence lowering the threat of cybercrime. With round-the-clock uptime, the ability of a network to live across multiple locations (sites, countries or institutions), and the shouldering of complex tasks by computer code, it is easy to see why DLT has many business applications. Indeed, the effect of DLT on capital markets could potentially be game-changing (see Table 1 below which shows the impact of DLT on the capital markets value chain).

[0004] While DLT holds the promise of reducing some of the inefficiencies embodied in the current market infrastructure, much rigorous testing remains to be done before DLT proves itself to be the *de facto* solution.

Table 1

Pre-Trade	Trade	Post-Trade	
TASK			
Research analytics and risk management	Order execution and matching	Clearing and settlement	Custody and asset servicing
CURRENT PAIN POINTS IN CAPITAL MARKETS			

Information flow lag time	Operational hours restricted to business hours and batch settlement	Counterparty risk, opportunity and financing costs	Costly and need for manual processing and reconciliation
BENEFITS OF DLT IN CAPITAL MARKETS			
Transparent and automated verification of asset ownership	24/7 access to markets and trading	Elimination of counterparty risk with more efficient settlement via automated DvP	Remove need of safekeeping assets through immutable transaction records
Improved confidence in market analysis based on immutable data history	Alignment for cross-border settlement capabilities	Speedier, seamless asset recovery enabled by smart contracts	Reduced operational costs
Market efficiency with availability of to-the-minute information	-	Reduced margin/collateral outlay and Central Clearing Party / Central Counterparty (CCP) costs	Automated reconciliation using blockchain

[0005] Although the “D” in DLT stands for Distributed, it should not be mistaken for a decentralised system. The fact is that every aspect of DLT – including contracts, standards, protocols, databases, and algorithms – are all centric implementations. While in some cases blockchain allows for disintermediation, in others it allows efficient and effective process automation that creates new value for customers and businesses.

Delivery-versus-Payment (DvP)

[0006] Simply put, a DVP settlement process is one where the cash payment for a purchased security occurs prior to, or upon, its delivery, much akin to two counterparties (traders) meeting at an agreed time to exchange the agreed assets. With the transfer of one asset conditioned upon the transfer of the other, counterparties are protected from counterparty risk, viz. the risk that the seller of a security could fail to receive payment despite fulfilling delivery, or the risk that the buyer of a security could fail to receive delivery despite fulfilling payment. Principal risk is mitigated by requiring the delivery only if payment occurs, thereby limiting the probability that securities or payment will be withheld during period of stress in the financial markets.

[0007] It is worth noting that DvP need not be instantaneous, and may be achieved through time-limited arrangements built into settlement mechanisms, where participants (e.g. buyers and sellers) are given a reasonable time frame to fulfil their settlement obligations, failing which an appointed independent third party (e.g. arbitrator) will intervene to resolve the failed transaction which often leads to inefficient, long, inflexible and expensive court proceedings. This creates certain problems.

[0008] On the subject of DvP, it has been observed that there has been a growing preference for shorter settlement periods over long-held industry norms. This trend is largely fuelled by concerns over the risks linked to lengthy and inefficient post-trade practices that were uncovered by the 2009 financial crisis. In fact, many regulators and stock exchanges have looked into their own settlement cycles over the last 10 years to reassess their risk exposures. Various CCPs in Europe, Hong Kong, Japan and Singapore, to name a few, have either initiated studies to examine or have completed the migration from T+3 (transaction date plus 3 working days) settlement period to T+2 (transaction date plus 2 working days) settlement period.

[0009] Furthermore, a 2014 study conducted by the U.S. Depository Trust & Clearing Corporation (**DTCC**) recommended the compression of trade settlement cycles for equities, municipal and corporate bonds, and unit investment trusts, from T+3 to T+2. DTCC also explored the possibility of shortening the settlement cycle further to T+1 (transaction date plus 1 working day) as a future consideration to enhance investor protection (by reducing counterparty and principal risks). In other words, to even move towards T+2, which is challenging to accomplish, is far from ideal.

[0010] Regardless of their reasons for pursuing DLT implementations or speedier DvP – or a combination of both – the common sentiment among financial institutions is clear: system

inefficiencies have a direct bearing on the amount of risks and costs one is subjected to. DLT has emerged as a technology that can possibly resolve such inefficiencies.

[0011] For high value transactions in the capital markets, a trusted third party (known as the arbitrator) is required to facilitate such high value transactions by stepping in to settle any disputes which may arise, for example disputes due to duplication or discrepancies. As mentioned above, there is counterparty and principal risk in all capital market transactions as either the buyer or seller may fail to perform its contractual obligations. Furthermore, when a manual intervention is required to unwind or resolve a failed transaction, the arbitrator has to liaise with both parties to the transaction, resulting in the need for the cooperation and mutual agreement of all three parties.

Gridlocks

[0012] In addition, there are gridlocks in the Real-Time Gross Settlement (**RTGS**) systems. RTGS systems are funds transfer systems that process a large number of high-value transactions requiring near immediate settlement or immediate settlement. There is therefore a demand on such systems to neutralise intraday liquidity gridlocks, by means of a Liquidity Saving Mechanism (**LSM**), to move transactions along. LSMs are traditionally found on centralised systems, as is the case for most RTGS systems around the world, where the algorithms necessary for their implementation usually require a consolidated, system-wide view of all payment instructions. This sharply contrasts with the concept of a decentralised LSM offered by DLT.

[0013] A typical payment gridlock is a paradoxical scenario where senders and receivers are unable to settle queued payment instructions one-to-one, in a sequential manner, due to insufficient funds, despite the fact that the net liquidity held by all participants in the gridlock is sufficient for the simultaneous settlement of all transactions. If there are LSMs (private or public queue mechanisms) that can prioritise all payment instructions to trigger gridlock resolution – that is, enable incoming and outgoing amounts to coincide without any risk of a deficit – smoother settlements can be achieved and costly deadlocks avoided. The idea of a DLT-based RTGS system with an efficient LSM is especially relevant in the context of capital markets, particularly with securities trading. While digitisation has shortened trading time frames considerably, the same cannot be said for clearing and settlement, which can stretch up to fifteen days (T+15). This delay is partly due to existing market structure and rules that dictate that both participants be given some time to secure the underlying assets during post-trade settlement.

[0014] With distributed ledgers' ability to ascertain a buyer's liquidity and to effect settlement within the trading phase itself, the time and monetary costs associated with post-trade financing may soon be a thing of the past (see Figure 1). This explains why a fully functional DLT-based RTGS system holds immense interest for industry players. Furthermore, DLT can also support the use of smart contracts to automate or replace convoluted processes currently performed by clearing houses, back office systems and registries.

Inherent risks in Atomic Swaps for DLT

[0015] In addition to the above challenges, other problems faced by the art include inherent risks in Atomic Swaps for DLT. Atomic Swaps mitigate counterparty risk by instituting that both parties have to acknowledge the receipt of funds within a specified timeframe using a cryptographic hash function. However, this raises the question of whether the public key received by the sender to encrypt the one-time password (**OTP**) is genuine, especially in cases where the beneficiary's identity is not known to the sender. In addition, if the beneficiary's private key is compromised, there is no route for recourse and the attacker would be able to manipulate the funds in the wallet.

[0016] In the current state of art, a two-factor authentication (**2FA**) mechanism is put in place for an extra layer of security for the purpose of authentication during transactions. Organizations are either reliant on hardware tokens or a one-time password (**OTP**) sent via Short Message Service (**SMS**), voice calls, secure emails or via an application. However, hardware tokens are prone to additional expenses with lost, broken or expiring tokens. OTPs sent via SMS, voice calls, secure emails or via an application are susceptible to man-in-the-middle attacks, spoofing attacks, eavesdropping attacks and bot attacks. OTPs sent by post are liable to lost mail or late mail. For all of the above, strong passwords need to be enforced, secure lock/passwords need to be set on electronic devices for the purpose of 2FA, physical security tokens and electronic devices need to be stored in a safe location, and users need to be wary of illegitimate notifications of password resets/ phishing scams. Further, before 2FA can be established and deployed, a user will usually have to apply for a hardware token or register an additional electronic device to receive OTPs. This creates an additional hassle and delay for the end users.

[0017] To compound the issue, OTPs are usually only valid for a limited period of time, and more often than not will expire before it is used by the recipient. This in turn creates inefficiencies as additional resources are then required to resend another OTP.

[0018] The present invention seeks to solve the above and other problems.

Summary

[0019] In a first aspect of the invention, there is provided a method of DvP settlement using a trusted independent entity (e.g. arbitrator, arbitration system) in a tokenised asset environment. In the transfer/delivery of tokenised assets, it is possible for the settlement date to be set in advance (e.g. at the point of entering the order into the trading system) or to be altered before the trade is confirmed. Hence, since settlement can be open-ended, it may be preferable to use an independent entity to oversee this process.

[0020] In the context of capital markets, methods of the invention are particularly suited for, but not limited to, high value transactions where a trusted independent entity (e.g. arbitrator) is appointed to facilitate such high value transactions and settle any duplication, disputes or discrepancies which may arise. The methods of the invention would also be used to verify the transaction for DvP settlement of transactions involving tokenised assets, e.g. securities and cash.

[0021] For high value transactions of tokenised assets, there are higher counterparty and principal risks in the DvP of securities and cash. In accordance with various embodiments of the first aspect of the invention, the respective parties or entities would register with the independent entity an identification document and a secure communication channel to receive a temporary password, e.g. OTP. After a counterparty matching of transaction in the trading system, the independent entity will generate password-protected encrypted files, e.g. Portable Document Format (**PDF**) file, containing the same OTP to send across to the seller and the buyer. Each of the seller and buyer then unlocks the respective encrypted PDF file to view the OTP and enter the OTP into the trading system to unlock the smart contracts to discharge their cash or securities obligations immediately after the verification from both the seller and the buyer. In an alternate scenario where the seller and/or the buyer intend to dispute the transaction, at least one of them would reach out to the independent entity. Here, the buyer is able to call on the independent entity to help (i) obtain the agreed amount of securities from the seller, or (ii) recover the cash that has already been paid out to the seller. The smart contracts are programmed such that 2 out of the 3 parties' (buyer, seller, independent entity) signatures (**2-out-of-3-signatures**) are required to unlock or discharge the smart contracts, and therefore the smart contracts can be unlocked or discharged with just the disputer's and the arbitrator's consents. In another scenario where a buyer's or seller's private key, e.g. password defined by the buyer or seller and registered with the independent entity, is lost, they could then reach out to the independent entity to reverse any unauthorised trades performed using their account. The independent entity would then reverse the trade with the other counterparty upon fulfilling the 2-out-of-3-signatures requirement.

[0022] According to the first aspect of the invention, a computer-implemented delivery versus payment (DvP) method comprises:

storing passwords and communication preferences defined by entities which
5 include a seller, a buyer and an independent entity;

in response to notification of a transaction between the seller and the buyer,
generating a temporary password which is configured to discharge a smart contract
generated at distributed ledgers for the transaction;

generating separate encrypted files which contain the temporary password
10 and are respectively decryptable by the stored passwords defined by the seller and
the buyer; and

electronically transmitting, by the independent entity, the encrypted files to the
seller and the buyer respectively.

[0023] In one embodiment of the aforementioned method of the first aspect, after
15 electronically transmitting, by the independent entity, the encrypted files to the seller and the
buyer respectively, the method further comprises:

receiving, from one of the distributed ledgers, notification of a dispute contract
which is initiated by a signature of the buyer or the seller; and

transmitting, by the independent entity, a signature of the independent entity to
20 the one of the distributed ledgers to provide one of two signatures required from at
least two of the group consisting of the seller, the buyer and the independent entity to
discharge the smart contract, wherein each signature includes the temporary password
or a hash value thereof.

[0024] In one embodiment of the aforementioned method of the first aspect, after
25 electronically transmitting, by the independent entity, the encrypted files to the seller and the
buyer respectively, the method further comprises:

after the smart contract is discharged by the distributed ledgers,

receiving, from either the seller or the buyer, a request to reverse the
30 transaction;

receiving, from one of the seller and the buyer other than a sender of
the request, consent to the request;

transmitting, by the independent entity, a signature of the independent
entity to the distributed ledgers to provide one of two signatures required from
35 at least two of the group consisting of the seller, the buyer and the

independent entity to reverse the transfer of the cash and of the securities, wherein each signature includes the temporary password or a hash value thereof.

