Internal distribution code:

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

Datasheet for the decision of 19 November 2025

Case Number: T 2078/22 - 3.5.01

Application Number: 16835873.7

Publication Number: 3335367

IPC: G06Q10/08, H04L9/00, H04L9/08, H04L9/32, H04L29/00, H04L29/02, H04L29/06

Language of the proceedings: EN

Title of invention:
SYSTEM AND METHODS TO ENSURE ASSET AND SUPPLY CHAIN INTEGRITY

Applicant:
Stollman, Jeff
Mateev, Martin

Headword:
Blockchain storing supply-chain data/STOLLMAN AND MATEEV

Relevant legal provisions:
EPC Art. 56, 84, 123(2)
RPBA 2020 Art. 13(2)

Keyword:
Inventive step - blockchain logging of supply-chain custody transfers (no - not technical)

Decisions cited:
T 0641/00

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 2078/22 - 3.5.01

D E C I S I O N
of Technical Board of Appeal 3.5.01
of 19 November 2025

Appellant: (Applicant 1)	Stollman, Jeff 407 Cannon Court Wayne, PA 19087 (US)
Appellant: (Applicant 2)	Mateev, Martin Ul. Georgi Zivkov 4 9000 Bulgaria (BG)
Representative:	Papula Oy P.O. Box 981 00101 Helsinki (FI)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 13 April 2022 refusing European patent application No. 16835873.7 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. 16835873.7 for lack of inventive step (Article 56 EPC).

II. The examining division held that claim 1 of the main, and first to sixth auxiliary requests did not involve an inventive step over a notoriously known blockchain system evidenced by the background document D2 (Wikipedia entry : "Blockchain", published on 7 August 2015).

III. In the statement setting out the grounds of appeal, the appellant appealed against the decision in its entirety and provided arguments in support of the inventive step of the refused requests.

IV. In the communication accompanying the summons to oral proceedings, the Board indicated that it understood the appellant's request to be that the decision be set aside and a patent be granted on the basis of the refused main request or one of the first to sixth auxiliary requests. Furthermore, the Board stated that, although oral proceedings had not been requested, the Board considered them appropriate in this case.

The Board set out its preliminary opinion that the main request appeared to contain added subject-matter and lack clarity (Articles 123(2) and 84 EPC), and that the main request and the first to fifth auxiliary requests lacked inventive step in view of document D4 ("Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies", F. Tschorsch and B. Scheuermann, published on 15 May 2015) which the Board introduced into the

proceedings under Article 114(1) EPC.

Concerning the additional features of the sixth auxiliary request, the Board considered that, starting from D4, they would have been obvious in view of either the skilled person's common knowledge or one of documents D3 (US 2014/0085479 A1) or D5 (US 2009/0160646 A1). D3 had been referred to in the examination proceedings, and D5 was introduced into the proceedings under Article 114(1) EPC by the Board.

V. By letter of 24 June 2025, the appellant filed a new main request and submitted arguments in support of its admissibility and allowability. They renumbered the previous requests as auxiliary requests 1 to 7.

VI. The oral proceedings were held by videoconference on 24 July 2025. The appellant's final requests were to set aside the decision under appeal and to grant a patent according to the main request, or alternatively, according to one of the auxiliary requests 1 to 7. At the end of the oral proceedings, the Chairman announced that the decision would be issued in writing.

VII. The sole claim of the main request reads:

"*An asset supply chain system for identifying anomalies to ensure integrity of an asset supply chain network, said system creating and using an electronic asset-tracking data record using encryption technology to record, monitor, and maintain asset tracking information, said system comprising:*

a. at least one host compute device;

b. a plurality of electronic user interface devices,

each of said plurality of electronic user interface devices being associated with at least one of a plurality of agents associated with said asset supply chain;

c. a software application operating on said at least one host compute device, with said software application having system rules for monitoring, managing, and analyzing asset supply chain information;

d. a communications network connecting each of said plurality of electronic user interface devices with said at least one host compute devices;

