Patents Act 1977 **Opinion Number** **18/21**

OPINION UNDER SECTION 74A

Patent	EP 3465578
Proprietor(s)	NChain Holdings Limited
Exclusive Licensee	-
Requester	Barker Brettell LLP
Observer(s)	UDL Intellectual Property
Date Opinion issued	17 November 2021

The request

1. The comptroller has been requested to issue an opinion as to whether EP 3465578, the patent, is valid by Barker Brettell LLP. In their letter, Barker Brettell LLP suggest that they represent the Open Crypto Foundation but have filed this request in their own name.

2. The request provides three pieces of prior art, in order to suggest that claims 1, 10 and 19 are either not novel or not inventive. Copies of the following documents were provided with the request:

    - Galindo et al.: “A Killer Application for Pairings: Authenticated Key Establishment in Underwater Wireless Sensor Networks”, Proceedings of the 7th International Conference on Cryptology and Network Security (CANS08), LNCS vol. 5339, pp. 120- 132, 2008.

    - Boneh & Franklin: “Identity-Base Encryption from the Weil Pairing”, SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003.

    - Nakamoto: “Bitcoin: A Peer-to-Peer Electronic Cash System”, referred to on the Cryptography Mailing List “Bitcoin P2P e-cash paper” 1 November 2008.

3. Observations have been filed by UDL Intellectual Property who represented NChain Holding Limited on this application. Observations in reply were then filed by Barker Brettell LLP.

The Patent

4. The Patent was filed on 4 June 2018 and granted on 24 July 2019 and is currently in force. The Patent relates to a method or apparatus, of node to node trusted

communication. In the main embodiment that is applied to a blockchain or distributed ledger, allowing consensus to be used to maintain a trusted record of transactions, such as Bitcoin within the ledger. However, claim 1 does not state that it relates to a blockchain.

5. The Patent describes the nature of decentralised peer-to-peer systems means that a node may not be able to communicate with another node in the network on a trusted basis. That is a result of the design decision in implementing a blockchain to create trust in a ledger through a consensus mechanism. The Patent therefore proposes a way to ensure that trusted communication between nodes can be achieved using group private keys, associated with a group of nodes.

6. There are three claims in question here, the two independent claims, and a dependent claim to a storage medium with the relevant program for claim 1, which is then executed. In practice, claim 19 adds no significant restriction, and it will stand or fall with claim 1. I have highlighted one part of the claim, as this is where most of the argument will later focus.

> *Claim 1: A computer-implemented method for a first node (102) to establish a trusted communication with a second node (102),*
> *the second node having a second node identifier and a second secret point, the second secret point being a group private key times a map-to-point hash of the second node identifier,*
> ***the group private key being associated with a group of nodes (100) configured to grant credentials,***
> *the method comprising:*
> *obtaining a first secret point from the group of nodes, wherein the first secret point is the group private key times a map-to-point hash of a first node identifier;*
> *sending the first node identifier to the second node;*
> *receiving the second node identifier;*
> *generating a first session key using a bilinear pairing operation with a map-to-point hash of the second node identifier and with the first secret point; and*
> *confirming that the first session key matches a second session key generated by the second node using the bilinear pairing operation with the second secret point and with a map-to-point hash of the first node identifier*
>
> *10. A first node (102) comprising:*
> *a processor;*
> *memory;*
> *a network interface; and*
> *a blockchain application containing processor-executable instructions to establish a trusted communication with a second node (102), the second node having a second node identifier and a second secret point, the second secret point being a group private key times a map-to-point hash of the second node identifier,* ***the group private key being associated with a group of nodes (100) configured to grant credentials,*** *wherein, when executed, the processor-executable instructions cause the first node to:*
> *obtain a first secret point from the group of nodes, wherein the first secret point is the group private key times a map-to-point hash of a first node*

identifier;
send the first node identifier to the second node;
receive the second node identifier;
generate a first session key using a bilinear pairing operation with a map-to-point hash of the second node identifier and with the first secret point; and confirm that the first session key matches a second session key generated by the second node using the bilinear pairing operation with the second secret point and with a map-to-point hash of the first node identifier.

