Internal distribution code:

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

Datasheet for the decision of 30 September 2025

Case Number: T 0450/23 - 3.5.01

Application Number: 14864642.5

Publication Number: 3095044

IPC: G06Q20/06

Language of the proceedings: EN

Title of invention:
BLOCK MINING METHODS AND APPARATUS

Patent Proprietor:
CIRCLE LINE INTERNATIONAL LIMITED

Opponent:
Manitz Finsterwald Patent- und Rechtsanwaltspartnerschaft mbB

Headword:
Bitcoin mining with mid-states/CIRCLE LINE

Relevant legal provisions:
EPC Art. 100(c), 123(2), 123(3)
RPBA 2020 Art. 12(6)

Keyword:

Added subject-matter (yes)
Extending the protection conferred (Article 123 (3) EPC) - moving part of a feature to another one - (yes - shift in the claim scope)

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

Case Number: T 0450/23 - 3.5.01

D E C I S I O N
of Technical Board of Appeal 3.5.01
of 30 September 2025

Appellant: (Patent Proprietor)	CIRCLE LINE INTERNATIONAL LIMITED Vistra Corporate Services Centre Wickhams Cay II Road Town Tortola VG1110 (VG)
Representative:	Ullrich & Naumann PartG mbB Schneidmühlstrasse 21 69115 Heidelberg (DE)
Respondent: (Opponent)	Manitz Finsterwald Patent- und Rechtsanwaltspartnerschaft mbB Martin-Greif-Straße 1 80336 München (DE)
Decision under appeal:	**Decision of the Opposition Division of the European Patent Office posted on 2 January 2023 revoking European patent No. 3095044 pursuant to Article 101(3)(b) EPC.**

Composition of the Board:

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

Summary of Facts and Submissions

I. This appeal is against the decision of the opposition division to revoke European patent No. 3 095 044.

II. The opposition division found that granted claim 1 contained added subject-matter and therefore the ground for opposition pursuant to Article 100(c) EPC prejudiced the maintenance of the patent. In addition, they held that claim 1 of the first to fifth auxiliary requests contained added subject-matter (Article 123(2) EPC) and that claim 1 of the sixth and seventh auxiliary requests extended the scope of the granted patent (Article 123(3) EPC). They did not admit the eighth and ninth auxiliary requests, which were filed during the oral proceedings, into the proceedings.

III. The appellant (proprietor) filed an appeal against this decision. They requested that the patent be maintained as granted (main request), i.e. that the opposition be rejected. Alternatively, they requested that the patent be maintained on the basis of one of the first to ninth auxiliary requests, re-filed with the statement setting out the grounds of appeal. They also made an auxiliary request for oral proceedings.

IV. The respondent (opponent) filed a reply to the appeal requesting that it be dismissed.

V. In a communication under Article 15(1) RPBA, the Board set out its preliminary opinion that it tended to agree with the opposition division's decision and was minded to dismiss the appeal.

VI. Following the reply to the appeal and before the issuance of the Board's communication, both parties filed a further reply, and the respondent filed a further reply after the communication had been issued.

VII. The oral proceedings by videoconference took place on 30 September 2025.

At the end of the oral proceedings, the Chairman announced the Board's decision.

VIII. The final requests of the parties were identical to their initial requests.

IX. Claim 1 as granted reads:

"*A method for mining a block in a blockchain, preferably Bitcoin, said block comprising a block header, as a function of a selected hash function applied on the block header, the selected hash function comprising an expansion operation and a compression operation, the method performed on a computer system, said computer system comprising a single expander entity for performing said expansion operation and a plurality of compressor entities each being adapted to perform a compression operation and all operating synchronously, comprising the steps of:*

[1] Computing a plurality, m, of mid-states, each as a function of selectively varying a selected first portion of the block header, starting from a respective unique mid-state of said plurality mid-states by a mid-state generator entity, wherein said mid-state generator entity computes a new-mide-state [sic] every compressor entity pipe clock with each mid-state being passed down the compressor entity chain at that same

pipe clock rate;

[1.1] Distributing said computed plurality of m mid-states to a beginning stage of said plurality of compressor entities,

[2] Computing by said single expander entity a message schedule, said message schedule comprising a plurality of message schedule elements, on input of a message and a nonce by performing said expansion operation on a selected second portion of the block header; said single shared expander entity being provided by a single shared rolled message expander entity or a cloud of combinatorial logic associated with each compressor entity;

[2.1] Sharing said computed message schedule between said one or more compressor entities by said expander entity;

[2.2] Delaying delivery of said computed plurality of m mid-states to a final stage of said plurality of compressor entities using a FIFO-memory, having a number of stages, the number of stages corresponding to said number of computed message schedule elements of said message schedule;

[3] Computing for each of the m mid-states by performing the compression operation on the computed mid-state and the computed message schedule, a respective one of m results"

X. Claim 1 of the first to seventh auxiliary requests all delete the wording "*starting from a respective unique mid-state of said plurality mid-states by a mid-state*

generator entity" from feature [1].