wherein said asset supply chain anomaly detector performs the steps of:

i. registering at least one unique agent identifier, by said at least one host computer device, for at least each of said plurality of agents having data input permission to said asset supply chain;

ii. providing said respective at least one unique agent identifier, by said at least one host compute device, via said communications network, to at least one of said plurality of agents, according to the rules;

iii. registering with said at least one host compute device, at least one asset identifier for each asset or group of assets, by at least one of said plurality of agents, where said at least one asset identifier is created or obtained by said at least one of said plurality of agents based upon rules provided by at least one source exogenous to said at least one host compute device, and according to the system rules;

iv. transforming said at least one asset identifier and said at least one agent identifier, by said at least one host compute device, into at least one first transaction record, according to the system rules;

v. recording said at least one first transaction record, by said at least one host compute device, into a non-repudiatable log, according to the system rules;

vi. sending a change of status notice, by at least one of said plurality of electronic user interface devices, to said at least one host compute device, for each change in status of said asset or group of assets or each change in status of said agent identifier, according to the system rules;

vii. transforming said change of status notice into at least one second transaction record, by said at least one host compute device, for each change in status of said asset or group of assets or each change in status of said agent identifier, and recording said at least one second transaction, according to the system rules;

viii. based upon said recording of at least one second transaction, automatically comparing, by said at least one host compute device, a total system-wide quantity of each asset and group of assets before and after said recording of said at least one second transaction, where said asset and group of assets being compared are determined by said recording of at least one second transaction, according to the system rules;

ix. based upon said comparing of total system-wide quantity of each asset or group of assets, with the non-repudiatable log of said asset supply chain, verifying in real-time, by said at least one host

compute device, consistency with said total system-wide asset quantity before and after said recording of at least one second transaction, according to the system rules;

x. if said total system-wide quantity verification is confirmed according to the system rules, then automatically adding said at least one second transaction record of each status change to said non-repudiatable log, by said at least one host compute device, according to the system rules; and

xi. if said total quantity verification is not confirmed according to the system rules, then

a. creating a policy violation report for said at least one anomalous transaction; and

b. automatically identifying, by at least one of said host compute devices, at least one of said plurality of agents associated with said at least one anomalous second transaction."

VIII. Claim 1 of the first auxiliary request reads:

"*A system (10) for ensuring integrity of an physical or digital product supply chain,*

1.1 said system (10) comprising at least one computer server, a plurality of terminals, each of said plurality of terminals being associated with at least one of a plurality of agents along said supply chain, and a software application operating on said at least one computer server, said system (10) configured for creating and using an electronic chain-of-custody data file;

1.2 said chain-of-custody data file configured to use blockchain encryption technology to record and maintain physical or digital product chain-of-custody change information using a chain-of-custody log distributed among the plurality of agents through a client application comprising:

1.2.1 a plurality of linked changes;

1.2.2 that is configured to utilize cryptographic techniques;

1.2.3 that enable detection of attempts to compromise data integrity of the physical or digital product supply chain including any of said plurality of linked changes;

wherein

1.3 said attempts are configured to be detected using said blockchain encryption technology by tracking a physical or digital product to be transferred along said supply chain, configured to:

1.3.1 register (200) said physical or digital product in an initial custody record in the chain-of-custody log, said initial custody record including an initial quantity and information identifying said physical or digital product;

1.3.2 wherein said initial custody record creates a beginning point of the chain-of-custody log in said encrypted chain-of-custody data file;

1.3.3 document (300) each change of custody of said

physical or digital product in said encrypted chain-of-custody data file comprising quantity of the physical or digital product being transferred;

1.3.4 generate (400, 410, 420, 430), at each change of custody of said physical or digital product, at least one change record documenting said change in custody of said physical or digital product based on the encrypted chain-of-custody log, said at least one change record confirming the information identifying said physical or digital product and that a quantity of said physical or digital product transferred is not greater than the initial quantity of said physical or digital product; and

1.3.5 update (350) the chain-of-custody log based on the at least one change record."