19. A non-transitory processor-readable medium storing processor-executable instructions that, when executed by one or more processors, cause the one or more processors to carry out the operations in the method claimed in any one of claims 1 to 9.

Claim construction

7. Before I can determine an opinion as to the validity and infringement of the patent, I must first construe the claims. This means interpreting the claims in light of the description and drawings as instructed by section 125(1) of the Patents Act: For the purposes of this Act an invention for a patent for which an application has been made or for which a patent has been granted shall, unless the context otherwise requires, be taken to be that specified in a claim of the specification of the application or patent, as the case may be, as interpreted by the description and any drawings contained in that specification, and the extent of the protection conferred by a patent or application for a patent shall be determined accordingly.

8. I must interpret the claims in context through the eyes of the person skilled in the art. Ultimately, the question is what the person skilled in the art would have understood the patentee to be using the language of the claims to mean. This approach has been confirmed in the decisions of the High Court in Mylan v Yeda[1] and the Court of Appeal in Actavis v ICOS[2].

9. In the request in their discussion of inventive step, Barker Brettell suggest that the skilled person is someone working in the field of cryptography. UDL suggest that the skilled person is someone working in cryptography and establishing trusted communication between entities. That is, I think, only a minor elaboration, and I am happy to take this definition of the skilled person.

10. I note that Barker Brettell in the observations in reply go on to suggest that the skilled person is aware of elliptic curve cryptography and Identity-Based encryption, in order to implement the Patent, or Galindo et al. and the scheme derived from Sakai, Ohgishi and Kasahara – which is one of the acknowledged references in Galindo et al.

11. The first point made in the request in relation to the claims, is that claim 1 makes no specific limitation to it being employed in relation to a blockchain. That is in contrast to claim 10, where a blockchain application is used to establish a trusted connection with a second node. This, the requester argues means that claim 1 could be applied

[1] Generics UK Ltd (t/a Mylan) v Yeda Research and Dev. Co. Ltd & Anor [2017] EWHC 2629 (Pat)
[2] Actavis Group & Ors v ICOS & Eli Lilly & Co. [2017] EWCA Civ 1671

in any insecure communications network, where individual nodes wish to communicate with each other without the possibility of eavesdropping by non-trusted third parties. Indeed, paragraph 6 of the application suggests that this is a challenge for decentralised peer-to-peer systems. In their observations, UDL Intellectual Property suggest that claim 10 is further distinguished by its reference to a blockchain, implying they agree that claim 1 is not limited to implementation in a blockchain environment. I therefore agree, claim 1 is not limited to the application of a blockchain.

12. The next question raised in relation to claim 1 is what the identifiers of the first and second nodes are. Barker Brettel suggest paragraph 13 indicates that an identifier "*may include an identifier string identifying the node and a role string identifying the role of the group of specialized nodes."* They further note that paragraph 54 gives an example of the id as "id=alice". They therefore suggest that the identifiers should be interpreted broadly to encompass any string or value that can be used to identify the node. This seems to me to be what in practice any such identifier would be.

13. The request then looks at the second secret point being "a group private key times a map-to-point hash of the second node identifier" and the first session key using a bilinear pairing operation. The request notes that there is only broad discussion of these features in paragraphs 17 and 71 respectively. The request suggests that paragraph 71 suggests that the map-to-point hash is one using a given elliptic curve. Paragraph 71 also talks about the need for collaborative generation by the group of nodes of the secret points. The request goes on to note that the absence of detail means that the skilled person is required to use their knowledge to implement these features. That seems to me to be a reasonable starting point, their scope is dependent on the skilled person applying known art in order to implement these features. However, I should be cautious in suggesting that the short description of the map to point hash in paragraph 71 is limiting, beyond what is defined in the claim.

