PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/IB2018/056734	04.09.2018	08.09.2017

International Patent Classification (IPC) or both national classification and IPC
INV. H04L9/32

Applicant
NCHAIN HOLDINGS LIMITED

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☒ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Spranger, Stephanie Telephone No. +49 89 2399-0

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IB2018/056734

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:

   a. ☐ forming part of the international application as filed:

      ☐ in the form of an Annex C/ST.25 text file.

      ☐ on paper or in the form of an image file.

   b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. ☐ furnished subsequent to the international filing date for the purposes of international search only:

      ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	11, 12, 15
	No:	Claims	1-10, 13, 14, 16, 17
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-17
Industrial applicability (IA)	Yes:	Claims	1-17
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following documents:

D1 MCCORRY PATRICK ET AL: "Towards Bitcoin Payment Networks", 30 June 2016 (2016-06-30), ECCV 2016 CONFERENCE; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 57 - 76, XP047348067, ISSN: 0302-9743 ISBN: 978-3-319-69952-3 [retrieved on 2016-06-30]

D2 Bitfury Group: "Smart Contracts on Bitcoin Blockchain", 4 September 2015 (2015-09-04), XP055382678, Retrieved from the Internet: URL:http://bitfury.com/content/5-white-papers-research/contracts-1.1.1.pdf [retrieved on 2017-06-19]

2 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims 1, 13, 14, 16 and 17 is not new.

2.1 Document D1 discloses (reference to D1 is made in parenthesis):

A method to secure or unlock an output, UTXO *("transaction comprising output")*, in a blockchain transaction, TXo *("transaction") (sec. 2, 3, 4, figs. 4, 5, 6)*, comprising:
using a time lock mechanism *("lock time")* to control or influence when the output, UTXO, can be unlocked *(sec.4)*;
wherein the time lock mechanism uses a value, $T_{Suppllied}$, that is generated as the result of a calculation which uses an input, A, that is supplied by a source external to the transaction TXo *("off-blockchain also referred to as micropayment channel network") (sec. 4: "The initial sender commits bitcoins in a payment channel shared with their PSP under the condition that the pre-image R is revealed within k blocks." with implementations in duplex micropayment channels and lightning channels)*.

2.2 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claims 13, 14, 16 and 17, which therefore are also considered not new.

3 Dependent claims 2-11 and 15 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty and/or inventive step.

3.1 Claims 2, 8 and 9: off-chain transactions in payment channel and D1, sec. 2.1 "Coins are transferred via transactions which have one or more inputs and one or more outputs. Each output specifies the number of bitcoins sent and the scriptprogram, whereas each input provides a reference to a previous transaction's output and the redeem script (i.e. "locking script") (e.g., a corresponding signature) that satisfies the output's spending conditions. Transactions cannot send more bitcoins than provided in the inputs, and there are no rules on how the bitcoins are split amongst the outputs."

3.2 Claim 3: D1, sec. 2.1 "Absolute Lock Time ensures an entire transaction or a child transaction that is spending an output of a parent transaction cannot be accepted into the Blockchain until a specified absolute block height k (or time) in the future. Relative Lock Time ensures a child transaction that is spending an output of a parent transaction cannot be accepted into the Blockchain until the parent transaction has achieved a relative depth of λ blocks."

3.3 Claims 4 and 5: D1, hash(R).

3.4 Claims 6 and 7: D1, sec. 2.2 absolute and and relative lock times of the Bitcoin payment network.

3.5 Claim 10: D1, fig. 5 and 6, invalidation tree according to the lock time mechanism and commitment transaction.

3.6 Claims 11, 12 and 15: obvious form the time lock mechanisms implemented with Bitcoin payment networks.

Re Item VII

Certain defects in the international application

4 The features of the claims are not provided with reference signs placed in parentheses to increase the intelligibility of the claims (Rule 6.2(b) PCT).

5 The most relevant prior art documents D1 and D2 are not identified in the description and the description is not adapted to the independent claims (Rule 5.1(a)(ii)(iii) PCT).

Re Item VIII

Certain observations on the international application

6 The application does not meet the requirements of Article 6 PCT, because claims 6, 9, 10, 11, 13 and 14 are not clear.

6.1 The acronyms in claims 6 and 14 are not defined.

6.2 An antecedence of "input A" and "value Tsupplied" in claims 9 and 11 is not defined. Hence, it is not clear whether the same input and value referred to in claim 1 is meant.

6.3 In the formulation of "functionally similar/equivalent" in claim 14 it is not clear how the functionality of the time lock mechanism is related to an existing one.

7 Although claims 1, 13, and 14 have been drafted as separate independent claims in the same category (method), they appear to relate effectively to the same subject-matter and to differ from each other only with regard to the definition of the subject-matter for which protection is sought and/or in respect of the terminology used for the features of that subject-matter. The aforementioned claims therefore lack conciseness and as such do not meet the requirements of Article 6 PCT.