[0025] According to the first aspect of the invention, a delivery versus payment (DvP) system comprises:

one or more databases configured to store passwords and communication preferences defined by entities which include a seller, a buyer and an independent entity;

a receiving module of the independent entity, configured to receive notification of a transaction between the seller and the buyer;

a processor of the independent entity, configured to:

in response to the notification of the transaction between the seller and the buyer, generate a temporary password which is configured to discharge a smart contract generated at distributed ledgers for the transaction,

generate separate encrypted files which contain the temporary password and are respectively decryptable by the stored passwords defined by the seller and the buyer; and

a transmission module of the independent entity, configured to electronically transmit the encrypted files to the seller and the buyer respectively, wherein the one or more databases, the receiving module and the transmission module are communicably coupled to the processor.

[0026] In one embodiment of the aforementioned system of the first aspect, the receiving module is further configured to receive, from one of the distributed ledgers, notification of a dispute contract which is initiated by a signature of the buyer or the seller; and the transmission module is further configured to transmit a signature of the independent entity to the one of the distributed ledgers to provide one of two signatures required from at least two of the group consisting of the seller, the buyer and the independent entity to discharge the smart contract, wherein each signature includes the temporary password or a hash value thereof.

[0027] In one embodiment of the aforementioned system of the first aspect, wherein after the smart contract is discharged by the distributed ledgers,

the receiving module is further configured to:

receive, from either the seller or the buyer, a request to reverse the transaction,

receive, from one of the seller and the buyer other than a sender of the request, consent to the request; and

the transmission module is further configured to transmit a signature of the independent entity to the distributed ledgers to provide one of two signatures required from at least two of the group consisting of the seller, the buyer and the independent entity to reverse the transfer of the cash and of the securities, wherein each signature includes the temporary password or a hash value thereof.

[0028] According to the first aspect of the invention, a computer-implemented delivery versus payment (DvP) method comprises:

in response to a transaction between a seller and a buyer, generating a smart contract for the transaction and notifying an independent entity to generate separate encrypted files which contain an identical temporary password and are respectively decryptable by passwords defined by the seller and the buyer, wherein the smart contract identifies cash, securities and a settlement time limit which are required to complete settlement of the transaction;

if the temporary password is separately received, by distributed ledgers comprising a cash ledger and a securities ledger, from the seller and the buyer within the settlement time limit, discharging the smart contract, including:

instructing a transfer of the cash to the seller,
instructing a transfer of the securities to the buyer,
posting the transfer of the cash to the cash ledger, and
posting the transfer of the securities to the securities ledger.

[0029] In one embodiment of the aforementioned method of the first aspect, before discharging the smart contract, the method further comprises:

based on a first securities instruction from the seller, posting a securities contract lock to a securities ledger to safekeep the securities;

based on a first cash instruction from the buyer, posting a cash contract lock at a cash ledger to safekeep the cash;

upon receiving the temporary password from the seller within a first time limit, posting a cash claim instruction at the cash ledger to claim the cash; and

upon receiving the temporary password from the buyer within a second time limit, posting a securities claim instruction at the securities ledger to claim the securities, and

wherein discharging the smart contract includes releasing the securities contract lock and releasing the cash contract lock.

[0030] In one embodiment of the aforementioned method of the first aspect, after posting the transfer of the cash to the cash ledger, and posting the transfer of the securities to the securities ledger, the method further comprises:

receiving a request to reverse transaction;

5 if at least two signatures are received from at least two of the group consisting of the seller, the buyer and the independent entity,
instructing a return of the cash to the buyer,
instructing a return of the securities to the seller,
posting the return of the cash to the cash ledger, and
10 posting the return of the securities to the securities ledger.

[0031] In one embodiment of the aforementioned method of the first aspect, the method comprises:

if the temporary password is not received, by the distributed ledgers, from both the seller and the buyer within the settlement time limit and if a return instruction is
15 received by the distributed ledgers, discharging the smart contract, including:
instructing a return of the cash to the buyer,
instructing a return of the securities to the seller,
posting the return of the cash to the cash ledger, and
posting the return of the securities to the securities ledger.

20 [0032] In one embodiment of the aforementioned method of the first aspect, wherein before discharging the smart contract, if the temporary password is not received, by the distributed ledgers, from both the seller and the buyer within the settlement time limit and if a return instruction is received by the distributed ledgers, the method further comprises:

based on a first securities instruction from the seller, posting a securities
25 contract lock at a securities ledger to safekeep the securities;

based on a first cash instruction from the buyer, posting a cash contract lock at a cash ledger to safekeep the cash;

upon receiving the temporary password from the seller, posting a cash claim instruction at the cash ledger to claim the cash; and

30 failing to receive the temporary password from the buyer within the settlement time limit.

[0033] In one embodiment of the aforementioned method of the first aspect, the method comprises:

if the temporary password is received, by the distributed ledgers, from either the
35 seller or the buyer within the settlement time limit and if a signed dispute contract is

received, by the distributed ledgers, from either the seller or the buyer, notifying the independent entity and receiving a signature from the independent entity, and

if at least two signatures are received from at least two of the group consisting of the seller, the buyer and the independent entity, discharging the smart contract including:

5 instructing a return of the cash to the buyer and/or instructing a return of the securities to the seller, posting the return of the cash to the cash ledger and/or posting the return of the securities to the securities ledger, wherein each signature includes the temporary password or a hash value thereof.

10 [0034] In one embodiment of the aforementioned method of the first aspect, wherein before notifying the independent entity and receiving a signature from the independent entity, the method further comprises:

 based on a first securities instruction from the seller, posting a securities contract lock at a securities ledger to safekeep the securities;

15 based on a first cash instruction from the buyer, posting a cash contract lock at a cash ledger to safekeep the cash;

 upon receiving the temporary password from the seller, posting a cash claim instruction at the cash ledger to claim the cash; and

 failing to receive the temporary password from the buyer within the settlement
20 time limit.

[0035] In a second aspect of the present invention, there is provided an encrypted file, e.g. PDF file, that serves as a transport layer for transporting a temporary password, e.g. one-time password (**OTP**), securely through multi-factor authentication. The PDF file can be transferred through electronic mail, messaging application, e.g. WhatsApp, Telegram, or any electronic
25 means to the respective parties and may be encrypted with Advanced Encryption Standard 256 (**AES256**) or other encryption algorithm. The encrypted PDF file can only be opened or decrypted with a private password which the respective party has registered with the independent entity. The PDF file contains the OTP which may be generated using the transaction details as the seed to ensure entropy. The PDF file may also contain a digital
30 signature from the independent entity, which may be generated by Secure Hash Algorithm 256 (**SHA256**) or other hashing algorithm. The digital signature is to verify the sender's identity. Public Key Cryptography Standards 12 (**PKCS12**) may be used to embed the public key of the independent entity into the PDF file. The OTP may be presented in two or more encoded formats to prevent bot attacks, e.g. presented as both a Completely Automated

Public Turing test to tell Computers and Humans Apart (**CAPTCHA**) code and a Quick Response (**QR**) code.

[0036] The first aspect of the invention, i.e. the DvP settlement process, can work without the second aspect of the invention, i.e. transport of a temporary password via an encrypted PDF file, and vice versa. In other words, other forms of encryption, including those mentioned earlier such as OTP, 2FA, etc. may be used with the first aspect of the invention. For example, the DvP settlement process can possibly use secured software token to transmit the OTP, but transport of the OTP via encrypted PDF file does provide further advantages, e.g. security, cost efficiencies and convenience. Also, the DvP settlement process according to the invention is different from existing practice at least in its integration of arbitration within a platform (system) and the use of smart contracts.

[0037] For DvP to successfully conclude, trade participants must perform their obligations within the specified time limits. The seller specifies a time limit before the settlement process is initiated where two distinct legs of the transaction will take place on the cash and securities ledgers. Time limits or boundaries are adopted to ensure a fair settlement and preventing unnecessary risk exposure to the parties involved.

[0038] Contract locks render the amount of cash and securities committed by both the buyer and seller untouchable on the respective ledgers. This prevents said assets from being used in another trade, hence removing the risk of payment and delivery defaults. The contract locks are in effect when counterparties commit to a transaction by sending instructions to the respective ledgers. The underlying assets will be locked and participants will be unable to use the same assets for other transactions until the contracts are discharged. Contracts are discharged when (i) the buyer and seller fulfill their obligations by mutually transferring the assets to each other or (ii) the contract expires due to the specified time boundaries.

[0039] Participants engaged in a trade or transaction are expected to fulfill the 2-out-of-3-signatures condition at various points of the settlement process to advance towards settlement finality. Buyer and seller will hold their individual private keys. Arbitrator, independent from buyer and seller, will be provided with an escrow private key for safekeeping — this enables the arbitrator to be able to resolve disputes on the condition that either of the parties provides the first signature.

[0040] Both the buyer and seller have to enter the same OTP to the trading system to effect asset transfer. This OTP would be generated by the independent entity. This OTP is sent to

each of the seller and buyer in the form of an encrypted and password-protected PDF file at the start of post-trade settlement, and is used for the verification of instructions issued by counterparties till settlement finality is reached.

- 5 [0041] According to the second aspect of the invention, a method for generation and secured transmission of temporary password comprises:

generating a temporary password;

- 10 generating a first and a second encrypted Portable Document Format (PDF) file which are respectively decryptable by a first password defined by a first entity and a second password defined by a second entity, wherein each PDF file is embedded with the temporary password as two or more distinct encoded formats and further embedded with a digital signature and/or certificate of a third entity; and

electronically transmitting the first and the second encrypted PDF document to the first and the second entity respectively.

- 15 [0042] In one embodiment of the aforementioned method of the second aspect, generating the temporary password is performed by the third entity in response to a notification of a transaction between the first entity and the second entity.

- 20 [0043] In one embodiment of the aforementioned method of the second aspect, generating a first and a second encrypted PDF file includes generating the digital signature using a password of the third entity and a cryptographic hash function; and embedding the digital signature and/or the digital certificate into each of the PDF documents.

- 25 [0044] In one embodiment of the aforementioned method of the second aspect, generating the temporary password includes generating the temporary password using at least one seed selected from the group consisting of the first password, the second password, a private key of the third entity, and details from the transaction.

- 30 [0045] In one embodiment of the aforementioned method of the second aspect, the details from the transaction includes at least one selected from the group consisting of date and/or time of the transaction, name of the first and/or the second entity, address of the first and/or the second entity, reference code of the transaction, agreed quantity and price of securities for the transaction, agreed settlement period.

[0046] In one embodiment of the aforementioned method of the second aspect, electronically transmitting the first and the second encrypted PDF document to the first and the second entity respectively includes electronically transmitting the first and the second encrypted PDF document, by a communication channel which is separate from a platform facilitating the transaction, to the first and the second entity respectively.

[0047] In one embodiment of the aforementioned method of the second aspect, electronically transmitting the first and the second encrypted PDF document to the first and the second entity respectively includes electronically transmitting the first and the second encrypted PDF document, by electronic mail or messaging application or Short Message Service (SMS) notification having a Uniform Resource Locator (**URL**) or any combination thereof, to the first and the second entity respectively.

[0048] In one embodiment of the aforementioned method of the second aspect, the encoded formats include at least two selected from the group consisting of Completely Automated Public Turing Test To Tell Computers and Humans Apart (CAPTCHA) code, Quick Response (QR) code and barcode.

[0049] According to the second aspect of the invention, a non-transitory computer readable storage medium comprises:

a first and a second encrypted Portable Document Format (PDF) document which are respectively decryptable by a first password defined by a first entity and a second password defined by a second entity, wherein each PDF document comprises:

a temporary password embedded in the PDF document as two or more distinct encoded formats; and

a digital signature and/or certificate of a third entity which generated the PDF document.

[0050] In one embodiment of the aforementioned computer readable storage medium of the second aspect, the encoded formats include at least two selected from the group consisting of Completely Automated Public Turing Test To Tell Computers and Humans Apart (CAPTCHA) code, Quick Response (QR) code and barcode.

