Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 10 October 2023

Case Number: T 0767/21 - 3.5.01

Application Number: 16864198.3

Publication Number: 3376455

IPC: G06Q20/06, G06Q20/22

Language of the proceedings: EN

Title of invention:
BLOCK CHAIN GENERATION DEVICE, BLOCK CHAIN GENERATION METHOD, BLOCK CHAIN VERIFICATION DEVICE, BLOCK CHAIN VERIFICATION METHOD AND PROGRAM

Applicant:
Nippon Telegraph and Telephone Corporation

Headword:
Blockchain generation method/NIPPON

Relevant legal provisions:
EPC Art. 56, 84
RPBA Art. 13(2)

Keyword:
Inventive step - a blockchain consensus protocol that alternates between two parameters: proof of stake and the number of counterparties a miner has transacted with (no - not technical)

Decisions cited:
T 0641/00, T 1358/09, T 0630/11, T 2330/13, T 0550/14, T 2314/16

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 0767/21 - 3.5.01

D E C I S I O N
of Technical Board of Appeal 3.5.01
of 10 October 2023

Appellant: (Applicant)	Nippon Telegraph and Telephone Corporation 5-1, Otemachi 1-chome Chiyoda-ku Tokyo 100-8116 (JP)
Representative:	Hoffmann Eitle Patent- und Rechtsanwälte PartmbB Arabellastraße 30 81925 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 22 January 2021 refusing European patent application No. 16864198.3 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Chandler
Members:	W. Zubrzycki
	D. Rogers

Summary of Facts and Submissions

I. This is an appeal against the decision of the examining division to refuse European patent application No. 16864198.3 for lack of inventive step (Article 56 EPC).

II. The examining division found that the independent claims according to the main and auxiliary request then on file lacked an inventive step over a conventional networked computer system. The decision mentioned that some of the claimed features were also known from D1 ("White Paper. ethereum/wiki Wiki. GitHub" [actually entitled "A Next-Generation Smart Contract and Decentralized Application Platform"], Internet citation published on 11 June 2015) and D2 (F. Tschorsch and B. Scheuermann: "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies" published on 15 May 2015).

III. In the statement setting out the grounds of appeal, the appellant requested that the decision of the examining division be set aside and a patent be granted on the basis of the refused requests.

IV. In a communication, the Board set out its preliminary opinion that the subject-matter of both requests was unclear (Article 84 EPC), and, as far as could be understood, lacked an inventive step over the disclosure of D6 (KOUROSH ET AL. "NeuCoin: The First Secure, Cost-Efficient and Decentralized Cryptocurrency", published on 25 March 2015) mentioned in the background art section of the application.

V. In a reply dated 1 July 2022, the appellant filed a new main and auxiliary request and provided arguments in

favour of clarity and inventive step.

VI. In the communication accompanying the summons to oral proceedings, the Board was inclined not to admit the main and auxiliary requests into the proceedings. Furthermore, the Board tended to consider that the appellant's arguments were not persuasive.

VII. By letter of 2 August 2023, the appellant filed a new second and third auxiliary request and provided arguments in favour of their clarity.

VIII. The oral proceedings took place per videoconference on 10 October 2023. The appellant's final requests were that the decision be set aside and a patent be granted upon the basis of either the second or the third auxiliary request, both filed under cover of the letter dated 2 August 2023.

IX. Claim 1 of the second auxiliary request reads:

"*A blockchain generation apparatus (1) configured to generate new blockchain data by linking a new block to blockchain data (112) which is a chain of blocks each including transactional datasets generated by a plurality of transaction generation apparatuses, the blockchain generation apparatus (1) comprising:*

a synchronizer (121) configured to acquire shared data which includes the blockchain data (112) and transaction datasets (113) not included in the blockchain data (112);

a parameter calculator (122) configured to

identify a parameter type to be used for linkage of the new block, based on block approval method data (114) specifying a blend pattern of a plurality of parameter types used for determination of

presence or absence of qualification regarding linkage of a plurality of blocks in the blockchain data (112), and the blockchain data (112), and

calculate a value for the identified parameter type based on transaction datasets which are among the transaction datasets in the blockchain data (112) and are related to an identifier of a generating party using the blockchain generation apparatus (1);

a block generation condition checker (125) configured to determine whether the generating party is qualified to generate the new blockchain data, based on the value calculated by the parameter calculator (122);

and a blockchain generator (126) configured to try to generate the new blockchain by referring to the shared data when the block generation condition checker (125) determines based on the parameter type identified by the parameter calculator that the generating party is qualified,

wherein the block approval method data (114) is configured to specify a blend pattern in which a combination of a predetermined number of successive parameter types includes at least one first parameter type and at least one second parameter type, the parameter types conflicting with each other."