14. The request then looks at claim 3, which states that the first secret point is obtained from portions obtained from each of a plurality of nodes in the group of nodes without reconstructing the group private key. The request suggests that claim 1 must therefore be broader than this, as it does not include this limitation. That is of course likely to be true, but there are a number of parts to this definition in claim 3:

> *3.. The method claimed in claim 1 or claim 2, wherein obtaining the first secret point comprises obtaining, from each of a plurality of nodes in the group of nodes, respective portions of the first secret point and combining the respective portions to form the first secret point without reconstructing the group private key.*

15. In their observations, UDL Intellectual Property do not challenge the points made on construction in the request. Instead the observations concentrate on the "group private key being associated with a group of nodes configured to grant credentials" and "obtaining a first secret point from the group of nodes." They do so, because they suggest that these are the points of distinction over the prior art document, Galindo et al. UDL Intellectual Property point to page 16 line 7- page 17 line 12 of WO2018224941 (the PCT application which entered regional phase as EP3465578) which are paragraphs 58-62 in EP3465578, which is the subject of this opinion. They

do so in order to argue that the secret points are obtained from the group of nodes and not from any one single node acting as a central authority.

16. As set out in paragraph 58, *“the nodes of the group of nodes collaborate to generate a secret point.*” (I could equally turn to figure 7, or paragraphs 10-12). It is therefore clear that this version is envisaged. However, does the claim also encompass the scenario where one node, within the group provides the group private key? Of course, the overall context here is described in paragraph 6 to be to address the challenges in a decentralised peer to peer system. However, that paragraph goes on to say:

> “*As the network architecture of some implementations evolves some nodes may take on more specialized tasks, and other nodes may rely on those specialized nodes as sources of certain data or as performers of certain functions. If a node is going to rely on another node for information or as a legitimate source, it needs to be able to establish a trusted relationship for communicating with that node. In the case where nodes may have different roles, it would be advantageous to have a mechanism for determining and verifying a node's role. Moreover, if a node turns out to be illegitimate or malicious, it should be possible for other nodes to remember it so as to ignore future communications from such a node, in a peer-to-peer system, the challenge is to solve these problems without compromising the peer-to-peer nature of the system by imposing a central authority”*

17. So when I turn to the phrase in the claim *“obtaining a first secret point from the group of nodes”;* does the skilled person see this as limiting the claim to this being collaborative, or is this a special function that a single node within the group might take on? In their request, Barker Brettell suggest the only requirement in claim 1 relating to the group of nodes is that the first and second secret points are obtained from the group of nodes. How the group private key is obtained is they suggest unclear from claim 1 alone. They therefore suggest that claim 1 encompasses the group private key being stored in one or more of the group of nodes including the possibility of the group private key not being held in any one node but being distributed between the group of nodes.

18. In the observations in reply, Barker Brettell take this argument one step further, referring to Datacard Corporation v Eagle Technologies Limited [2011] EWHC 244 where Arnold J said at paragraph 96:

> *Secondly, the inventive concept of a patent must apply to all embodiments falling within the relevant claim. It is not legitimate to define the inventive concept as something narrower than the scope of the relevant claims. In particular, it is not legitimate to identify a narrow sub-group of embodiments falling within the claims and which have certain technical advantages and then to define the inventive concept in terms which apply to the sub-group but not the rest of the claim. If a patentee chooses to advance broad claims, the inventive concept will be broadened in an equivalent way: see Brugger v Medic-Aid Ltd [1996] RPC 635 at 656-657.*

19. They do so in order to advance the idea that figure 1 (which shows a blockchain

network) (and its associated discussion in paragraphs 29-41) envisage an arrangement of nodes in which two of those nodes arrange to establish a trusted communication by way of a group private key provided by a group of nodes. Having read those passages, and looked at figure 1, I am not convinced that I would go so far. Figure 1 is described as being an example network of blockchain nodes. None of those passages go on to describe the setting up of such an in group trusted communication link. I note that there is no statement that this passage, or the figure 1 example are a description of the prior art, it may be that they are statements that would have been conventional at the time of filing.