[0051] In one embodiment of the aforementioned computer readable storage medium of the second aspect, the temporary password is generated using at least one seed selected from

the group consisting of the first password, the second password, a private key of the third party, and details from the transaction.

[0052] In one embodiment of the aforementioned computer readable storage medium of the second aspect, the details from the transaction includes at least one selected from the group consisting of date and/or time of the transaction, name of the first and/or the second entity, address of the first and/or the second entity, reference code of the transaction, agreed quantity and price of securities for the transaction, agreed settlement period.

10 **Brief Description of the Drawings**

[0053] Embodiments of the invention are disclosed hereinafter with reference to the drawings, in which:

[0054] Figure 1 shows an ability of distributed ledgers to effect settlement within the trading phase;

15 [0055] Figure 2 shows MEPS+ which is an RTGS system implemented and operated by the Monetary Authority of Singapore (**MAS**), comprising two subsystems: MEPS+-SGS and MEPS+-IFT (interbank fund transfer system);

[0056] Figure 3A is an overall schematic representation of DvP settlement in an environment where cash and securities are implemented on a network comprising at least two different
20 blockchains;

[0057] Figure 3B shows an example of an architecture for implementing some embodiments of the present invention;

[0058] Figure 4A is a flow chart which describes settlement success;

[0059] Figure 4B describes a rights and obligations model in DvP for securities in an
25 embodiment of the present invention;

[0060] Figure 5A is a sequence diagram illustrating settlement success;

[0061] Figure 5B is a sequence diagram illustrating seller dispute after settlement time limit expires;

[0062] Figure 5C is a sequence diagram illustrating seller dispute before settlement time limit
30 expires;

[0063] Figure 5D is a sequence diagram illustrating buyer dispute after settlement time limit expires;

[0064] Figure 5E is a sequence diagram illustrating buyer dispute before settlement time limit expires;

35 [0065] Figure 5F is a sequence diagram illustrating transaction reversal after settlement success;

[0066] Figure 6 is a flow chart which describes generation of a temporary password;

[0067] Figure 7 is a schematic representation of seed(s) used in generation of a temporary password; and

[0068] Figure 8 is a schematic representation of decrypting an encrypted PDF file to reveal the temporary password.

5

Detailed Description

[0069] In the following description, numerous specific details are set forth in order to provide a thorough understanding of various illustrative embodiments of the invention. It will be understood, however, to one skilled in the art, that embodiments of the invention may be practised without some or all of these specific details. In other instances, well known process operations have not been described in detail in order not to unnecessarily obscure pertinent aspects of embodiments being described. In the drawings, like reference numerals refer to same or similar functionalities or features throughout the several views.

10

15

[0070] Embodiments described in the context of one of the methods or devices are analogously valid for the other methods or devices. Similarly, embodiments described in the context of a method are analogously valid for a device, and vice versa.

20

[0071] Features that are described in the context of an embodiment may correspondingly be applicable to the same or similar features in the other embodiments. Features that are described in the context of an embodiment may correspondingly be applicable to the other embodiments, even if not explicitly described in these other embodiments. Furthermore, additions and/or combinations and/or alternatives as described for a feature in the context of an embodiment may correspondingly be applicable to the same or similar feature in the other

25

[0072] As used herein, the articles “a”, “an” and “the” as used with regard to a feature or element include a reference to one or more of the features or elements.

30

[0073] As used herein, the term “and/or” includes any and all combinations of one or more of the associated listed items.

[0074] As used herein, the terms “first,” “second,” and “third,” etc. are used merely as labels, and are not intended to impose numerical requirements on their objects.

35

[0075] As used herein, the terms “buyer”, “seller” and “counterparties” may be used in place of “trade participants”. References to “first entity”, “first party” and “seller” are interchangeable; references to “second entity”, “second party” and “buyer” are interchangeable; references to “third entity”, “independent entity”, “third party” and “arbitrator” are interchangeable; references to “trade” and “transaction” are interchangeable; references to “tokenised ledgers” and “distributed ledgers” are interchangeable; references to “computer” and “processor” are interchangeable.

[0076] As used herein, references to “arbitrator” may include references to “arbitration system”, and vice versa. As used herein, references to “temporary password” may include references to “OTP”, and vice versa. As used herein, references to “computer” and “processor” may include references to “node”, and vice versa.

[0077] As used therein, the term “coupled” and related terms are used in an operational sense and are not necessarily limited to a direct physical connection or coupling. Thus, for example, two devices or entities may be coupled directly, or via one or more intermediary devices or entities.

Overview

[0078] The invention supports the market feasibility of DvP on DLT with respect to (i) the current market structures and practices, (ii) the overarching regulatory framework that governs post-trade settlement processes such as arbitration, and (iii) enhancing investor security and confidence. In particular, this invention not only supports the commercial application of DLT in securities settlement to enable efficient trade settlement and reconciliation, but also drives down operational costs. Savings garnered could then be passed on to investors through lower trading costs, which would in turn boost market participation and trading volume.

[0079] The present invention realises DvP settlement (interledger connectivity and settlement finality) of two tokenised assets across separate and different blockchain platforms (distributed ledgers). The two tokenised assets may be MAS-issued Singapore Government Securities (**SGS**) and an MAS-issued central bank digital currency in the form of Digital SGD (digital Singapore dollar currency). It is to be appreciated that the invention is equally suitable to support DvP of other financial instruments and/or currencies.

[0080] The invention may be implemented on various architectures that allow for the transfer of tokenised assets. As a first step, the assets would need to be “converted” into tokenised form. For example, a tokenised form of an asset, such as a digital currency issued by a central bank, may be used for inter-bank payments and settlement on a distributed ledger. In such a system, participant banks pledge cash into a custody account held at the central bank. The central bank will then create the equivalent value in digital currency on the distributed ledger, and assign them to the respective banks. It is to be appreciated that the invention is equally applicable to commercial bank issued digital currency. Once the banks have received their digital currency transfers from the central bank or another commercial bank, they are then free to make transfers (payments) to each other or the central bank. Interbank payments can be made possible by the integration and synchronisation of the distributed ledger with MEPS+ (electronic payment system), the MAS’s RTGS system. This implies that beyond enabling round-the-clock uptime and the traceability of records, distributed ledgers also possess the ability to preserve the integrity of the data held by existing electronic payments and book-entry systems. A digital currency money market, where banks can lend to and borrow digital currency from one another is also no longer a distant possibility.

MEPS+ DvP system

[0081] MEPS+ is an RTGS system implemented and operated by the MAS, comprising two subsystems: MEPS+-SGS and MEPS+-IFT (interbank fund transfer system). The former handles the scripless settlement of MAS-issued SGS on a DvP basis while the latter enables high-value SGD-denominated interbank funds transfers. Market participants must be registered with MAS before they can engage in transactions (see Figure 2). The MAS SGS Market Committee also has provenance over dispute resolution as an arbitrator.

Systemic Operational Risks

[0082] In a conventional settlement system, all participating banks that require settlement services will have to be connected to central operators (i.e. clearing houses and central banks) in order to settle their transactions. A central operator represents a single point of failure in this closed loop system (i.e. systemic risk).

[0083] Where DLT is used as a way to achieve connectivity between asset ledgers built on separate systems, the systemic risk of siloed infrastructures, such as MEPS+, can be effectively removed. Distributing control to participants would in fact strengthen security

resilience in the system since DLT makes the simultaneous hacking of multiple nodes extremely difficult.

[0084] Although the transactional mechanisms could be replaced by DLT, the need for a central operator with legal oversight over transaction and to assume the role of arbitrator would be an issue that needs to be resolved.

Operating Hours

[0085] In addition to the payment gridlock described above, MEPS+ operates with fixed operating hours, and the limitations imposed by fixed operating hours are a problem that plagues most, if not all, RTGS systems around the world. Going by current standards, it is simply unrealistic to expect round the clock trade-by-trade settlement. While clearing and settlement cycles characterised by T+2 or T+3 have become an industry norm, any delay in the settlement process fundamentally exposes trade participants to principal and counterparty risks.

[0086] With DLT possibly enabling 24/7 uptime and continuous trade-by-trade settlement facilitated by LSMs, clearing cycles of T+3 or T+2 can be compressed and their associated risks reduced.

Compliance

[0087] Adherence to contractual obligations is difficult for the central operator (clearing house) to enforce in practice. Often, extra processes, labour and financial resources have to be committed to ensure compliance. Additionally, the current market setup does not completely mandate provenance on the securities. For example, it typically takes a number of years for a regulator to complete an overhaul in the financial industry, particularly with regulatory changes, changes in compliance standards and system upgrades.

[0088] A DLT system can make use of smart contracts to contractually bind participants to operate in compliance. Although the benefits of such functionalities are appealing, there is a need for prudence due to the high-risk nature of the financial services industry. One will have to consider whether a hybrid system that combines a distributed network and a central operator would work in practice, and whether the system includes certain operational requirements to ensure that the framework is sufficiently robust to facilitate dispute resolutions.

[0089] While the proposed implementation of DLT in the current settlement system could very well address the drawbacks which are inherent in existing RTGS systems, the real test lies in proving its efficacy. In order to achieve this, DvP-on-DLT prototypes or architectures that can accomplish the following were designed and created:

5

[0090] Interledger interoperability between cash and securities ledgers built on separate DLT platforms;

[0091] Mitigation of counterparty risks in DvP by enabling recovery on cash and securities ledgers;

10 [0092] Enabling of counterparties to achieve DvP settlement finality with clearing members;

[0093] Strengthening of investor confidence and an enhanced user experience in DvP with safe and sound recovery.

15 [0094] In the invention, DvP settlement is achieved in an environment where cash and securities are implemented on a network comprising at least two different blockchains (see Figure 3A). Various embodiments of the invention also describe key participants and their roles, key architecture features and a baseline settlement process flow, with examples of success and failure cases.

20 **Key participants and ledgers**

[0095] **Market Operator (MO)** (this may be a stock exchange, e.g., the Singapore Exchange or the operator of any other exchange and/or trading platform). This entity has oversight of both ledgers and dealer activities. It could also assume the role of an independent entity (e.g. arbitrator) that has access to an escrow private key.

25

[0096] **Buyer:** This entity is an MO-registered trader with accounts on both the cash and securities ledger, and two pairs of keys (a pair for the cash and securities ledgers, respectively). Each pair includes one public key and one private key.

[0097] **Seller:** This entity is an MO-registered trader with accounts on both the cash and securities ledger, and two pairs of keys (a pair for the cash and securities ledgers, respectively). Each pair includes one public key and one private key.

30

[0098] **Cash Ledger:** This entity is the central or commercial bank-managed ledger for the tokenised digital asset.

[0099] **Securities Ledger:** This entity is an MO-managed ledger for the tokenised asset.

35

Key architecture features

[0100] To achieve a DvP-on-DLT architecture that is fit for purpose, the proposed system must be able to (i) aid trade participants in their fulfilment of obligations, (ii) mitigate, among others, principal and counterparty risks, (iii) allow for the conclusive state of settlement finality and (iv) improve investor confidence.

Time Boundary

[0101] For DvP to successfully conclude, trade participants must perform their obligations within the specified time limits. Before the settlement process is initiated, the seller specifies a time window during which two distinct legs of the transaction will have to take place on the cash and securities ledgers. The present invention adopts time limits to ensure a fair settlement and to prevent unnecessary risk exposure to the participants. It also highlights the possibility of having a pricing mechanism for controlling the time validity of a transaction. For example, if participants need more time to acquire sufficient capital through financing, they could stipulate a longer settlement time frame pending agreement between participants.

Contract Locks

[0102] Contract locks render the amount of cash and securities committed by both the buyer and seller untouchable on the respective ledgers pending settlement of the transaction between the parties. This prevents said assets from being used in another trade, hence removing the risk of payment and delivery defaults. The contract locks are in effect when counterparties commit to a transaction by sending instructions to the respective ledgers. The underlying assets will be locked and participants will be unable to use them in other transactions until the contracts are discharged when (i) the buyer and seller fulfilled their obligations by transferring the relevant asset (i.e. cash or securities, as the case may be) to another party or (ii) the contract expires due to the expiry of the time limit.