X. Claim 1 of the third auxiliary request adds:
- the wording "*and including a number of transaction patterns of a generating party and a number of coins saved of the generating party*" to the definition of the block approval method data
- *the feature: "and the predetermined number is the number of blocks necessary for approving a transaction for a certain block*" at the end of the claim.

XI. The appellant argued as follows:

Claim 1 of the third auxiliary request was clear. The skilled reader understood that "*approving a transaction*" occurred when a blockchain branch containing the transaction became the official blockchain and other branches were discarded. This happened after the transaction was included at a depth of a predetermined number of blocks. Furthermore, the description made it clear that the "*number of transaction patterns of a generating party*" was the number of the party's transaction counterparties.

The consensus protocol in claim 1 was technical. Firstly, the blockchain possessed an inherently technical character which came from linking blocks with hash pointers, making it tamper-proof, and from the fact that it could be updated by any participant. This inherent technical character extended to the distinguishing features. Secondly, granting the right to generate a block based on the number of saved coins and the number of transaction patterns was based on the technical consideration that these parameters were conflicting, making it difficult for one user to control both of them. This reduced the risk of so-called 51% attacks and improved the blockchain security which was a technical effect.

The idea to alternate these two parameters within a specific number of blocks required for approving a transaction was a further technical consideration.

Preventing malicious attackers from falsifying the blockchain was comparable to using electronic signatures to ensure the authenticity of electronic

communication, which was classified as technical by the Guidelines for examination.

Reasons for the Decision

1. Admittance

The Board admits the second and third auxiliary requests into the proceedings under Article 13(2) RPBA 2020. These requests are a *bona fide* attempt to overcome clarity objections raised by the Board for the first time. This is an exceptional circumstance in the sense of Article 13(2) RPBA 2020.

2. The invention

2.1 The invention concerns the problem of preventing malicious agents taking control of a blockchain storing a digital currency, thereby being able to falsify transactions, such as spending the same coin twice - "double spending" (published European application, [2]).

2.2 To remove the need for a central governing authority, such as a bank, cryptocurrencies rely on a peer-to-peer network of nodes, usually coin owners' computers, each maintaining a copy of a ledger that records transactions involving the transfer of coins from one owner to another.

The problem of protecting the ledger against tampering is addressed by storing transactions in blocks on a tamper-proof blockchain. The transactions are signed, making it (currently) impossible to steal coins, and the blocks are linked with hash pointers, making it

impossible to tamper with the ledger.

2.3 Any of the nodes can generate a new block ([4]), but essentially all the nodes need to agree on the next block that goes onto the blockchain, in particular that it contains only valid transactions. In order to achieve this agreement, all nodes follow a set of rules, known as a consensus protocol. As one of its primary objectives, a consensus protocol incentivises nodes to act honestly, e.g. not include a transaction spending a single unit of cryptocurrency more than once, when generating new blocks.

Firstly, the incentive is to receive some of the currency itself in return for generating a correct block. Secondly, in order to avoid a free-for-all resulting in too many candidate blocks, the right to generate the new block incurs some effort or "cost" [4]; hence the analogy with "mining".

2.4 Two known examples of consensus protocols involve the parameters of Proof of work (PoW) and Proof of stake (PoS) ([5] to [8]).

PoW grants the right to generate the block to the node which most quickly solves a mathematical problem; the parameter thus reflects the computational power invested ([6]). This also ensures that a random node generates each new block.

PoS uses the amount of cryptocoins possessed as the parameter ([7]). The key idea in PoS is that if someone has a financial stake in the cryptocurrency system, they will not sabotage it, as this could lead to the collapse in their own coins' value ([11]; decision, point 1.2.1).

One problem with these known protocols is that they may be subject to a so-called 51% attack ([10] to [13]) in which malicious attackers control 51% of the overall block generation rate in the case of PoW or possess 51% of the available coins in the case of PoS. In such situations, the attackers could generate and agree on blocks containing invalid transactions in a tampered blockchain branch which eventually becomes the official blockchain ([5] and [8]).

2.5 To address this problem, instead of relying on a single parameter, e.g PoS or PoW, the invention alternates according to a "blending" pattern in a predetermined number of blocks between at least two "conflicting parameter types" ([45], [47], [48]). Since it is more challenging for a single miner (or a group of miners) to take control of two parameters than one ([48] and [51]), monopolising the mining process becomes more difficult.

