Claims

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

storing, at one or more databases of an independent entity, passwords and communication preferences defined by entities which include a seller, a buyer and the independent entity;

in response to notification of a transaction between the seller and the buyer, generating, by the independent entity, a temporary password which is configured to be provided by the seller and the buyer to distributed ledgers associated with the transaction to discharge a smart contract generated at the distributed ledgers;

generating, by the independent entity, separate encrypted files which contain the temporary password 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.

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 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 the group consisting of the seller, the buyer and the independent entity to discharge the smart contact, 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 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 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. 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.

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 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) 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 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 of an independent entity, configured to store passwords and communication preferences defined by entities which include a seller, a buyer and the 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 be provided by the seller and the buyer to distributed ledgers associated with the transaction to discharge a smart contract generated at the distributed ledgers,

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.

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

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 contact, 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,

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.

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, by distributed ledgers, 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 generated by the independent entity is separately received, by the 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;

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.

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,

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,

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:

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 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:

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 of the seller, the buyer and the independent entity, discharging the smart contact 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 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 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.

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.

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.

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

generating a temporary password;

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, 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.

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,

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.

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.

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.

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 combination thereof, to the first and the second entity respectively.

37. 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:

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, 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.

38. The computer readable storage medium of claim 37, 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.

39. The computer readable storage medium of claim 38,

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.