Account Controls

[0103] Counterparties are expected to fulfill 2-out-of-3-signatures condition at various points of the settlement process to advance towards settlement finality:

[0104] Buyer and seller will each hold their individual private keys.

[0105] Arbitrator will be provided with an escrow private key for safekeeping.

[0106] Participants engaged in a trade are subjected to the requirement that two of the three above mentioned authorised signatories must endorse the transaction in order for it to proceed to the next step. This also enables the arbitrator to be able to resolve disputes on the condition that either of the participants provides the first signature.

Self-Enforcing Smart Contracts

[0107] Self-executing smart contracts can automate processes and transactions, however for the purpose of ensuring investor protection and trade finality, self-executing smart contracts could pose an issue. Self-enforcing smart contract is contract between two or more parties that is enforced only by those stipulated two or more parties; an external party, which is not stipulated in the contract, cannot enforce the contract. In various embodiments, smart contracts that are self-enforcing are used. With the market operator also assuming the role of an arbitrator, buyers and sellers are rendered a greater degree of protection.

Secure OTPs (PDF)

[0108] Various embodiments mandate the creation of a temporary password, e.g. OTP, and its hash value, which may be a unique hash password, as a means to ensure DvP finality. In other words, both the buyer and seller *have* to use the same OTP to effect the asset transfer. This OTP may be generated by the independent entity or market operator but is not limited as such. This OTP is sent to each of the buyer and the seller in the form of an encrypted and password-protected PDF file at the start of post-trade settlement, and is used for the verification of instructions issued by counterparties till finality is reached.

[0109] In addition, the PDF file may allow cross-verification. If the file recipients are able to open the PDF file using their respective passwords, this means the PDF files have been sent to the correct seller and buyer. The seller and buyer may verify the identity of the file sender by verifying a digital signature and/or validity of a digital certificate which is embedded in the PDF files. This secure PDF file is sent off-chain and out-of-band, thus enhancing security for the market participants by being independent of the blockchain network as neither the OTP nor its hash needs to be stored on the blockchain.

Process flow of DvP-on-DLT

[0110] In some embodiments of the present invention process flow, the following takes place: Both the seller and the buyer of securities have agreed to the “asset type”, “asset amount”, “locking time” and Hash Password (**HashPwd**) to be exchanged. The agreement comprises two sets of asset transfers: (i) transfer of securities from seller to buyer within a specified time limit, e.g. 48 hours, and (ii) transfer of cash from buyer to seller within a specified time limit, e.g. 24 hours. Both seller and buyer have access to the distributed ledgers, e.g. securities ledger and cash ledger, where securities and cash are settled respectively and the flow of time of these networks is predictable by both counterparties.

[0111] Four scenarios where DvP is carried out in a DLT-enabled environment are possible:

Scenario 1: Settlement success

Scenario 2: Settlement failure with automatic recovery using smart contracts

Scenario 3: Failed transaction highlighting the need for arbitration

Scenario 4: Failed transaction introducing an arbitrator to the settlement process

[0112] Figure 4A is a flow chart which describes Scenario 1. The dash boxes indicate the entities performing the blocks or steps.

Scenario 1: Settlement success

[0113] In this scenario, settlement is successful as both buyer and seller fulfil their trade obligations in the following steps:

1. Counterparty matching – block 401

[0114] Buyers and sellers submit orders to the trading platform. The trading platform matches a buyer's bidding price for a security with a seller's asking price. It then notifies these two counterparties that it will initiate post-trade settlement based on the exchange of the agreed asset type and amount, along with the payment amount. On the other hand, at the distributed ledgers, e.g. cash ledger and securities ledger, which may be integrated or communicably coupled to the trading platform, one or more smart contracts are generated for this transaction to enforce the DvP settlement process thereof.

2. OTP and Hash Password generation – block 402

[0115] An independent entity (e.g. arbitrator) generates an **OTP (α)** and a Hash Password (**HashPwd = H(α)**) which is a hash value of the OTP and shares them with the seller via an

encrypted and password-protected file. Both the OTP and Hash Password will be used as a means to verify the instructions subsequently exchanged between the two counterparties in the settlement process.

5 **3. First Securities Instruction (Seller) – block 403**

[0116] Referencing the Hash Password, the seller creates a First Securities Instruction related to the transfer (delivery) of securities. In this instruction, the seller confirms the quantity of assets to be exchanged for the agreed price, and sets down the conditions for two possible end states (see Figure 4B).

10

[0117] The first end state (Tx1) sees the buyer granted the right to claim the seller's securities if (i) the buyer supplies the OTP that matches the Hash Password (contract-lock condition); and (ii) if one of the following conditions is satisfied: (a) both buyer and seller endorse this end state; or (b) either the buyer or seller, together with the arbitrator, endorses this end state. In other words, condition (i) and either condition (ii)(a) or (ii)(b) need to be satisfied.

15

[0118] The second end state (Tx2) sees the seller granted the right to have its securities returned if (i) the buyer fails to supply the OTP that matches the Hash Password within the specified time limit e.g. 48 hours (timeout condition); and (ii) if one of the following conditions is satisfied: (a) both buyer and seller endorse this end state; or (b) either the buyer or seller, along with the arbitrator, endorses this end state. In other words, condition (i) and either condition (ii)(a) or (ii)(b) need to be satisfied.

20

[0119] The seller then endorses the First Securities Instruction, e.g. using his electronic signature, and submits or posts it to the securities ledger.

25

4. Consensus (Securities Ledger) – block 404

[0120] The consensus mechanism of the securities ledger verifies and confirms the First Securities Instruction. It then posts the verification result to the securities ledger. At the same time, a Securities Contract Lock – a smart contract referencing the Hash Password – is posted to the securities ledger to safekeep or lock up the amount of securities required by the seller for the trade. With the securities set aside or safekept on the securities ledger, a default on delivery is prevented.

30

35

5. First Cash Instruction (Buyer) – block 405

[0121] After verifying the content of the First Securities Instruction submitted by the seller, the buyer creates the First Cash Instruction relating to the transfer (payment) of cash. In this instruction, the buyer sets down the conditions for two possible end states (see Figure 4B).

[0122] The first end state (Tx3) sees the seller granted the right to claim the buyer's cash if (i) the seller supplies the OTP that matches the Hash Password (contract-lock condition); and [(ii) both seller and buyer endorse this end state; or (iii) either the seller or buyer, along with the arbitrator, endorses this end state].

[0123] The second end state (Tx4) sees the buyer granted the right to have its cash returned if (i) the seller fails to supply the OTP that matches the Hash Password within a specified time limit, e.g. 24 hours (timeout condition); and (ii) if one of the following conditions is satisfied: (a) both seller and buyer endorse this end state; or (b) either the seller or buyer, along with the arbitrator, endorses this end state. In other words, condition (i) and either condition (ii)(a) or (ii)(b) need to be satisfied.

[0124] The buyer then endorses the First Cash Instruction, e.g. using its electronic signature, and submits or posts it to the cash ledger.

6. Consensus (Cash Ledger) – block 406

[0125] The consensus mechanism of the cash ledger verifies and confirms a First Cash Instruction. It then submits or posts the verification result to the cash ledger. At the same time, a Cash Contract Lock – a smart contract referencing the Hash Password – is posted to the cash ledger to safekeep or lock up the amount of cash required by the buyer for the trade. With the cash set aside or safekept on the cash ledger, a default on payment is prevented.

7. Second Cash Instruction – block 407

[0126] After verifying the contents of the First Cash Instruction of the buyer, the seller creates the Second Cash Instruction (claiming the agreed amount of cash) that reveals or includes the OTP. The seller then endorses this instruction (e.g. using his electronic signature) and submits or posts it to the cash ledger.

8. Payment complete – block 408

[0127] The consensus mechanism of the cash ledger verifies and confirms a Second Cash Instruction. It then updates or posts the verification result to the cash ledger. At this point, the cash contract is discharged, i.e. the cash contract lock is released and the seller receives the agreed amount of cash from the buyer. Payment is now complete. The transfer of cash from the buyer to the seller is posted to the cash ledger.

9. Second Securities Instruction – block 409

[0128] After the OTP supplied in the Second Cash Instruction of the seller is verified in block 408, the buyer creates a Second Securities Instruction (claiming the agreed quantity of securities) which includes the OTP. The buyer then endorses this instruction (electronic signature) and submits or posts it to the securities ledger.

10. Delivery complete – block 410

[0129] The consensus mechanism of the securities ledger verifies and confirms the Second Securities Instruction and the OTP. It then updates or posts the verification result to the securities ledger. At this point, the securities contract is discharged, i.e. the securities contract lock is released and the buyer receives the agreed quantity of securities from the seller. Delivery is now complete. The transfer of securities from the seller to the buyer is posted to the securities ledger.

Scenario 2: Settlement failure with auto recovery

[0130] Regardless of how technically faultless a trading platform may be, it is still susceptible to human error: settlement failure could occur if any of the steps previously described in Scenario 1 is not followed through.

[0131] For example, settlement could fail if the seller does not send the Second Cash Instruction (i.e. seller does not perform block 407) within a specified time limit, e.g. 24 hours. This results in inability of the seller to obtain or claim payment. Having received no instruction to verify and confirm, the buyer is unable to proceed with the Second Securities Instruction. Yet both the seller and buyer suffer no risk of losing their respective assets because the assets have not changed hands or transferred to the counterparty.

[0132] Through the use of smart contracts, the invention enables automatic recovery, e.g. posting a return instruction to the ledgers. The buyer, upon meeting the timeout condition of end state Tx4, is free to submit a cash instruction that will unlock and return the buyer's cash

to the cash ledger after a specified time limit, e.g. 24 hours. Similarly, the seller upon meeting the timeout condition of end state Tx2 is free to submit a securities instruction that will unlock and return the seller's securities to the securities ledger after a specified time limit, e.g. 48 hours.

5

Scenario 3: Settlement failure requiring arbitration

[0133] In this scenario, settlement could fail if the buyer fails to submit the Second Securities Instruction within the specified time limit, e.g. 48 hours. This results in inability of the buyer to obtain or claim the securities even after the payment is delivered, thereby exposing the buyer to principal risk and liquidity risk.

10

[0134] On the other hand, the seller has already discharged the cash contract and claimed the payment (end state Tx3). The securities contract is still valid for recovery for the committed securities (end state Tx2) – resulting in a lop-sided scenario, and a possible dispute between the counterparties. Arbitration is now required.

15

Scenario 4: Settlement failure with introduction of an arbitrator

[0135] In this scenario, settlement fails but arbitration is introduced to the settlement process. Here, the buyer is able to call on an arbitrator which may be the market operator like an Exchange to help (i) obtain the agreed quantity of securities from the seller, or (ii) recover the cash that has already been paid out to the seller.

20

[0136] To achieve (i), the arbitrator, together with the buyer or seller must endorse end state Tx1 (First Securities Instruction), to trigger the discharge of the smart contract and transfer of securities from seller to buyer. Alternatively, if (ii) is preferred, the arbitrator, together with the buyer or seller, must endorse end state Tx4 (Second Cash Instruction) to trigger the rightful return or recovery of cash from seller to buyer.

25

Assurance against account compromise

30

[0137] The requirement of obtaining at least two signatures or consents from the three parties involved (the 2-out-of-3 multi-signatures condition) functions as a useful account control. In a trade, no single participant can remove or steal the assets involved without the knowledge and endorsement of the other participant or the arbitrator. Hence, an arbitrator may resolve disputes by intercepting the transaction using an escrow private key.

35

[0138] For example, if the seller loses the device that is used to access the email account to which the OTP is sent, the assets cannot be stolen or removed by anyone in possession of the device (and OTP) without knowledge of the private keys held by the buyer or trading platform/arbitrator. Likewise, even if a non-trading member knows the individual private key(s) of the seller, buyer or trading platform/arbitrator, it cannot claim the assets involved without knowledge of the other participants' private keys and the OTP.