IX. Claim 1 of the second auxiliary request differs from claim 1 of the first auxiliary request in that it adds:

- the feature "*1.3.4.1 register (330) acceptance of said physical or digital product by a new agent, at each change of custody of said physical or digital product;*"

- the feature "*1.3.5.1 add a record of such registration acceptance to the chain-of custody log.*"

X. Claim 1 of the third auxiliary request adds to claim 1 of the first auxiliary request:

- the wording "*based on the chain-of-custody log*" after "*supply chain*" in feature 1.3

- the wording "*is signed with encryption key and*" after

"*custody record*" in feature 1.3.2

- the wording "*wherein each change of custody is confirmed with encryption key pairs associated with the custodians*" at the end of feature 1.3.3

XI. Claim 1 of the fourth auxiliary request differs from claim 1 of the first auxiliary request in that:

- In feature 1.2, the wording "*a chain-of-custody log*" is replaced by "*a plurality of chain-of-custody logs*".

- Features 1.3.1 to 1.3.5 are amended as follows (additions underlined, deletions struck through):

"1.3.1 register (200) components of said physical or digital product in ~~an~~ separate initial custody ~~record~~ records in ~~the~~ separate chain-of-custody ~~log~~ logs, said initial custody ~~record~~ records including an initial quantity and information identifying said component of said physical or digital product;

...

1.3.3 document (300) each change of custody of said component of said physical or digital product in said encrypted chain-of-custody data file comprising quantity of the component of the physical or digital product being transferred;

1.3.4 generate (400, 410, 420, 430), at each change of custody of said component of said physical or digital product, at least one change record documenting said change in custody of said component of said physical or digital product based on the encrypted chain-of-custody log, said at least one change record confirming the

information identifying said component of said physical or digital product and that a quantity of said component of said physical or digital product transferred is not greater than the initial quantity of said component of said physical or digital product;and

1.3.5 update (350) the respective chain-of-custody log based on the at least one change record."

XII. Claim 1 of the fifth auxiliary request differs from claim 1 of the first auxiliary request in that it adds:

"*1.3.6 generate (400), at each change of custody of said physical or digital product, at least one report transmitted to the prior and new agent to confirm a change in custody of said physical or digital product.*"

XIII. Claim 1 of the sixth auxiliary request differs from claim 1 of the fifth auxiliary request in that it adds:

"*1.3.7 generate (500) further reports transmitted to at least one member of said supply chain, and at least one party not a member of said supply chain, said reports including an alert of a policy violation.*"

XIV. Claim 1 of the seventh auxiliary request differs from claim 1 of the first auxiliary request in that:

- It adds the feature *"1.3.5 record, by at least one sensor (93), observations and/or evidence of physical or digital product condition, including spoilage, degradation, or damage of said physical or digital product;*"

- It renumbers the last claim feature from 1.3.5 to 1.3.6 and adds the wording "*and the detected spoilage,*

degradation, or damage of said physical or digital product." at the end of this feature.

XV. Concerning the main request, the appellant argued as follows:

The late filing of this request was triggered by a change in the factual situation following the Board's communication, in particular due to the introduction of new prior art documents and new objections under Articles 123(2) and 84 EPC. This was an exceptional circumstance justifying the admittance of the request under Article 13(2) RPBA.

This request was intended to distinguish the claimed invention from the Bitcoin blockchain disclosed in D4. While in D4 users maintained local copies of the transaction log, this was not required in the invention claimed in the main request – here the log could be entirely centralised.

All features of claim 1 had a basis in the original application. In particular, features (vi) and (vii) were based on the description at page 16, at page 12, paragraph 2, and at the top of page 18. Feature (iii) was based on the paragraph bridging pages 6 and 7 and on step 210 of Figure 4. As regarded its part relating to the application of rules, the description used the term "*rules*" and "*policies*" interchangeably.