20. However, Barker Brettell also note that the claims include reference numerals 100 and 102, which are drawn from this figure. Such reference numbers are described in the Manual of Patent Practice at 14.135 as not influencing the construction of the claim, acting rather as a helpful indication of features which may help a reader orient themselves. However, following Rodi and Wienenberger AG v Henry Showell Ltd, [1966] RPC at page 453, the inclusion of such reference letters or numerals is that the claim must be interpreted to include the specific example. In this case, there is nothing surprising in that. The description clearly envisages the use of this trusted communication in such a blockchain network.

21. Nonetheless, Barker Brettell's contention is that claim 1 should be interpreted to encompass any arrangement of nodes in which two nodes arrange to establish a trusted communication , and that there is no distinction in stating that the group private key is associated with a group of nodes configured to grant credentials. I do not however, think that the skilled person reading this document is lead directly to the embodiment that Barker Brettell are implying here. There is no smoking gun, where the embodiment involves a secret key being provided for the group from a single node (102) within the figure 1 blockchain network.

22. UDL Intellectual Property in their observations do not expand on this question of construction, asserting that the application is distinguished as a result of the group private key being associated with a group of nodes configured to grant credentials, and not a base station configured to grant credentials acting as a single party. From that I take it that they do not believe that the claim covers a base station acting here as a single party to manage credentials.

23. I must also note the end of the phrase in question from claim 1: the group private key being associated with a group of nodes (100) **configured to grant credentials.** I further note the reference in the Patent to the desire to avoid the imposition of a centralised certificate authority on a blockchain network (for example in paragraph 50). Ultimately, that leads me to the view that the skilled person, having this context of a peer-to-peer and decentralised network in mind, reads this phrase as suggesting that the secret point is obtained from across nodes within the group, rather than from a single node.

24. Finally, on the construction of claim 1, the request states that the final step of the claim is confirming that the first session key matches a second session key generated by the second node using the bilinear pairing operation with the second secret point and with a map to point hash of the first node identifier. The request uses paragraph 71, and text in paragraph 72 *"If the secret points were legitimately collaboratively generated by the group of nodes using the same group private key k*

and the identifiers of the respective nodes A and B then the pairing operations should result in KA = KB." It does so in order to suggest that the use of a second session key which is the same as the first session key, means that claim 1 defines a method in which symmetric encryption is set up. That may practically be the case, but the claim is clear in requiring there to be a match, and I can correspondingly analyse any document using the claim, rather than taking any further step.

The Prior Art

25. The request uses three pieces of prior art to suggest that the Patent is invalid under Section 1(1) of the Act which reads:

> *A patent may be granted only for an invention in respect of the following conditions are satisfied, that is to say –*
> *(a) the invention is new;*
> *(b) it involves an inventive step…*

However, in practice, the arguments raised in the request, the observations and the observations in reply focus largely on Galindo et al.

26. Galindo et al. describes a pairing method designed for an underwater wireless sensor network. The document, in section 2 explains how a base station can be used to coordinate a network of sensor nodes and explains some of the particular considerations of an underwater network, in terms of radio transmission.

27. The request points to Section 3.1 of Galindo et al. which discusses the use of a bilinear map, such that a secret key for Node A and a second code for Node B can be generated, from a master secret key known only to the base station (Node B.) Barker Brettell describe the disclosure of Galindo et al. as relating to a key exchange protocol following Sakai, Ohgishi and Kasahara (SOK), a fuller disclosure of which is in the publication cited as a reference in Galindo et al. This protocol involves bilinear pairing, a hash function, a master secret key z and identifiers id», ida for respective nodes A and B. A secret key sk« for node A is generated from a hash of the identifier for node A times the master secret key. A corresponding secret key ska for node B is generated from a hash of the identifier for node B times the master secret key. It should be noted that, while the notation in Galindo et al. of sk« = H(idA)$_2$ suggests that the hash of the node identifier is raised to the power of the master secret key, in elliptic curve cryptography the meaning is the same as the hash times the master secret key.