[0139] In addition to such conditional account controls, off-chain (this refers to a recording and validation method that works outside the realm of blockchain technology) and out-of-band contract locks safeguard OTPs using encrypted and password-protected files as defined by ISO 32000. These files may include an electronic signature with document lock(s) to further protect the files from being tampered, thereby strengthening investor confidence and enhancing the experience.

Arbitrator presence

[0140] With the growing prominence of blockchain technology, account and transaction security issues have risen to the forefront. Convenient as it may seem to blame rogue dealers for exploiting technology for unlawful gains, such losses often stem from the lack of due diligence in conducting background checks, a healthy scepticism and, most glaringly, an avenue for recourse should things go wrong.

[0141] Embodiments of the invention promote the introduction of an arbitrator presence to ensure transaction integrity and protection of the market participants. Indeed, having a regulatory authority in place to oversee the follow-through of transactions, remind dealers of their obligations to facilitate the meeting of deadlines, and to amicably resolve disputes should they arise (including instances of errant trading), serves to not only to assure participants, but also imbue confidence in the marketplace. This is especially important in instances of erroneous trades, such as fat-finger errors, which may cause extensive issues that have to be resolved by the financial intermediary (e.g. the stock exchange or platform operator).

Conventional Arbitration

[0142] Although it is true that arbitration can provide respite and closure for errors, one needs to be clear on what the process entails, as well as the possible implications of DLT on current practices. Some considerations include:

1. Deadlines

[0143] Currently, the Singapore Exchange Securities Trading Limited (**SGX-ST**)’s trading rules (**SGX-ST Trading Rules**) stipulate that where a buyer and seller cannot agree to the cancellation of an error trade, either of them may request SGX-ST to review the error trade and that “the matter must be referred to SGX-ST within sixty (60) minutes from the time the error trade occurred or before 18:00 hours on that trading day, whichever is earlier”. The requesting party must also separately inform its counterparty that it has referred the matter to SGX-ST. (The SGX-ST has the discretion to allow such extension of the aforesaid time frame as it deems appropriate.) With DLT, automated reminders encoded as smart contracts may instead be sent to the counterparties to aid them in safeguarding their interests.

2. Asset classes

[0144] Different asset classes are governed by different rules. In particular, under the SGX-ST Trading Rules, “SGX-ST will not review an error trade referred to it by a trading member, where the error trade falls at or within the upper and lower limits of a no-cancellation range”, and this rule is applied to the following instruments: (i) structured warrants; and (ii) all other securities and futures contracts excluding bonds. Here again, smart contracts can be employed to automatically determine if conditions are met, and to smoothen the arbitration process.

3. Costs

[0145] The SGX-ST Trading Rules state that “The requesting trading member must pay a trade review fee of \$1,000 for each referral accepted for review by SGX-ST, regardless of the outcome of the review”, unless a waiver is granted by SGX-ST. Administrative costs, no matter how small, can add up when one considers the loss of capital and liquidity that is incurred in parallel.

[0146] Proponents of DLT may not be supportive of a market regulator becoming a standard feature of trading markets, on the basis that it runs contrary to a “decentralised” system as there could be some arguments as to whether a network of distributed nodes (where each adheres to a common set of rules) amounts to a decentralised system or a centralised one. However, there are reasons supporting the view that systems built on DLT will always be centric in nature, even if without the installation of an arbitrator. On this note, a 2016 paper published by the European Central Bank on DLTs in securities post-trading concluded that

irrespective of the technology used and the market players involved, certain processes that feature in the post-trade market for securities will still need to be performed by institutions. This further substantiates the need for governance over blockchain applications in financial markets.

5

[0147] Implications of an arbitrator's presence in a DvP-on-DLT securities settlement model, and in particular how it enhances the settlement process, are elaborated below.

10 [0148] Figures 5A to 5F are sequence diagrams showing possible scenarios of the DvP according to embodiments of the invention.

15 [0149] Reference is made to Figure 5A which illustrates a DvP process in which settlement is successful. In block 501, various sellers and buyers register with an arbitration system (also referred to as independent entity), e.g. exchange, independent entity or arbitrator. During registration, each seller or buyer may provide or define one or more of the following: (i) his private password (also referred to as seller password and buyer password respectively), (ii) communication preferences or channels, e.g. electronic mail, messaging or other application, (iii) identifier and/or identification document. The aforementioned information is stored in one or more databases which may be provided at the arbitration system or in distributed databases

20 communicably coupled to the arbitration system.

[0150] In block 502, a seller (also referred to as a first entity) and a buyer (also referred to as a second entity) respectively execute their sell and buy requests using a platform which may be integrated with or communicably coupled to tokenised cash and securities ledgers. After the sell and buy requests are executed at the platform, a notification of a transaction between the seller and the buyer is sent to the arbitration system which may operate the ledgers. A receiving module of the arbitration system receives this notification which may include transaction details, identifiers of the seller and the buyer. On the other hand, at the distributed ledgers, one or more smart contracts are generated for the transaction. The smart contract may identify cash, securities and settlement time limit (stipulated by both the buyer and seller) which are required to complete DvP settlement of the transaction.

25

30

[0151] In block 503, after receiving the notification, the arbitration system generates a temporary password, e.g. one-time password (OTP), which is required to complete the transaction including DvP settlement process. The temporary password is encrypted before the encrypted password is electronically transmitted to the buyer and the seller. This generation and encryption of OTP may be performed by a processor (node) of the arbitration

35

system while this transmission may be performed by a transmission module of the arbitration system. In some embodiments, a first and a second encrypted Portable Document Format (PDF) file are generated and respectively transmitted to the seller and the buyer. Each of the two encrypted PDF files includes the (identical) temporary password and may further include a digital signature and/or digital certificate of the arbitration system. The first and the second encrypted PDF files are encrypted and decryptable by a password defined by the seller (seller password) and a password defined by the buyer (buyer password) respectively. More details of this temporary password generation are provided in the paragraphs below.

[0152] Also in block 503, the seller receives the first encrypted PDF file while the buyer receives the second encrypted PDF file.

[0153] In block 504, using the seller password, the seller opens the first encrypted PDF file to reveal the temporary password, e.g. OTP. Within a first specified time limit, the seller provides the temporary password to the ledgers, which may be sent together with Second Cash Instruction for posting to the cash ledger in block 407 of Figure 4A. On the other hand, using the buyer password, the buyer opens the second encrypted PDF to reveal the OTP. Within a second specified time limit, the buyer provides the OTP to the ledgers, which may be sent together with Second Securities Instruction for posting to the cash ledger in block 409 of Figure 4A.

[0154] In block 505, if within the settlement time limit, the aforementioned instructions from both buyer and seller are posted to the appropriate ledgers and OTPs provided by both buyer and seller are successfully verified, such as by verifying the OTP or a hash value of the OTP entered into or provided to the smart contract, the smart contract for settlement of the transaction is discharged to fulfil obligations. These may be ascertained and/or performed by one or more processors of the distributed ledgers.

[0155] In block 506, discharge of smart contracts may include releasing the securities contract lock and the cash contract lock; instructing a transfer of the cash from the buyer to the seller and instructing a transfer of the securities from the seller to the buyer; and updating the ledgers by posting the transfer of the cash and the transfer of the securities to the cash ledger and the securities ledger respectively. These may be performed by one or more processors of the distributed ledgers.

[0156] It is to be appreciated that, within block 505, if verification of the OTP provided by the seller and/or buyer is unsuccessful, one or more opportunities may be provided within the specified time limit(s) to allow for the re-provision and re-verification of the OTP.

5 [0157] Reference is made to Figure 5B which illustrates a DvP process in which seller disputes after a settlement time limit or boundary expires. Blocks 501, 502 and 503 of Figure 5B are similar to Figure 5A and therefore will not be described here.

10 [0158] In block 504B, using the seller password, the seller opens the first encrypted PDF to reveal the temporary password, e.g. OTP. Within a first specified time limit, the seller provides the OTP which may be sent together with Second Cash Instruction for posting to the cash ledger in block 407 of Figure 4A.

15 [0159] However, within specified time limits, the distributed ledgers failed to receive the OTP from the buyer, which may be sent together with Second Securities Instruction for posting to the securities ledger (see block 409 of Figure 4A). Consequently, in block 507B, after the settlement time limit expires, the seller initiates a dispute contract, e.g. by signing a dispute contract after which the signed dispute contract may be posted to the ledgers. Signing the dispute contract may include provision of the OTP by the seller. A transmission module of the
20 ledgers may send a notification of the dispute contract to the arbitration system.

[0160] In block 508B, the arbitration system receives a notification of the dispute contract. This notification may be received by a receiving module of the arbitration system. In order to discharge the dispute contract which is a smart contract, signatures from at least two of the
25 three parties involved are required. In this scenario, the 2- out-of-3 signature condition may be fulfilled by using a signature of the seller, e.g. verified OTP when signing the dispute contract, and a signature, e.g. private key, OTP or hash value of OTP, of the arbitrator. The arbitration system enters or provides the signature of the arbitrator to the dispute contract. If the 2-out-of-3 signatures condition is verified and fulfilled, a transmission module of the
30 arbitration system may send an instruction to the ledgers to discharge the dispute contract.

[0161] In block 509B, discharge of dispute contract may include releasing the securities contract lock; instructing a return of the securities to the seller; and updating the ledgers by posting the return of the securities to the securities ledger. These may be performed by one
35 or more processors of the distributed ledgers.

[0162] Reference is made to Figure 5C which illustrates a DvP process in which seller disputes before a settlement time boundary or limit expires. Blocks 501, 502 and 503 of Figure 5C are similar to Figure 5A and therefore will not be described here.

5 [0163] In block 507C, using the seller password, the seller opens the first encrypted PDF to reveal the temporary password, e.g. OTP. Before the settlement time limit expires, the seller initiates a dispute contract, e.g. by signing a dispute contract after which the signed dispute contract may be posted to the ledgers. Signing the dispute contract may include provision of a signature, e.g. the OTP, by the seller. A transmission module of the distributed ledgers may
10 send a notification of the dispute contract to the arbitration system.

[0164] In block 508C, the arbitration system receives a notification of the dispute contract from one of the distributed ledgers. This notification may be received by a receiving module of the arbitration system. In order to discharge the dispute contract which is a smart contract,
15 signatures from at least two of the parties involved are required. In this scenario, the 2-out-of-3 signatures condition may be fulfilled by using a signature of the seller, e.g. verified OTP password when signing the dispute contract, and a signature, e.g. private key, OTP or hash value of OTP, of the arbitrator. The arbitration system enters or provides the signature of the arbitrator to the dispute contract. If the 2-out-of-3 signatures condition is verified and fulfilled,
20 a transmission module of the arbitration system may send an instruction to the ledgers to discharge the dispute contract.

[0165] In block 509C, discharge of the dispute contract is similar to block 509B and will not be described here.

25 [0166] Reference is made to Figure 5D which illustrates a DvP process in which buyer disputes after a settlement time limit or boundary expires. Blocks 501, 502 and 503 of Figure 5D are similar to Figure 5A and therefore will not be described here.

30 [0167] In block 504D, using the buyer password, the buyer opens the second encrypted PDF to reveal the temporary password, e.g. OTP. Within a first specified time limit, the buyer provides the OTP to the ledgers, which may be sent together with Second Securities Instruction for posting to the cash ledger in block 409 of Figure 4A.

35 [0168] However, within specified time limits, the ledgers failed to receive the OTP from the seller, which may be sent together with Second Cash Instruction for posting to the cash ledger (see block 407 of Figure 4). Consequently, in block 507D, after the settlement time limit

expires, the buyer initiates a dispute contract, e.g. by signing a dispute contract after which the signed contract may be posted to the distributed ledgers. Signing the dispute contract may include provision of a signature, e.g. the OTP, by the buyer. A transmission module of the distributed ledgers may send a notification of the dispute contract to the arbitration system.

5

[0169] In block 508D, the arbitration system receives a notification of the dispute contract. This notification may be received by a receiving module of the arbitration system. In order to discharge the dispute contract which is a smart contract, signatures from at least two of the three parties involved are required. In this scenario, the 2-out-of-3 signatures condition may be fulfilled by using a signature of the buyer (e.g. verified OTP password when signing the dispute contract) and a signature (e.g. private key, OTP or hash value of OTP) of the arbitrator. The arbitration system enters or provides the signature of the arbitrator to the dispute contract. If the 2-out-of-3 signatures condition is verified and fulfilled, a transmission module of the arbitration system may send an instruction to the ledgers to discharge the dispute contract.