XVI. Concerning the auxiliary requests, the appellant argued as follows:

First auxiliary request

By recording data documenting how a product moved

within a supply chain onto a distributed blockchain, the invention eliminated the possibility of compromising this supply-chain data through a single attack. Thus, the invention provided the technical effect of assuring the integrity of the recorded supply-chain data.

Second auxiliary request

While in conventional cryptocurrency blockchains entries were recorded by transferring parties, in the invention a product transfer was recorded by the receiving party upon acceptance of the transfer. This design choice was a technical decision; the improvement in the security of supply-chain operations achieved thereby was a technical contribution.

Third auxiliary request

The appellant made no relevant arguments concerning the third auxiliary request.

Fourth auxiliary request

Maintaining separate blockchains for components of products enabled tracking ownership changes at the level of those components rather than at the level of entire products. This ensured the integrity of the supply-chain data at a more granular level.

Fifth and sixth auxiliary requests

Sending reports to parties involved in product transfers further improved the integrity of the supply-chain data, as it enabled a quick reaction to any irregularity. Sending additional reports on a

policy violation to a party within the supply chain and to one outside it increased the number of parties alerted to potential abuses, which improved the security of the supply chain.

Seventh auxiliary request

Tracking product integrity through the supply chain using sensors enabled the generation of automatic alerts indicating when and where conditions adverse to the product's integrity had occurred, as well as the recording of these alerts on the blockchain.

Reasons for the Decision

1. Since, as discussed below, the main request was not admitted into the proceedings, the Board finds it convenient to address first the auxiliary requests.

2. The Invention

2.1 The invention in the auxiliary requests applies blockchain technology to record the movements of a product through a supply chain, see the published application, page 1, second paragraph.

2.2 The blockchain (or "*chain-of-custody data file configured to use blockchain encryption technology*" - feature 1.2) contains the full history ("*chain-of-custody change information*" or "*change-of-custody log*") of a product's transfers between parties ("*agents*") in the supply chain, see page 15, second paragraph.

2.3 Agents run a client application (feature 1.2) that enables them to submit digitally signed transactions ("*linked changes*") to the blockchain, see page 10,

second and third full paragraphs; page 13, last paragraph.

The blockchain is initiated by the product's manufacturer, who creates its genesis block (features 1.3.1 and 1.3.2: "*initial custody record*") that identifies the product and its initial quantity supplied, see page 11, fourth paragraph. Subsequently, each transfer of a quantity of the product is recorded on the blockchain by a receiving agent (feature 1.3.3), see page 12, second paragraph; page 18, second paragraph.

2.4 Independently of the above, the invention generates reports ("*change records*") detailing the product transfers (feature 1.3.4) and provides them to the agents involved, see page 18, third paragraph to page 19, first paragraph.

3. First auxiliary request

Claim 1, Articles 123(2) and 84 EPC

3.1 Although not discussed in the decision, the Board tends to consider that amendments concerning the use of cryptographic techniques to enable the detection of attempts to compromise data integrity, and the configuration of such attempts to be detected (features 1.2.2, 1.2.3 and 1.3), constitute added subject-matter (Article 123(2) EPC).

3.2 These features are not derivable from passages offered by the appellant during the examination proceedings, namely pages 9 to 11 and 16 to 17, see letters of 10 September 2020 and 18 February 2022.

Neither these passages nor the remainder of the application disclose detecting attempts to compromise data integrity, let alone configuring such attempts for detection. Furthermore, it is not clear (Article 84 EPC) how the latter is to be achieved. These objections apply equally to all other auxiliary requests.

In light of the application, the Board interprets the features in question as stating the use of asymmetric cryptography to sign blockchain transactions, see published application, page 3, penultimate paragraph and the paragraph bridging pages 9 and 10.

Article 56 EPC

3.3 Despite the clarity issues mentioned above, the Board is in a position to analyse inventive step of claim 1 on the basis of the above summary of the invention and the claim's interpretation in the preceding point.