28. Galindo et al. discloses that a secret key KAa is generated for identity ida from a bilinear pairing operation using the hash of the identifier and the secret key of the other node sk»: A corresponding bilinear pairing operation for the identity id» generates the same secret key KAa.

29. Barker Brettell go on to describe Galindo et al. using the wording of claim 1 of the patent, suggesting it discloses a computer implemented method for a first node (node A) to establish a trusted communication with a second node (node B), the second node having a second node identifier (ida) and a second secret point (ska), the second secret point being a group private key master key z) times a map-to-point

hash of the second node identifier (ska = H(ida)$_{2}$,the group private key being associated with a group of nodes (the base station, node A and node B) configured to grant credentials. Galindo et al. states that the master secret key is only known to the base station, implying that the entity configured to grant credentials is not a group of nodes but a single node.

30. Barker Brettell therefore argue that Galindo et al. therefore discloses the same feature because, although the master secret key is only known to the base station, an association is made with the first and second nodes, since these nodes are provided with keys that are derived from (i.e. associated with) the master key.

31. Galindo et al. also discloses: obtaining a first secret point (skA) from the group of nodes (the base station and the first and second nodes), wherein the first secret point is the group private key times a map-to-point hash of a first node identifier (sk« = H(idA)); sending the first node identifier (idA) to the second node; receiving the second node identifier (the first and second nodes cannot generate their respective secret keys without first receiving the identity of the other node, so this feature is implicitly present); generating a first session key (KAa) using a bilinear pairing operation with a map-to-point hash of the second node identifier and with the first secret point (KAa +--- KDF (e(H(ida), skA))); and confirming that the first session key matches a second session key generated by the second node using the bilinear pairing operation with the second secret point and with a map-to-point hash of the first node identifier (this is implicit in Galindo et al., since the same session key KAa is inherently produced by the corresponding operation for the second node).

32. UDL Intellectual Property agree that Galindo et al. only discloses the use of the base station (Node B) to grant credentials, and that the base station acts as a single party in so doing. UDL Intellectual Property then point to a passage in section 3, paragraph 3 of Galindo et al. which reads:

> *"Additionally, in WSN [wireless sensor networks] it is often the case that a single party (base station) sets up the network and this base station can naturally play the role of the Key Generation Center in an IBC system."*

33. I think therefore that there is no real dispute here over what Galindo et al. proposes. It discloses a central base station which manages the keys for communications within its network. Barker Brettell disagree that the definition of the use of i) "a group private key being associated with a group or nodes configured to grant credentials" and ii)" obtaining a first secret point from the group of nodes" limits the claim to exclude a single base station granting credentials. Barker Brettell therefore contend that that is enough to fall within the scope of the claim and that claim 1 is therefore not novel.

34. However, having come to the view above on the construction of claim 1 above, that it does not cover the use of a single node to manage the credentials, I do not agree. Claim 1 therefore seems to me to be distinguished from the Galindo et al. document.

35. I say that, noting the ambiguity in the sentence I quote for section 3 above, which implies that there is some other way for the network to be set up, and what might naturally flow from that. However, neither the request nor the observations really expand on what the alternative to this "often" case with "natural" consequences is,

and what the skilled person can therefore take from this about alternatives.

36. Turning to claim 10, as both parties acknowledge, this introduces a further limitation, to use with a blockchain application. In the request, Barker Brettell suggest that blockchains are well known in order to make an inventive step objection rather than a challenge on novelty. Claim 19 as a dependent claim is similarly distinguished.