15

[0170] In block 509D, discharge of dispute contract may include releasing the cash contract lock; instructing a return of the cash to the buyer; and updating the ledgers by posting the return of the cash to the cash ledger. These may be performed by one or more processors of the cash ledger.

20

[0171] Reference is made to Figure 5E which illustrates a DvP process in which buyer disputes before a settlement time limit or boundary expires. Blocks 501, 502 and 503 of Figure 5E are similar to Figure 5A and therefore will not be described here.

25

[0172] In block 504E, using the buyer password, the buyer opens the second encrypted PDF to reveal the temporary password, e.g. OTP. Before the settlement time limit expires, the buyer initiates a dispute contract, e.g. by signing a dispute contract after which the signed dispute contract may then be posted to the ledgers. Signing the dispute contract may include provision of a signature, e.g. the OTP, by the buyer. A transmission module of the distributed ledgers may send a notification of the dispute contract to the arbitration system.

30

[0173] In block 508E, the arbitration system receives a notification of the dispute contract. This notification may be received by a receiving module of the arbitration system. In order to discharge the dispute contract which is a smart contract, signatures from at least two of the parties involved are required. In this scenario, the 2-out-of-3 signatures condition may be fulfilled by using a signature of the buyer (e.g. verified OTP password when signing the dispute contract) and a signature (e.g. private key, OTP or hash value of OTP) of the arbitrator. The

35

arbitration system enters or provides the signature of the arbitrator to the dispute contract. If the 2-out-of-3 signatures condition is verified and fulfilled, transmission module of the arbitration system may send an instruction to the ledgers to discharge the dispute contract.

5 [0174] In block 509E, discharge of dispute contract is similar to block 509D and will not be described here.

[0175] Reference is made to Figure 5F which illustrates a DvP process in which one of the private keys is compromised. Figure 5F incorporates blocks 501, 502, 503, 504, 505 and 506
10 and therefore settlement of the transaction is completed and smart contract for the transaction is discharged —these blocks are similar to Figure 5A and therefore will not be described here.

[0176] In block 510F, after completing the settlement and discharging the smart contract of the transaction, the arbitration system receives a “compromised key” notification from one of
15 the parties, e.g. the buyer, which may include a request to reverse the transaction. This request may be received by a receiving module of the arbitration system. In order to reverse the transaction, signatures from at least two of the three parties involved are required. In this scenario, this 2-out-of-3 signatures condition may be fulfilled by using a signature provided by a party other than the sender of the request to reverse the transaction, i.e. seller, after the
20 seller consents to the reversal of transaction, and a signature, e.g. private key, OTP or hash value of OTP, of the arbitrator. The arbitration system enters or provides the signature of the arbitrator to the smart contract for the transaction at the distributed ledgers. This may be performed by one or more processors and/or transmission module of the arbitration system. If the 2-out-of-3 signatures condition is verified and fulfilled, a notification is sent by the
25 arbitration system to the ledgers to reverse the smart contract for the transaction. This may be performed by one or more processors and/or transmission module of the arbitration system.

[0177] In block 510F, reversing transaction includes reversing the smart contract for the transaction. Reversal of smart contracts may include reversing the transfer of the cash (which
30 took place in block 506) by returning the cash from the seller to the buyer, and reversing the transfer of the securities (which took place in block 506) by returning the securities from the buyer to the seller; and updating the ledgers by posting the return of the cash and the return of the securities to the cash ledger and the securities ledger respectively. These may be performed by one or more processors of the cash ledger and the securities ledger.

35

[0178] It is to be appreciated that Figure 5F and related description are applicable, with suitable modifications, to a scenario where the compromised-key notification is transmitted by the seller, which may include a request to reverse the transaction.

5 [0179] Embodiments of the invention may be implemented by various architectures. A non-limiting example is illustrated in Figure 3B. As shown, each seller and buyer is configured to be communicably coupled with a trading engine or platform via its user interface (UI). The trading platform is configured to be communicably coupled with a custodian entity (wallet) which may hold tokenised cash and/or securities required for each transaction and on behalf
10 of the buyer and/or seller. The custodian entity is configured to be communicably coupled with the aforementioned arbitration system. The arbitration system is configured to be communicably coupled with the custodian entity and the distributed ledgers. The arbitration system may comprise: one or more non-transitory computer readable storage medium or non-volatile memories, a receiving module, a transmission module which are communicably
15 coupled to one or more processors for performing the above-described steps in relation to Figures 4A, 5A, 5B, 5C, 5D, 5E, and 5F. The non-transitory computer storage readable medium or non-volatile memories may comprise one or more databases for storing the passwords of the sellers and buyers and/or transaction details.

20 [0180] Separate distributed ledgers, e.g. cash ledger and securities ledger, are provided, which may be implemented as separate blockchains in a network and may be operated by the arbitrator. Each blockchain may be configured to process and record transactions as part of a block in the blockchain. Once a block is completed, the block is added or posted to the blockchain and thus the transaction record is updated into the blockchain. The blockchain may
25 be a ledger of transactions which are arranged in chronological order or any other order that may be suitable for use by the blockchain network. Each blockchain is communicably coupled with one or more mechanisms for issuance and settlement for transferring cash and/or securities.

30 [0181] At each of the cash ledger and securities ledger, one or more non-transitory computer readable storage medium or non-volatile memories, a receiving module, a transmission module may be communicably coupled to one or more processors for performing or implementing the above-described steps in relation to Figures 4A, 5A, 5B, 5C, 5D, 5E, and
35 5F.

Observations on the architecture

1. Rulebook integration

5 [0182] The current landscape of primary participants largely involves becoming a member of an Exchange, and having a set of rules to maintain the operations of a fair, orderly and transparent marketplace as determined by the Exchange. Smart contracts are use case agnostic to accommodate to many different logic conditions. The present invention allows for smart contracts to act as a replacement for compliance requirements due to the inherently
10 integrated rulebook. For example, having arbitration built into the smart contracts' conditions to validate the transfer instructions. Furthermore, error margins that define an error trade can be pre-programmed into the trade itself to prevent market participants from partaking in erroneous trades.

15 [0183] The present DvP has provided a proof-of-concept that smart contracts can be used to program and embed conventional rulebook conditions. This can result in significant implications in situations where a central bank or financial services institution may require enforcement on its members in multiple countries who are subjected to different degrees of regulation scrutiny and compliance standards.

20 [0184] One such application can be coupon payments associated with the underlying fixed income security, where it can be instituted with smart contracts to allow transactions on separate DLT implementation.

25 2. Compression of Settlement Cycles

[0185] In Singapore, the current market practice for securities settlement cycles is T+2 days, after the SGX-ST ported over to a new post trade system on 10 December 2018. Previously, the market practice for securities settlement cycle was T+3 days. In many parts of the world,
30 most securities settlement cycles are either T+2 days, T+3 days or more. Having a solution design that is built based on DLT for interledger operability helps to illustrate the potential of compressing the post-trade settlement process to T+1 or potentially even round-the-clock, real-time settlement.

35 Moving the industry forward to T+1 or real-time settlement may have many implications. For instance, with a shorter timeframe to settle, it will lower exposures to counterparty, principal and liquidity risks.

3. Arbitration Design for Interledger DvP

[0186] Interledger transactions involving cash and securities settlement give rise to principal risk exposure to the counterparties during specific segments of the process flow when the participants do not abide by the transaction sequence. Case in point, the instance where the buyer does not discharge the securities contract by withdrawing the securities before the specified time boundary expires, the seller can then expire the contract and recover the securities while having received the cash payment. There are additional scenarios which require arbitration:

- Error in the entry of the volume of an order
- Error in the entry of the price of an order
- Operational error (e.g. fat-finger trades)
- Where the arbitrator deems the transaction to be an error trade
- Where the participant's account is used to execute a trade after the participant has lost their private key
- Where the participant faced liquidity issues and does not have enough cash/assets for DvP settlement

[0187] Hence, it is necessary to appoint an arbitrator for the purpose of dispute resolution; and the present invention has shown possible options for the arbitrator to act on. The arbitrator can assess the circumstances of the disputed trade before making a determination on the possible recourse, e.g. (i) recovery of cash payment for the buyer or (ii) allowing the transaction to proceed by permitting the transfer of ownership of the underlying asset to the buyer and transfer of the cash to seller; or (iii) recovery of the underlying asset by the seller. This can be accomplished using smart contracts that are established at the beginning of the settlement cycle or upon the discharge of the cash contract (completing the payment).

[0188] Further work may be required to provide a robust arbitration framework. For example, during the arbitration period, the buyer may be exposed to liquidity risk if the seller has insufficient funds after the transaction reached finality. Possible solutions include providing safeguards in a contract requiring a buyer to have a minimum amount of cash reserves, or providing for a smart contract to be built on top of the cash payment to restrict fund movement.

4. Enhanced Security and Privacy

[0189] Embodiments of DvP according to the invention work for various types of platforms, including central limit order book (**CLOB**) or over the counter (**OTC**) request for quotes/auctions.

[0190] To maintain market competitiveness while complying with regulatory requirements, the identities of the participants of the trade should not be made known to one another, especially in the financial services industry where anonymity needs to be addressed. In our proposed DLT solution, an inclusion of a secure-PDF file containing the OTP is an important off-chain and out-of-band feature to ensure that investors' interests are protected.

(a) Verification of recipient

[0191] Investors are able to use the PDF file, that contains either a randomly encrypted address (i.e. a proxy for the public key) or the public key, to cross verify the identity of the file recipients with the execution platform (i.e. user interface) before agreeing to the asset transfers. If the file recipients are able to open the PDF file using their respective passwords, this means the PDF files have been sent to the correct seller and buyer. On the other hand, the seller and buyer may verify the identity of the file sender by verifying a digital signature and/or validity of a digital certificate which is embedded in the PDF files.

(b) OTP-sharing

[0192] The OTP used for the transaction is sent through an encrypted PDF file and independent of the blockchain network. By not using the blockchain or its network to store or propagate the OTP, one can ensure that the OTP is not made known to other participants in the network.

[0193] This is to ensure security and privacy are not compromised with an off-chain and out-of-band design. These includes remodelling the CLOB where the certificate authority keeps a record of its registered users, and uses it to generate a pseudo address that is used for transactional purposes without revealing the identity of a participant to other participants in the market. This will ensure that the participants' identities are kept anonymous as there will be a new address generated for each transaction.

[0194] In addition, in an OTC model, the buyer and seller would be able to review the counterparty similar to the existing market design. The same off-chain and out-of-band design can be applied to an OTC model too.

5 5. Market Structure

Round-the-clock operations

[0195] Building a solution design on DLT for interledger operability illustrates the potential of compressing the post-trade settlement process to T+1 or potentially even round-the-clock, real-time settlement. This can be further explored for cross-border transactions where time-zone differences could result in a delay in settlement times, thereby exposing participants to unnecessary foreign exchange rate fluctuations as well as principal and counterparty risks.

Merging of trading and settlement processes

[0196] The conventional models of trade order execution and post-trade settlement have been predominantly distinct processes, and an array of specific functionalities built for the purpose of counterparty matching or settlement have created a void of inefficiencies. By showing that smart contracts can be used as a tool for rulebook integration, the present invention has highlighted the possibility of converging these processes by applying a specific DLT solution design that utilises contract locks within multiple ledgers for cash and securities to safeguard investors' interests during and post trade.

[0197] Specifically, smart contracts for the transaction are created during the trade execution phase to ensure that both participants possess the necessary assets required to proceed with settlement. This would ensure that participants will be able to settle the obligations of the trades that are executed.

Broadening of suitable asset classes and markets

[0198] Embodiments of the invention could have implied use cases for other asset classes, such as securities, corporate and government bonds, commodities, and derivative products. The current market setup has different clearing houses for specific asset classes. For example, in Singapore, the Singapore Exchange Derivatives Clearing Limited (**SGX-DC**) is a clearing house for derivatives, while The Central Depository (Pte) Limited (**CDP**) acts as the clearing house for equities and fixed income. This distinction arose from the different underlying risks associated with the different asset classes.

