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/IB2018/055604	26.07.2018	15.08.2017

International Patent Classification (IPC) or both national classification and IPC
INV. H04L9/08 H04L9/30 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	Bec, Thierry Telephone No. +49 89 2399-0

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IB2018/055604

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	2-4
	No:	Claims	1, 5-34
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-34
Industrial applicability (IA)	Yes:	Claims	1-34
	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

1 **Re Item V**

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

1.1 Reference is made to the following documents:

D1	DIKSHIT PRATYUSH ET AL: "Efficient weighted threshold ECDSA for securing bitcoin wallet", 2017 ISEA ASIA SECURITY AND PRIVACY (ISEASP), IEEE, 29 January 2017 (2017-01-29), pages 1-9, XP033117504, DOI: 10.1109/ISEASP.2017.7976994
D2	IBRAHIM M H ET AL: "A robust threshold elliptic curve digital signature providing a new verifiable secret sharing scheme", MIDWEST SYMPOSIUM ON CIRCUITS AND SYSTEMS. CAIRO, EGYPT, DEC. 27 - 30, 2003; [MIDWEST SYMPOSIUM ON CIRCUITS AND SYSTEMS], PISCATAWAY, NJ, IEEE, US, vol. 1, 27 December 2003 (2003-12-27), pages 276-280, XP010867444, DOI: 10.1109/MWSCAS.2003.1562272 ISBN: 978-0-7803-8294-7
D3	VOLKER MÜLLER: "A SHORT NOTE ON SECRET SHARING USING ELLIPTIC CURVES :", SECRYPT 2008. PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON SECURITY AND CRYPTOGRAPHY : PORTO, PORTUGAL, JULY 26 - 29, 2008, 1 January 2008 (2008-01-01), pages 359-362, XP055471217, DOI: 10.5220/0001918303590362 ISBN: 978-989-8111-59-3
D4	Steven Goldfeder ET AL: "We Securing Bitcoin wallets via threshold signatures", , 3 June 2014 (2014-06-03), XP055326412, Retrieved from the Internet:

URL:http://www.cs.princeton.edu/~stevenag/bitcoin_threshold_signatures.pdf
[retrieved on 2016-12-06]

D5 GUY ZYSKIND ET AL: "Decentralizing Privacy: Using Blockchain to Protect Personal Data", THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC. (IEEE) CONFERENCE PROCEEDINGS, 1 May 2015 (2015-05-01), page 180, XP055360065, Piscataway

D6 BINU V P ET AL: "Threshold Multi Secret Sharing Using Elliptic Curve and Pairing", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 31 March 2016 (2016-03-31), XP080807612,

D7 MICHAEL BACKES ET AL: "Asynchronous MPC with t", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20140217:075007, 17 February 2014 (2014-02-17), pages 1-33, XP061015387,

D8 KATE A ET AL: "Distributed Key Generation for the Internet", DISTRIBUTED COMPUTING SYSTEMS, 2009. ICDCS '09. 29TH IEEE INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 22 June 2009 (2009-06-22), pages 119-128, XP031485519, ISBN: 978-0-7695-3659-0

D9 SYTA EWA ET AL: "Keeping Authorities "Honest or Bust" with Decentralized Witness Cosigning", 2016 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (SP), IEEE, 22 May 2016 (2016-05-22), pages 526-545, XP032945718, DOI: 10.1109/SP.2016.38

1.2 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claim 1 is not new.

D1 discloses:

Claim 1	D1
A method of digitally signing a digital message by means of a private key of a public-private key pair of a cryptography system, to provide a digital signature which can be verified by means of a public key of the public-private key pair, the method comprising:	Paragraph IV "our proposed scheme" page 7 and signature generation page 8 left hand column
receiving at least a threshold number of partial signatures of said digital message, wherein each said partial signature includes a respective first part based on the message and a respective second part based on a respective share of the private key, wherein the private key is accessible to said threshold number of shares of the private key and is inaccessible to less than said threshold number of shares, wherein each said partial signature corresponds to a respective value of a first polynomial function such that the first polynomial function is accessible to said threshold number of partial signatures and is inaccessible to less than said threshold number of partial signatures; and	See page 8 left hand column points 3) and 5)-6) and 9)-10)
determining said first polynomial function, by means of determining coefficients of the first polynomial	See page 8 "second part of the signature "right hand column points 2)-5)

function from a plurality of known values of said partial signatures, to effect digital signature of the message.	
determining and revealing a second signature component share based on the message, the private key share, the first signature component, the ephemeral key share, masked by the second additive mask share,	See page 8 "second part of the signature "right hand column point 5)

Therefore the subject-matter of independent claim 1 is not new over D1 (Article 33(1) and (2) PCT).