3. Third auxiliary request

3.1 The Board finds it convenient to analyse the more specific third auxiliary request first.

Claim 1 of this request further specifies that the two "conflicting" parameters are the number of coins saved (PoS) and "*a number of transaction patterns of a generating party*" ([58]), see penultimate feature. While not claimed, the number of transaction patterns is the number of cryptocurrency participants that a given participant has carried out transactions with ([100] and [103] to [105]). The use of this parameter is based on the assumption that a participant who has engaged in transactions with many counterparties has

earned their trust. The loss of this trust, resulting from an attempt to perform a 51% attack, is considered a deterrent to such an attack ([100]). This is also considered to be a "conflicting" parameter with PoS, as a participant is unlikely to at the same time possess many coins and have carried out many transactions, although this assumes that the transactions are spending transactions, which is not claimed. The predetermined number of blocks in the blending pattern is that necessary for approving a transaction for a certain block (last feature). Although not claimed but disclosed in the application, this number can be for example set to six, in line with common business practice in the bitcoin community, see [32] and [96].

Article 84 EPC

3.2 The Board considers that claim 1 does not comply with the requirements of Article 84 EPC because the following features are unclear:

- "*the predetermined number is the number of blocks necessary for approving a transaction for a certain block".* It is not clear how, in terms of blockchain data, an approved transaction differs from other transactions on the blockchain. The Board judges that the meaning asserted by the appellant (see section XI above) is not derivable from this wording, not least because there is no indication that the certain block and the predetermined number of blocks are in the same branch.

- "*a number of transaction patterns of a generating party*". The appellant argued that this wording was clear in the light of the application and had the meaning outlined in point 3.1 above. However, the Board

judges in line with established case law that the claim must be clear in itself, without reference to the description (Case Law of the Boards of Appeal, 10th ed., 2022, II.A.6.3.5, paragraph 4ff.). Moreover, if these transactions are not spending transactions, it is not clear that the parameter conflicts with the number of coins saved (see point 3.1, above).

Article 56 EPC

3.3 Notwithstanding the lack of clarity, the Board is able to assess inventive step interpreting the transaction patterns as the number of cryptocurrency participants to whom a generating party has transferred coins, and assuming that each sequence of six blocks within the blockchain contains at least one block generated using this number of participants and at least one block generated using the number of saved coins.

3.4 The examining division started from a conventional networked computer system and held that the steps performed by the claimed components constituted a business scheme the implementation of which would have been obvious (decision, points 1.2.8, 1.2.9 and 1.2.14). The decision mentioned that the steps of mining blocks and determining whether a node was qualified to participate in mining were conventional, as shown by documents D1 and D2, for example (decision, point 1.2.9).

3.5 The Board considers document D6, mentioned in the background art section of the application, as a more appropriate starting point. D6 not only discloses the conventional features of blockchain technology, disclosed in D1 and D2, but also the use of Proof of Stake (POS). This avoids an unnecessary discussion of

these features' technicality (cf. T 550/14 - Catastrophe relief/SWISS RE, reasons, point 3.5). This is particularly prudent where a prominent technology, such as blockchain, is involved and the outcome of such a technicality discussion may have far-reaching consequences for patentability.

3.6 It is common ground that claim 1, interpreted in the aforementioned manner, differs from D6 by:

- The features added in the third auxiliary request (blend pattern containing (six) blocks necessary for approving a transaction including at least one of two conflicting parameter types, namely a number of cryptocurrency participants to whom a generating party has transferred coins and a number of coins saved by it).
- A block generation condition checker (125) configured to determine whether the generating party is qualified to generate a new blockchain data, based on the value of the identified parameter (fourth feature).
- An attempt to generate a new blockchain when the block generation condition checker (125) determines, based on the parameter type identified by the parameter calculator, that the generating party is qualified (fifth feature).

3.7 The Board judges that, compared to D6 that relies solely on the proof of stake (PoS), the claimed consensus protocol does indeed make it more difficult for a single user or a small group of users to monopolise the mining process. The is because it certainly requires more effort to take control of two parameters than one.

Although the Board agrees with the examining division's

observation that the effectiveness of the protocol's deterrence would vary from user to user and depend on the potential financial gain expected from an attack against the blockchain (decision, points 1.2.19 and 1.2.23), the Board does not consider that this would entirely cancel the alleged effect.

3.8 There remains, however, the key question of whether the protocol derives technical character from this effect or considerations involved in achieving it.

3.9 In the Board's judgement it does not because it is a non-technical policy which is based on business and psychological considerations.