[0199] Additionally, being able to tokenise assets and giving them a digital identity would enable illiquid assets (e.g. real estate, priced art pieces) to be traded outside of conventional means. By achieving interledger operability, DLT opens opportunities with potentially even cross-border trade settlement. With DLT, additional asset classes can be traded unconventionally and more markets can be connected, opening up liquidity and opportunities for investors globally. DLT is able to empower new business models for the financial services industry and revamp the existing primary and secondary market structures.

[0200] Figure 6 is a flowchart 600 illustrating a method for the generation and secured transmission of temporary password, which may be employed in the above-described DvP settlement process.

[0201] In block 601, a temporary password, e.g. OTP, is generated.

[0202] In block 602, a first and a second encrypted file are generated to be sent to a first entity, e.g. seller, and a second entity, e.g. buyer, respectively. The encrypted files may be generated as PDF files regardless of the application and platform used to create the file.

[0203] Each encrypted PDF file is embedded with the temporary password which is presented as two or more distinct encoded formats. Each encrypted PDF file may be further embedded with a digital signature and/or certificate of a third entity, e.g. arbitration system, which generated the PDF file. The encrypted PDF files received by the first entity and the second entity can be decrypted or unlocked respectively by the stipulated passwords, which the first entity and the second entity defined and registered with the arbitration system earlier on.

[0204] In block 603, the first and the second encrypted PDF file are electronically transmitted to the first entity and the second entity respectively.

[0205] Blocks 601, 602 and 603 may include the following steps or combinations thereof in various embodiments.

[0206] In block 601, generation of the temporary password may be performed by a processor of an independent or third entity, e.g. arbitration system, which is distinct from the first entity, e.g. seller, and the second entity, e.g. buyer. Generation of the temporary password may be

performed upon receipt of a notification of a transaction between the first entity and the second entity, or notification of other events. After receiving the notification, the third entity may retrieve the passwords (of buyer and seller), public keys (of buyer and seller), and the transaction details (to be used as the seed for key generation) of the first entity and the second entity from one or more databases which may be provided at the arbitration system and/or from distributed databases communicably coupled to the arbitration system.

[0207] In the database storing passwords of the buyer and the seller, the passwords may be protected by a Data Encryption Key (**DPK**) using an encryption algorithm including but not limited to Advanced Encryption Standard (**AES**) – AES-128, AES-192, AES-256, Triple Data Encryption Standard (**3DES**), Twofish and RSA algorithm. After which, the DPKs may be protected by a Key Encryption Key (**KEK**).

[0208] The transaction details or data may include at least one of the following: print or transaction date and time, name or legal name of seller and/or buyer, address of seller and/or buyer, reference code or number of the transaction, agreed quantity and price of securities for the transaction, agreed settlement period.

[0209] Password(s) and public keys of the first entity (seller) and the second entity (buyer) may also be retrieved from the database of the third entity or other databases to provide one or more seed(s) to generate the OTP. In addition, or alternatively, transaction details and private key, e.g. password, of the third entity may be retrieved from the database of the third entity or other databases to provide a seed to generate the OTP. Figure 7 shows one embodiment where passwords of the first entity and the second entity (i.e. the parties to the transaction), transaction details or data, and private key of the third entity are used as seeds to generate the temporary password. It is to be appreciated that any combination of password(s) of the first entity and/or the second entity, transaction details or data, private key of the arbitrator or arbitration system, and any other parameters may provide one or more seeds to generate the OTP.

[0210] In block 602, the temporary password may be embedded and presented in the form of a CAPTCHA code and a QR code. It is to be appreciated that other encoding formats are possible, e.g. variations of CAPTCHA or a barcode. Hence, in certain embodiments, the temporary password may be embedded and presented using at least two selected from the group consisting of CAPTCHA code, QR code and barcode. Further, the encoded formats

may include one which is human-readable (to prevent bot attacks) and another which is machine-readable.

[0211] The PDF files may be protected or encrypted by AES encryption algorithm, e.g. AES-128, AES-192 or AES-256.

[0212] The PDF files may be digitally signed by the private key, e.g. password, of the third entity which generated the PDF files. This digital signature, may be generated by a Secure Hash Algorithm-2 256 (SHA-2 256). Other hash algorithms such as the hash algorithms in the SHA-2 family (SHA-224 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256) and the SHA-3 family may alternatively be used. The digital signature may be embedded in the encrypted file, e.g. PDF file, in a digital certificate. This is for the recipient to verify the sender's identity. Public Key Cryptography Standards, e.g. PKCS12, may be used to embed the public key of the third entity into the PDF file.

[0213] Certificate Authority (CA) may be used to create the digital identity of the third entity i.e. the CA may generate public/private key pair of the third entity in a secure environment including but not limited to Hardware Security Module (**HSM**), Key Management Service (**KMS**) or Trusted Platform Module (**TPM**).

[0214] According to some embodiments, Figure 8 shows a schematic representation of an encrypted PDF file which is unlocked by a registered password to reveal the contents. Contents of the PDF file include the temporary password presented in two encoded formats, e.g. CAPTCHA and QR code, and a digital signature of the sender of encrypted PDF file.

[0215] In block 603, the PDFs are transmitted, e.g. in an out-of-band fashion to the first entity and the second entity via communication channels which are separate from the transaction platform or blockchain network, or via preferred communication channels pre-defined by the first entity and the second entity. The PDF files may be transferred through electronic mail, or messaging application, e.g. WhatsApp, Telegram, Bloomberg Chat, Symphony, WeChat, or SMS notification with Uniform Resource Locator (**URL**) which provides or allows access to the PDF file, or any combination thereof, and/or other electronic communication means to the respective entities. In the event the primary preferred communication channel fails (e.g., bounced email address or mobile number is unreachable), the PDF file may be re-routed to a secondary preferred communication channel.

[0216] The generated PDF files may be stored in a non-transitory computer readable storage medium or non-volatile memory of the third entity.

5 **Advantages of embodiments of the present invention**

1. Enhanced Security and Privacy

10 [0217] To maintain market competitiveness while complying with regulatory requirements, the identities of the participants of the trade should not be made known to one another, especially in the financial services industry where anonymity needs to be addressed. In embodiments of the DLT solution, an inclusion of a secure-PDF file containing the OTP is an important off-chain and out-of-band features to ensure that investors' interests are protected.

15 [0218] Investors are able to use the PDF file that contains either a randomly encrypted address (i.e. a proxy for the public key) or the public key to cross verify the recipient's identity with the execution platform (i.e. user interface) before agreeing to the transfer.

20 [0219] The OTP used for the transaction is sent through an encrypted PDF and independent of the blockchain network. By not using the blockchain or its network to store or propagate the OTP, one can ensure that the OTP is not made known to other participants in the network.

[0220] Secure random OTP which is seeded by details relating to the transaction and/or parties involved to ensure entropy (the lack of predictability).

25

[0221] OTP is presented in two or more distinct encoded formats, e.g. both a CAPTCHA code and a QR code, to prevent automated agent performing bot attacks (i.e. to be bot resistant).

30 [0222] Certificate authorities (PKCS12) and hash functions (SHA256) may be used to prevent man-in-the-middle attacks. The authenticity and provenance of the OTP could be determined by the digital signature. This prevents the forging of the identities of the respective parties.

[0223] A secondary device is not needed to receive the OTP; a device which is able to open PDF files is all that is required to receive the OTP.

35

[0224] The PDF file may be encrypted with AES256 to prevent eavesdropping attacks.

[0225] The PDF file may be generated and sent over to the respective parties immediately, instead of the long waiting time required to receive a mail which contains the OTP by post.

[0226] The process remodels the CLOB where the certificate authority keeps a record of its registered users, and using it to generate a pseudo address that is used for transactional purposes without revealing the identity of a participant to the other participants in the market. Alternatively, an OTC model can be adopted, where the buyer and seller are able to review the counterparty similar to the existing market design.

2. Operational efficiency

[0227] With distributed ledgers' ability to not only to ascertain a buyer's liquidity, but also to effect settlement on a trade-by-trade basis, the time and monetary costs associated with post-trade settlement could be solved with this process. Furthermore, DLT supports the use of smart contracts to automate or replace convoluted processes currently performed by clearing houses, back office systems and registries.

3. Mitigation of counterparty risks

[0228] Counterparty risks in DvP is mitigated by enabling recovery on cash and securities ledgers with the arbitrator and the use of contract locks to prevent said assets from being used in another trade.

4. Strengthening of investor confidence and an enhanced user experience

[0229] The invention, particularly the 2-out-of-3 signatures condition and arbitrator's presence, provides the safe and sound recovery of the compromised assets of the investor when they are compromised or lost.

[0230] The 2-out-of-3-signatures condition functions as a useful control. In a trade involving three participants (buyer, seller, trading platform), no single participant can remove or steal the assets involved without the knowledge and endorsement of another participant. An arbitrator may resolve disputes, e.g. by using an escrow private key to enable a transaction to proceed or reverse a transaction.

[0231] The arbitrator's presence ensures transaction integrity and protection of the market participants. The arbitrator will be able to oversee the follow-through of transactions, remind dealers of their obligations to facilitate the meeting of deadlines, and amicably resolve disputes should they arise (including instances of errant trading), and serves to not only to assure participants, but also to imbue investor confidence.

[0232] In Singapore, the current market practice surrounding settlement cycles is T+2. Having a solution design that is built based on DLT for interledger operability helps to illustrate the potential of compressing the post-trade settlement process to T+1 or potentially even round-the-clock, real-time settlement.

[0233] With a shorter timeframe to settle, it will lower exposures to counterparty, principal and liquidity risks.

[0234] Different aspects of the present invention may be used separately. However, the core PDF encryption method described in this application may be issued and signed by an independent third entity (e.g. arbitrator) with the proper authority to provide investors with assurance as to the authenticity of the communication.

[0235] In a compromised/ lost private key scenario, the arbitrator has to work with the counterparty to provide 2-out-of-3 signatures to reverse the trade for the victim. If the counterparty refuses to cooperate to reverse the trade, the arbitrator can "force reverse" the trade. This is not possible in the process outlined, however the trade can be "force reversed" through a 2-out-of-4 signatures condition, where the fourth party is the custodian.

[0236] The present invention may be applied to execute cross-border settlement of both payments and securities.

[0237] Whilst there has been described in the foregoing description preferred embodiments of the present invention, it will be understood by those skilled in the technology concerned that many variations or modifications in details of design or construction may be made without departing from the present invention.

Claims

1. A computer-implemented delivery versus payment (DvP) method comprising:

storing passwords and communication preferences defined by entities which include
5 a seller, a buyer and an independent entity;

in response to notification of a transaction between the seller and the buyer,
generating a temporary password which is configured to discharge a smart contract
generated at distributed ledgers for the transaction;

generating separate encrypted files which contain the temporary password and are
10 respectively decryptable by the stored passwords defined by the seller and the buyer; and

electronically transmitting, by the independent entity, the encrypted files to the seller
and the buyer respectively.

2. The computer-implemented DvP method of claim 1, wherein after electronically
transmitting, by the independent entity, the encrypted files to the seller and the buyer
15 respectively, the method further comprising:

receiving, from one of the distributed ledgers, notification of a dispute contract which
is initiated by a signature of the buyer or the seller; and

transmitting, by the independent entity, a signature of the independent entity to the
one of the distributed ledgers to provide one of two signatures required from at least two of
20 the group consisting of the seller, the buyer and the independent entity to discharge the
smart contract, wherein each signature includes the temporary password or a hash value
thereof.

3. The computer-implemented DvP method of claim 1, wherein after electronically
transmitting, by the independent entity, the encrypted files to the seller and the buyer
25 respectively, the method further comprising:

after the smart contract is discharged by the distributed ledgers,

receiving, from either the seller or the buyer, a request to reverse the
transaction;

receiving, from one of the seller and the buyer other than a sender of the
30 request, consent to the request;

transmitting, by the independent entity, a signature of the independent entity
to the distributed ledgers to provide one of two signatures required from at least two
of the group consisting of the seller, the buyer and the independent entity to reverse

the transfer of the cash and of the securities, wherein each signature includes the temporary password or a hash value thereof.