37. At this point, I turn to the question of inventive step. To determine whether or not an invention defined in a particular claim is inventive over the prior art, I will rely on the principles established in Pozzoli SPA v BDMO SA [2007] EWCA Civ 588, in which the well-known Windsurfing steps were reformulated:

> *(1)(a) Identify the notional "person skilled in the art";*
> *(1)(b) Identify the relevant common general knowledge of that person;*
> *(2) Identify the inventive concept of the claim in question or if that cannot readily be done, construe it;*
> *(3) Identify what, if any, differences exist between the matter cited as forming part of the "state of the art" and the inventive concept of the claim or the claim as construed;*
> *(4) Viewed without any knowledge of the alleged invention as claimed, determine whether those differences constitute steps which would have been obvious to the person skilled in the art.*

38. As I have identified above, the skilled person is someone working in cryptography and establishing trusted communication between entities.

39. In their observations, UDL Intellectual Property argue that Namamoto (and its disclosures in relation to bitcoin) would not have been common general knowledge in 2017 at the priority date (and therefore also in 2018 at the filing date of this application.) However, they also characterise the document as giving a very general overview of bitcoin technology. Indeed, they describe cryptocurrencies as being notorious for their lack of trust between entities. This means, I do not think that they argue that bitcoin technology was not common general knowledge. Rather I think they are trying to make a point in relation to step 4 of the Pozzoli approach, so I shall return to that later.

40. Barker Brettell, in their request suggest that the use of a group private key is disclosed in Boneh & Franklin, where they point to page 2 lines 2-3) which reads:

> *"Using standard techniques from threshold cryptography, the PKG in our scheme can be distributed so that the master key is never available in a single location."*

41. They do so, in order to suggest that the use of distributed keys might be part of the common general knowledge of the skilled person and re-iterate this in their observations in reply. UDL Intellectual Property do not discuss whether this should be considered part of the common general knowledge. I shall therefore take distributed master keys to be part of the common general knowledge of this skilled person.

42. Turning to step (2) and (3), I have construed the claim above, and discussed how it

is distinguished from Galindo, which both parties have taken to represent the closest prior art. The difference I have identified results from the group private key being associated with a group of nodes configured to grant credentials.

43. That brings me to step (4). First, Barker Brettell in their request point out that Galindo et al. references Boneh & Franklin. That is true, in Section 3.1, Galindo directs the reader to Boneh & Franklin, as well as another document in order to direct the reader to ways of constructing bilinear maps. Barker Brettell suggest that the skilled person will therefore also note the disclosures in Boneh & Franklin in relation to a group private key.

44. However, UDL Intellectual Property disagree, suggesting that there is no motivation for the skilled person to rely on any other entity than the base station in Galindo et al. They then go on to suggest that the teaching of distributing the master key is incompatible with that of Galindo et al. whose purpose is in saving energy in data communication in relation particularly to underwater sensor networks.

45. Barker Brettel, in their observations in reply, suggest that the disclosure of Galindo et al. is broader than the specific application to underwater sensor networks. They use the reference in Galindo et al, to Sakai, Ohgishi and Kasahara “Cryptosystems based on pairing over elliptic curves” to support that argument.

46. So what do I take from Galindo et al. of its purpose? The document is entitled “A killer application… in underwater wireless sensor networks.” The abstract focusses on underwater wireless sensor networks, and it concludes by suggesting that future work should include evaluation in real underwater wireless sensor networks. It is perhaps one step to argue that Galindo could be applied to wireless sensor networks, or other underwater networks, but another to say that is could be applied broadly to any network. I am not therefore convinced that the skilled person when reading Galindo et al. is led to apply its teaching broadly in any communications network, given the breadth of networks that exist.