XI. Claim 1 of the eighth and ninth auxiliary requests do not delete this wording from feature [1].

XII. Claim 1 of the first, second, sixth and seventh auxiliary requests add the wording "*such that each of the compressors starts from a respective unique [state] generated by said mid-state generator entity*" to the end of feature [1.1].

XIII. The appellant argued as follows:

The opposition division erred in finding that the inclusion of the wording *"starting from a respective unique mid-state of said plurality mid-states by a mid-state generator entity"* in claim 1 introduced added subject-matter.

In the technical context of claim 1, the term "mid-states" did not only denote the result of applying a hash function to the first block of a candidate header, but also encompassed all intermediate states of this hash computation. Before yielding the final result, the hash function iterated through multiple rounds, and at the end of each round an intermediate result was produced and provided to the next round. This intermediate result was also a mid-state. Accordingly, the final mid-state was computed starting from these intermediate mid-states.

In addition, the amendment in question was even derivable from Figure 11, which showed that a set of mid-states was computed at the outset of the claimed method and then extended using a hash function in further steps. The extended mid-states corresponded to

the plurality of pre-computed mid-states in claim 1, and the initial set of mid-states corresponded to the "*respective unique mid-state*" from which this computation started.

In several auxiliary requests, the wording "*starting from a respective unique mid-state … by a mid-state generator entity*" was not deleted but essentially transposed to feature [1.1]. Unlike the deletion of this wording, such a transposition did not shift the scope of protection contrary to Article 123(3) EPC. Regardless of whether the wording in question formed part of feature [1] or [1.1], unique mid-states were generated and used in further hash computations.

Furthermore, this transposition was analogous to moving features between the preamble and the characterising portion of a claim; established case law did not regard moving features from one to the other as affecting the scope of protection and contravening Article 123(3) EPC.

XIV. The respondent argued as follows:

The claimed invention related to Bitcoin mining. In this context, the term "mid-state" had a well-established meaning, namely the result of applying a hash function to the first block of a candidate header.

The invention built upon a conventional Bitcoin mining process, which involved:
- a first execution of the hash function on the first block of the candidate header, and
- a second execution of this function on the second block, which included the nonce.

Looking at claim 1 of the main request, the first stage of this hashing process was reflected in feature [1], and the second stage in features [2] and [3].

This understanding was consistent with Figure 11 of the application, which showed that the "*extended mid-states*" were the results of applying the hash function to the second block, whereas feature [1] concerned its first execution, which yielded a set of mid-states.

Regarding the auxiliary requests, the transposition of the wording in question from feature [1] to feature [1.1] resulted in an extension of the scope of feature [1], contrary to Article 123(3) EPC. This transposition was not comparable to moving an entire feature within a claim, as stated by the appellant, as in the latter case the scope of the feature remained unchanged.

Reasons for the Decision

1. Background

1.1 The invention aims to speed up proof-of-work blockchain mining, preferably in Bitcoin. The mining process involves repeatedly hashing the candidate header of a block to be added to the blockchain, incrementing each time a variable portion of the header, called the nonce, until the hash signature is below a predefined target value, see paragraph [5] of the patent. The first miner to achieve this earns the right to add the block to the blockchain and receive a mining reward.

1.2 The invention builds upon the conventional Bitcoin mining process which successively hashes the first and second block of the candidate header (Figure 6). The hasher has an expander that takes and processes a block

of the input message and produces a message schedule, and a compressor that takes and processes the message schedule and produces a hash value [8]. Successive blocks of the header are expanded and fed into the compressor which keeps updating the hash value in a set of registers. In Bitcoin, only the second block of the header, containing the nonce is actually changing each time the header is hashed. As the first block is not changing its compressed value can be reused as the starting value for the hash value in the compressor for each new value of the second block. This value is called the mid-state [13].

1.3 It is common ground that the invention's key idea is to improve the conventional mining process by coming up with multiple candidate headers that have the same second block (essentially all having the same last 4 tail bytes of the Merkle root) apart from the nonce value (paragraph [25], step 2). Then, instead of expanding and compressing the second block with a new nonce for each hash, a second block with a given nonce is expanded once ([25], step 3.1) and compressed with the mid-states of each of the first blocks of the candidate headers ([25], steps 1 and 3.1.1). This reduces the number of expansions per change of nonce.