4. The computer-implemented DvP method of any one of claims 1 to 3, wherein the encrypted files include Portable Document Format (PDF) files.

5 5. The computer-implemented DvP method of any one of claims 1 to 4, wherein electronically transmitting, by the independent entity, the encrypted files to the seller and the buyer respectively includes transmitting the encrypted files via communication channels specified by the communication preferences of the seller and the buyer.

10 6. The computer-implemented DvP method of claim 5, wherein the communication channels include electronic mail or messaging application or Short Message Service (SMS) notification having a Uniform Resource Locator (URL) or any combination thereof.

7. The computer-implemented DvP method of any one of claims 1 to 6, wherein generating separate encrypted files which contain the temporary password and are respectively decryptable by the stored passwords defined by the seller and the buyer
15 includes embedding the temporary password as two or more distinct encoded formats and embedding a digital signature of the independent entity into each of the encrypted files.

8. The computer-implemented DvP method of claim 7, wherein the encoded formats include at least two selected from the group consisting of Completely Automated Public Turing Test To Tell Computers and Humans Apart (CAPTCHA) code, Quick Response (QR)
20 code and barcode.

9. The computer-implemented DvP method of any one of claims 1 to 8, wherein generating a temporary password which is configured to discharge a smart contract generated at distributed ledgers for the transaction includes generating the temporary password using at least one seed selected from the group consisting of the stored password
25 defined by the seller, the stored password defined by the buyer, a private key of the independent entity, and details of the transaction.

10. A delivery versus payment (DvP) system comprising:

one or more databases configured to store passwords and communication preferences defined by entities which include a seller, a buyer and an independent entity;

30 a receiving module of the independent entity, configured to receive notification of a transaction between the seller and the buyer;

a processor of the independent entity, configured to:

in response to the notification of the transaction between the seller and the buyer, generate a temporary password which is configured to discharge a smart contract generated at distributed ledgers for the transaction,

5 generate separate encrypted files which contain the temporary password and are respectively decryptable by the stored passwords defined by the seller and the buyer; and

10 a transmission module of the independent entity, configured to electronically transmit the encrypted files to the seller and the buyer respectively, wherein the one or more databases, the receiving module and the transmission module are communicably coupled to the processor.

11. The DvP system of claim 10, wherein the receiving module is further configured to receive, from one of the distributed ledgers, notification of a dispute contract which is initiated by a signature of the buyer or the seller; and

15 wherein the transmission module is further configured to transmit a signature of the independent entity to the one of the distributed ledgers to provide one of two signatures required from at least two of the group consisting of the seller, the buyer and the independent entity to discharge the smart contract, wherein each signature includes the temporary password or a hash value thereof.

12. The DvP system of claim 10, wherein after the smart contract is discharged by the distributed ledgers,

the receiving module is further configured to:

receive, from either the seller or the buyer, a request to reverse the transaction,

25 receive, from one of the seller and the buyer other than a sender of the request, consent to the request; and

30 the transmission module is further configured to transmit a signature of the independent entity to the distributed ledgers to provide one of two signatures required from at least two of the group consisting of the seller, the buyer and the independent entity to reverse the transfer of the cash and of the securities, wherein each signature includes the temporary password or a hash value thereof.

13. The DvP system of any one of claims 10 to 12, wherein the encrypted files include Portable Document Format (PDF) files.

14. The DvP system of any one of claims 10 to 13, wherein the transmission module is further configured to transmit the encrypted files via communication channels specified by the communication preferences of the seller and the buyer.

15. The DvP system of claim 14, wherein the communication channels include electronic mail or messaging application or Short Message Service (SMS) notification having a Uniform Resource Locator (URL) or any combination thereof.

16. The DvP system of any one of claims 10 to 15, wherein the processor is further configured to embed the temporary password as two or more distinct encoded formats and embed a digital signature of the independent entity into each of the encrypted files.

17. The DvP system of claim 16, wherein the encoded formats include at least two selected from the group consisting of Completely Automated Public Turing Test To Tell Computers and Humans Apart (CAPTCHA) code, Quick Response (QR) code and barcode.

18. The DvP system of any one of claims 10 to 17, wherein the processor is further configured to generate the temporary password using at least one seed selected from the group consisting of the stored password defined by the seller, the stored password defined by the buyer, a private key of the independent entity, and details of the transaction.

19. A computer-implemented delivery versus payment (DvP) method comprising:

in response to a transaction between a seller and a buyer, generating a smart contract for the transaction and notifying an independent entity to generate separate encrypted files which contain an identical temporary password and are respectively decryptable by passwords defined by the seller and the buyer, wherein the smart contract identifies cash, securities and a settlement time limit which are required to complete settlement of the transaction;

if the temporary password is separately received, by distributed ledgers comprising a cash ledger and a securities ledger, from the seller and the buyer within the settlement time limit, discharging the smart contract, including:

instructing a transfer of the cash to the seller,

instructing a transfer of the securities to the buyer,

posting the transfer of the cash to the cash ledger, and

posting the transfer of the securities to the securities ledger.

20. The computer-implemented DvP method of claim 19, wherein before discharging the smart contract, the method further comprising:

based on a first securities instruction from the seller, posting a securities contract lock to a securities ledger to safekeep the securities;

5 based on a first cash instruction from the buyer, posting a cash contract lock at a cash ledger to safekeep the cash;

upon receiving the temporary password from the seller within a first time limit, posting a cash claim instruction at the cash ledger to claim the cash; and

10 upon receiving the temporary password from the buyer within a second time limit, posting a securities claim instruction at the securities ledger to claim the securities, and

wherein discharging the smart contract includes releasing the securities contract lock and releasing the cash contract lock.

21. The computer-implemented DvP method of any one of claims 19 to 20, wherein after posting the transfer of the cash to the cash ledger, and posting the transfer of the securities to the securities ledger, the method further comprising:

receiving a request to reverse transaction;

if at least two signatures are received from at least two of the group consisting of the seller, the buyer and the independent entity,

20 instructing a return of the cash to the buyer,

instructing a return of the securities to the seller,

posting the return of the cash to the cash ledger, and

posting the return of the securities to the securities ledger.

22. The computer-implemented DvP method of claim 19, further comprising:

if the temporary password is not received, by the distributed ledgers, from both the seller and the buyer within the settlement time limit and if a return instruction is received by the distributed ledgers, discharging the smart contract, including:

instructing a return of the cash to the buyer,

30 instructing a return of the securities to the seller,

posting the return of the cash to the cash ledger, and

posting the return of the securities to the securities ledger.

23. The computer-implemented DvP method of claim 22, wherein before discharging the smart contract, if the temporary password is not received, by the distributed ledgers, from both the seller and the buyer within the settlement time limit and if a return instruction is received by the distributed ledgers, the method further comprising:

- 5 based on a first securities instruction from the seller, posting a securities contract lock at a securities ledger to safekeep the securities;
- based on a first cash instruction from the buyer, posting a cash contract lock at a cash ledger to safekeep the cash;
- upon receiving the temporary password from the seller, posting a cash claim
- 10 instruction at the cash ledger to claim the cash; and
- failing to receive the temporary password from the buyer within the settlement time limit.

24. The computer-implemented DvP method of claim 19, further comprising:

- 15 if the temporary password is received, by the distributed ledgers, from either the seller or the buyer within the settlement time limit and if a signed dispute contract is received, by the distributed ledgers, from either the seller or the buyer, notifying the independent entity and receiving a signature from the independent entity, and
- if at least two signatures are received from at least two of the group consisting
- 20 of the seller, the buyer and the independent entity, discharging the smart contract including:
- instructing a return of the cash to the buyer and/or instructing a return of the securities to the seller, posting the return of the cash to the cash ledger and/or posting the return of the securities to the securities ledger, wherein
- 25 each signature includes the temporary password or a hash value thereof.

25. The computer-implemented DvP method of claim 24, wherein before notifying the independent entity and receiving a signature from the independent entity, the method further comprising:

- based on a first securities instruction from the seller, posting a securities contract
- 30 lock at a securities ledger to safekeep the securities;
- based on a first cash instruction from the buyer, posting a cash contract lock at a cash ledger to safekeep the cash;

upon receiving the temporary password from the seller, posting a cash claim instruction at the cash ledger to claim the cash; and

failing to receive the temporary password from the buyer within the settlement time limit.

5 26. The computer-implemented DvP method of any one of claims 19 to 25, wherein each of the cash ledger and the securities ledger includes a blockchain.

27. The computer-implemented DvP method of any one of claims 19 to 26, wherein the encrypted files include Portable Document Format (PDF) files.

10 28. The computer-implemented DvP method of claim 27, wherein the temporary password is embedded in each of the PDF files as two or more distinct encoded formats.

29. The computer-implemented DvP method of claim 28, wherein the encoded formats include at least two selected from the group consisting of Completely Automated Public Turing Test To Tell Computers and Humans Apart (CAPTCHA) code, Quick Response (QR) code and barcode.

15 30. A method for generation and secured transmission of temporary password, the method comprising:

generating a temporary password;

20 generating a first and a second encrypted Portable Document Format (PDF) file which are respectively decryptable by a first password defined by a first entity and a second password defined by a second entity, wherein each PDF file is embedded with the temporary password as two or more distinct encoded formats and further embedded with a digital signature and/or certificate of a third entity; and

electronically transmitting the first and the second encrypted PDF document to the first and the second entity respectively.

25 31. The method of claim 30,

wherein generating the temporary password is performed by the third entity in response to a notification of a transaction between the first entity and the second entity.

32. The method of claim 31,

30 wherein generating a first and a second encrypted PDF file includes generating the digital signature using a password of the third entity and a cryptographic hash function; and embedding the digital signature and/or the digital certificate into each of the PDF documents.

33. The method of any one of claims 31 to 32,

wherein generating the temporary password includes generating the temporary password using at least one seed selected from the group consisting of the first password, the second password, a private key of the third entity, and details from the transaction.

5 34. The method of claim 33,

wherein the details from the transaction includes at least one selected from the group consisting of date and/or time of the transaction, name of the first and/or the second entity, address of the first and/or the second entity, reference code of the transaction, agreed quantity and price of securities for the transaction, agreed settlement period.

10 35. The method of any one of claims 30 to 34,

wherein electronically transmitting the first and the second encrypted PDF document to the first and the second entity respectively includes electronically transmitting the first and the second encrypted PDF document, by a communication channel which is separate from a platform facilitating the transaction, to the first and the second entity respectively.

15 36. The method of any one of claims 30 to 35,

wherein electronically transmitting the first and the second encrypted PDF document to the first and the second entity respectively includes electronically transmitting the first and the second encrypted PDF document, by electronic mail or messaging application or Short Message Service (SMS) notification having a Uniform Resource Locator (URL) or any
20 combination thereof, to the first and the second entity respectively.

37. The method of any one of claims 30 to 36, wherein the encoded formats include at least two selected from the group consisting of Completely Automated Public Turing Test To Tell Computers and Humans Apart (CAPTCHA) code, Quick Response (QR) code and barcode.

25 38. A non-transitory computer readable storage medium comprising:

a first and a second encrypted Portable Document Format (PDF) document which are respectively decryptable by a first password defined by a first entity and a second password defined by a second entity, wherein each PDF document comprises:

30 a temporary password embedded in the PDF document as two or more distinct encoded formats; and

a digital signature and/or certificate of a third entity which generated the PDF document.

39. The computer readable storage medium of claim 38, wherein the encoded formats include at least two selected from the group consisting of Completely Automated Public Turing Test To Tell Computers and Humans Apart (CAPTCHA) code, Quick Response (QR) code and barcode.

5 40. The computer readable storage medium of any one of claims 38 to 39, wherein the temporary password is generated using at least one seed selected from the group consisting of the first password, the second password, a private key of the third party, and details from the transaction.

41. The computer readable storage medium of claim 40,

10 wherein the details from the transaction includes at least one selected from the group consisting of date and/or time of the transaction, name of the first and/or the second entity, address of the first and/or the second entity, reference code of the transaction, agreed quantity and price of securities for the transaction, agreed settlement period.

15

20

25