1.3 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claim is not new.

D1 discloses:

Claim 5	D1
A method of digitally signing a digital message by means of a private key of a public-private key pair of a cryptography system, to provide a digital signature which can be verified by means of a public key of the public-private key pair, the method comprising:	Paragraph IV "our proposed scheme" pages 7-8 and signature generation page 8 left hand column
receiving at least a threshold number of partial signatures of said digital message, wherein each said partial signature includes a respective first part	See page 8 left hand column points 9)-10)

based on the message, a respective second part based on a respective share of the private key,	
wherein the private key is accessible to said threshold number of shares of the private key and is inaccessible to less than said threshold number of shares, and a respective third part corresponding to a respective value of a third polynomial function having a zero constant term,	See page 8 "second part of the signature "right hand column points 5)-6)
wherein the third polynomial function is accessible to said threshold number of shares of the third polynomial function and is inaccessible to less than said threshold number of shares, and wherein each said partial signature corresponds to a respective value of a fourth polynomial function such that the fourth polynomial function is accessible to said threshold number of partial signatures and is inaccessible to less than said threshold number of partial signatures; and	See page 8 "second part of the signature "right hand column points 4)-5)
determining the fourth polynomial function to effect digital signature of the message.	See page 8 "second part of the signature "right hand column point 7)

It is further noticed that in claim 5 a first and a second polynomial have not been defined, thereby leading to a lack of clarity. In this case the third and fourth polynomial can be interpreted as a first and a second polynomial.

Therefore the subject-matter of independent claim 5 is not new over D1 (Article 33(1) and (2) PCT).

1.4 Dependent claims 2-17 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, see

Preliminary remark: it is noted that in a secret sharing scheme, the number of participant is unlimited, therefore the number of polynomial associated as well. Since the applicant does not define to which element the polynomials are referring to the interpretation has been made that a polynomial relates to a user.

For claims 2 to 4 see in combination with D2 §VII.

For claims 6, 7 see D1 page 8.

For claim 8, 33 see D1 title.

For claim 9, 15 by definition of the secret sharing e.g. see §III.

For claims 10-12 as an implementation details.

For claims 13,14, 17-32 see Paragraph IV "our proposed scheme" pages 7-8.

For claim 16, 21 see preliminary remark.

For claim 34 as the program implementing the methods claim of claims 1-33.

2 **Re Item VII**

Certain defects in the international application

2.1 Independent claims 1 and 5 are not in the two-part form in accordance with Rule 6.3(b) PCT, which in the present case would be appropriate, with those features known in combination from the prior art D1 being placed in the preamble (Rule 6.3(b)(i) PCT) and the remaining features being included in the characterising part (Rule 6.3(b)(ii) PCT).

2.2 The features of claims 1-34 are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).

2.3 Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in D1 to D9 is not mentioned in the description, nor are these documents identified therein.

3 **Re Item VIII**

Certain observations on the international application

3.1 Although claims 1 and 5 have been drafted as separate independent claims, 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.

The reasons being as follows.

As it can be seen from below, claim 5 only defines a further third and fourth polynomial instead of a first polynomial. Therefore the scope of claim 5 is included into the scope of claim 1 thus, claim 5 should be dependent on claim 1.

"A method of digitally signing a digital message by means of a private key of a public-private key pair of a cryptography system, to provide a digital signature which can be verified by means of a public key of the public-private key pair, the method comprising:
receiving at least a threshold number of partial signatures of said digital message,-
wherein each said partial signature includes a respective first part based on the ~~message and~~ message, a respective second part based on a respective share of the private key,-
wherein the private key is accessible to said threshold number of shares of the private key and is inaccessible to less than said threshold number of shares, ~~wherein each said partial signature corresponds~~ and a respective third part corresponding to a respective value of a ~~first~~ third polynomial function ~~such that~~ having a zero constant term, wherein the ~~first~~ third polynomial function is accessible to said threshold number of ~~partial signatures~~ shares of the third polynomial function and is inaccessible to less

than said threshold number of shares, and wherein each said partial ~~signatures; and~~signature corresponds ~~determining said first polynomial function, by means~~ to a respective value of ~~determining coefficients of~~ a fourth polynomial function such that the ~~first~~ fourth polynomial function ~~from a plurality of known values~~ is accessible to said threshold number of partial signatures and is inaccessible to less than said threshold number of partial ~~signatures,~~ signatures; and determining the fourth polynomial function to effect digital signature of the message."