Firstly, the idea to prevent blockchain takeovers by making them financially or socially expensive is a business consideration. Secondly, the number of coins saved and the number of the counterparties with whom the miner transacted in the past have no technical meaning; they are of purely business nature. Furthermore, as outlined at points 2.4 and 2.5 above, those parameters were not chosen based on technical considerations, but rather based on assumptions concerning the user's behaviour when they own cryptocoins or enjoy the market's trust. Thirdly, the use of six blocks as the length of the blending pattern is an arbitrary value in the claimed protocol as it was proved to be an optimum result, and thus only makes sense, in connection with the PoW protocol.

3.10 One of the principles derived from the COMVIK case (decision T 641/00 - *Two identities/COMVIK*) is that a non-technical feature may be used to formulate a technical problem. Accordingly, in this case, starting from D6, the technical problem is to implement a

consensus protocol, wherein:
- In successive block generation rounds, the right to add a block is granted to a cryptocurrency participant based on their number of saved coins or the number of cryptocurrency participants to whom they have transferred coins.
- Each sequence of six blocks within the blockchain contains at least one block generated using each of these parameters.

The implementation is claimed in functional terms and directly follows from the technical problem; facing this problem, it would have been self-evident to provide the required functionality at a blockchain client of D6.

3.11 The appellant argued that the technical character of the protocol was inherent from the tamper-proof properties of the blockchain. These were such that one could have only developed the claimed protocol having previously understood their technical advantages, especially in terms of security. Without this understanding, the protocol's development would have been impossible from the outset. If this argument were accepted, the situation here would be similar to that in T 2314/16 - *Distributing rewards by assigning users to partial advertisement display areas/RAKUTEN*, where in order to devise the concept of dividing a website advertisement area into clickable partial areas and allocating them to influencers, one must firstly understand how a website is constructed on the technical level.

3.12 However, the Board is not convinced by this argument.

Regardless of its computer implementation, the

blockchain is a vehicle for doing business. At a business level, it is a transaction ledger to which all participants can add blocks of transactions. Contrary to the appellant, the Board considers that deciding who can add transaction blocks to the blockchain is not based on technical considerations.

The claimed consensus protocol could have been developed based on this business-level understanding of the blockchain without any need to consider properties that make it tamper-proof, such as robust cryptography and block linking through pointers. Accordingly, any technical character, that possibly results from these properties, does not carry through to the claimed consensus protocol.

3.13 Hence, the situation here is different from that in T 2314/16, *supra*. Rather, it resembles the scenario outlined in T 630/11 - *Gaming Server/WATERLEAF* under reason 11, where a reader who wants to give a book, which is a technical artefact, as a gift or have a copy of it, is not concerned with technical issues, but rather formulates his desire in terms of the book as an art object.

3.14 Contrary to the appellant's view, the Board considers that a consensus protocol does not improve the blockchain security, but rather the accuracy of transaction data recorded on the blockchain, i.e. how correctly the blockchain represents transactions over time. However, this accuracy is not a technical parameter and improving it, for example by preventing double spending fraud, is *per se* not a technical effect. Furthermore, the coexistence of multiple blockchain branches, generated by different miners, is not a technical malfunction and the question which of

those branches eventually prevails is *per se* not a technical one.

3.15 Nor is the Board persuaded by the argument that the claimed consensus protocol is comparable to an electronic signature scheme and therefore technical. Digital signature schemes are not concerned with the semantics of transmitted information; they operate at bit level. As long as the sequence of bits, transmitted as an electronic message, was created by the signee and was not altered during a transmission, the transmitted content does not play any role. This is fundamentally different from the blockchain consensus protocols which operate at the semantic level and are concerned with ascertaining that the blockchain's business content accurately reflects business reality over time.
In view of this fundamental difference, an electronic signature scheme, is not comparable to the blockchain consensus protocols.

3.16 The Board notes that while the claimed consensus protocol does not involve any technical considerations, this would probably not be true for all consensus protocols. For example, a PoW protocol taking into account specific hardware factors that make it ASIC resistant would be likely to have technical character (see T 1358/09 - C*lassification/BDGB ENTERPRISE SOFTWARE*, reasons, point 5.5; T 2330/13 - *Checking selection conditions/SAP*, reasons, point 5.7.5).

3.17 Hence, claim 1 lacks an inventive step (Article 56 EPC).

4. Second auxiliary request

Since claim 1 of the second auxiliary request is

broader than claim 1 of the third auxiliary request, it lacks an inventive step for the same reasons (Article 56 EPC).

5. Since neither of the appellant's requests are allowable, it follows that the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek W. Chandler

Decision electronically authenticated