47. At this point, I note what was said by Laddie J in Pfizer Ltd’s Patent [2001] FSR 16 at paragraph 66:

> *“When any piece of prior art is considered for the purposes of an obviousness attack, the question asked is “what would the skilled addressee think and do on the basis of the disclosure?” He will consider the disclosure in the light of the common general knowledge and it may be that in some cases he will also think it obvious to supplement the disclosure by consulting other readily accessible publicly available information. This will be particularly likely where the pleaded prior art encourages him to do so because it expressly cross-refers to other material.”*

48. Similarly, in Phil & Ted’s Most Excellent Buggy Co Ltd v TFK Trends for Kids GmbH [2014] EWCA Civ 469, the approved approach of Asahi Medical Co Ltd v Macopharma (UK) Ltd [2002] EWCA Civ 466 at paragraph 21 is set out:

> *“ “… Of course any prior art document relied on must be deemed to be read properly and in that sense with interest. To conclude otherwise would*

> *deprive the public of their right to make anything which is an obvious modification of a published document. By obvious I mean that which would be obvious to the skilled person …"*

means that:

> *the crucial issue was whether the judge had any proper basis for concluding that the skilled person who had read the utility model would have been interested in putting it into practice, so that that would have been an obvious thing to do. On the evidence the judge was entitled to conclude that the patent was obvious."*

49. From these passages it seems to me that the references should be read as indications of supporting material, used to implement the disclosure of Galindo et al. and that I must then be clear that the skilled person would then have been interested in putting the result into practice.

50. I do so also mindful of what Barker Brettell and UDL Intellectual Property say in relation to the idea that energy requirements might be a relevant consideration for the skilled person. Barker Brettell acknowledge that the sensor nodes in Galindo et al. are battery powered and they therefore suggest that the skilled person's solution to this problem would be to provide more than one base station within the group, since base stations are not so energy constrained. Barker Brettell do not provide detail on whether the implementation of two or more base stations within a cell or group is a solution that is widely adopted. It is certainly the case that a single base station in wireless networks is common. I am not therefore convinced by the arguments raised here that this is a solution that the skilled person would readily adopt.

51. Barker Brettell make this argument, because UDL Intellectual Property had argued in their observations, that the energy required by distributing the master key in the manner described in Boneh & Franklin would be greater, and that the skilled person would therefore not be provided with the necessary motivation to apply this teaching.

52. For me to find that the claim is obvious, I need to be conclude that the skilled person would come up with the invention (not just that they could). Here, UDL Intellectual Property suggest that the adaption would require a *complete* redesign of the system. I do not think that Barker Brettell really disagree on this point, they are proposing adapting the design of Galindo. Their argument is rather I think based on the idea that the skilled person would read the two disclosures together, and then embark on some new project, designing a system that means the claim is obvious.

53. However, Barker Brettell do not expand on what the nature of that task might be, and why the skilled person might adapt the design in this way. From all this, it seems to me that I have not been provided with a clear train of thought that leads the skilled person to implement Galindo et al. in a way that leads to the invention defined in the Patent.

54. Finally, Barker Brettell make an argument using Nakamoto to the skilled person implementing the teachings of Galindo et. Al in a blockchain network. Although, Barker Brettell noted in their request, in a standard blockchain network trusted

communications channels between nodes are not required. UDL Intellectual Property note that trusted communication between nodes in a blockchain network can be useful for example in sending information about your transaction and what block it has been mined in.

55. Nonetheless, it does not seem to me that the Nakamoto document helps to bridge the gap I have identified above, whilst it does disclose the use of cryptography within a network of nodes, it does not address the idea of secret communications by using a group private key and the group of nodes being configured to grant credentials.

Opinion

56. It is therefore my opinion that claims 1, 10 and 19 are novel in respect of the prior art raised in this request.

57. Furthermore, based on the documents and arguments filed in this request, it is my opinion that claims 1, 10 and 19 are inventive.

Robert Shorthouse
Examiner

NOTE

This opinion is not based on the outcome of fully litigated proceedings. Rather, it is based on whatever material the persons requesting the opinion and filing observations have chosen to put before the Office.