Deriving the group of the candidate headers is claimed as "*varying a selected first portion of the block header*" (i.e the first 28 head bytes of the Merkle root in the first block that are different) in feature [1] of claim 1.

The second block with the constant tail of the Merkle root is claimed as a "*selected second portion of the block header*" and its expansion as a "*message schedule*" in feature [2]. The compression of the second block

with all the mid-states of the group is claimed in feature [3].

2. Main request, Article 100(c) EPC

2.1 The Board agrees with the opposition division and judges that claim 1 of the granted patent contains added subject-matter (Article 100(c) EPC).

2.2 The reason is that the following amendment in feature [1] (amended wording underlined) is not derivable from the original application:

"*Computing a plurality, m, of mid-states, each as a function of selectively varying a selected first portion of the block header, starting from a respective unique mid-state of said plurality mid-states by a mid state generator entity*"

2.3 The Board agrees with the respondent that, in the context of Bitcoin mining, to which the claim relates, "mid-states" have a clear, established meaning, namely the result of applying a hash function to the first block of the header, which is used as the initial value for the registers in the compressor when hashing the second block.

2.4 The Board disagrees with the appellant's attempt to give this term a broader meaning, namely as intermediate internal states of the hash computation, see section XIII., above.

The skilled person, reading the claim with their common general knowledge, would immediately understand the term in the established sense rather than in the alleged broader one. Furthermore, the original

application supports the invention only in combination with this established meaning.

Thus, paragraph [45] of the original application, being the only potential basis for this amendment, discloses that the mid-state computation step takes the first block of a candidate header as its only input. In particular step 1 states "[p]re-compute s mid-states $MS_0,...,MS_{s-1}$ by applying the first chunk processing of SHA to a block header modified by setting the Merkle-roots field to each of the s Merkle-roots $MR_0,...,MR_{s-1}$". The mid-states are therefore computed starting from the data in the first block of the header and not from any other mid-states.

2.5 The Board also disagrees with the appellant that feature [1] is derivable from Figure 11 and, in particular, that extended mid-states obtained in the seventh step of this figure could be considered to correspond to the plurality of mid-states computed in feature [1]. As stated by the respondent, this is incorrect because the extended mid-states in Figure 11 are the result of executing the hash function on the expansion of the second block of the header (B1), whereas feature [1] concerns the generation of mid-states from its first block.

2.6 Hence, since claim 1 of the main request contains added subject-matter, the ground of opposition under Article 100(c) EPC prejudices the maintenance of the granted patent.

3. First to seventh auxiliary requests, Article 123(3) EPC

The Board agrees with the opposition division (decision, points 5 and 6) that claim 1 of the sixth

and seventh auxiliary requests shifts the protection conferred by the granted patent, contrary to the requirements of Article 123(3) EPC. Although not stated in the decision, the Board judges that claim 1 of the first to fifth auxiliary requests likewise shifts the protection conferred by the patent.

3.1 The amendment causing this shift is the deletion of the wording "*starting from a respective unique mid-state of said plurality mid-states by a mid-state generator entity*" from feature [1] in claim 1 of all those requests. This amendment generalises feature [1], which is no longer limited to starting from a respective unique mid-state.

3.2 In the first, second and sixth to seventh auxiliary requests, this wording was essentially transposed from feature [1] to feature [1.1].

Contrary to the appellant's view, the Board judges that the mere fact that the wording remained in the claim is necessary but not sufficient to meet the requirements of Article 123(3) EPC. As stated by the opposition division (decision, point 5.6), this Article prohibits any shift in a claim's scope, including shifts resulting from partial generalisations of particular claim features. A shift in scope arising from such a partial generalisation cannot be remedied by narrowing other aspects of the claim.

4. Eighth and ninth auxiliary requests - admittance

The Board does not admit the eighth and ninth auxiliary requests into the proceedings under Article 12(6) RPBA.

The opposition division, exercising its discretion, did

not admit these auxiliary requests into the proceedings. They argued that, in addition to being late-filed, the requests did not *prima facie* overcome objections of added subject-matter previously raised for the main request, see decision, points 7.8 and 8.4.

The Board judges that it was a correct use of discretion (Article 12(6) RPBA, first paragraph). Given that claim 1 of these requests contains, in feature [1], the previously discussed wording ("*starting from a respective unique mid-state...")* of the main request, they indeed *prima facie* gave rise to the same objection of added subject-matter.

5. Since none of the appellant's requests is allowable, it follows that the appeal must be dismissed and the opposition division’s decision to revoke the patent upheld.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek W. Chandler

Decision electronically authenticated