3.4 In their analysis of inventive step, the examining division started from a blockchain system with nodes performing cryptographic techniques which they considered to be notoriously known as evidenced by the Wikipedia article D2, see decision, points 1.1, 1.2 and 4.1. However, given the emphasis in this appeal on the security features of blockchain technology, the Board prefers to start from document D4 which, unlike D2, discusses these features in detail. The Board is aware of D4 from the earlier case T 0767/21.

More specifically, D4 discloses that users run a digital wallet application to submit transactions to a cryptocurrency blockchain, of which they maintain local copies, see section 2.2, first paragraph and section 2.4. Thus, when starting from D4, the appellant's

arguments that emphasise this feature as advantageous (see section XVI above) are no longer relevant. Furthermore, as in the application, the blockchain in D4 employs digital signatures (section 2.4, second paragraph, and section 3.1) to ensure data integrity, cf. claim interpretation at point 3.2 above.

3.5 Claim 1 differs from D4 (lettering added by the Board):

A) In that the blockchain's genesis block indicates a product and its initial quantity (features 1.3.1 and 1.3.2) and transactions in following blocks indicate how this product moves within the supply chain (1.3.3).

B) By generating reports indicating product transfers and confirming that the quantity transferred by an agent does not exceed the quantity they previously received (feature 1.3.4).

C) By the server computer and the application it runs (feature 1.2).

3.6 The Board tends to agree with the examining division that feature A, which merely defines the blockchain's business content, lacks technical character, see decision, point 3.4. As the examining division stated (decision, points 3.2 and 3.5), this feature does not improve the known blockchain technology in terms of security or otherwise but merely uses it to record a particular business content, cf. published application, page 3, penultimate paragraph. Accordingly, the Board judges that any technical character that might arise from the blockchain’s security properties does not extend to this feature.

3.7 Feature B is a business feature with no technical implementation and, therefore, no technical contribution. Although not really claimed, even assuming — as essentially argued by the appellant in connection with the fourth auxiliary request — that the generated reports are provided to parties within the supply chain in order to assist them in detecting irregularities, this is a purely business effect with no technical considerations involved in achieving it.

3.8 Concerning feature C, as long as the server application is not used, this feature has no technical effect. Moreover, even assuming that this application is used to register a new agent (published application, page 25, point c.i), applying the Comvik approach (see T 641/00 - *Two identities/COMVIK)*, this would still be an obvious implementation of the business requirement to enable such a registration.

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

4. Second to seventh auxiliary requests, Article 56 EPC

The Board judges that claim 1 of these auxiliary requests does not add anything inventive. The reasons are as follows:

- Registering the acceptance of a product transfer by the receiving agent and recording this acceptance on the blockchain (second auxiliary request, features 1.3.4.1 and 1.3.5.1) are further non-technical business features.

Although the appellant argued that assigning the creation of a blockchain entry to the agent who

received the product was a technical decision, the Board agrees with the decision (point 8.1) that this design choice is not based on any technical considerations. Rather, it merely involves the non-technical considerations relating to who is to record the product transfer and when.

- The use of a pair of keys to sign blockchain transactions (third auxiliary request, features 1.3.2 and 1.3.3), is disclosed in D4, section 2.4.

- The Board agrees with the examining division and judges that using a separate blockchain for different product components (fourth auxiliary request, features 1.3.1, 1.3.3 and 1.3.4) is a business requirement (see decision, point 12.1). The advantage of enabling the tracking of ownership changes at a component level, rather than only at the coarser product level, is of a purely business nature.

- Sending reports to agents involved in the product transfer (fifth auxiliary request, feature 1.3.6) lacks technical character for the reasons given for the first auxiliary request, see point 3.7 above.

- Reporting business policy violations occurring during the transfer of products to a party within the supply chain and to one outside it (sixth auxiliary request, feature 1.3.7) is a further business idea whose implementation is not really claimed. Even assuming, in line with the appellant’s argument, that reporting such violations to multiple parties might contribute to preventing commercial abuse, this remains a purely business effect.

- The Board agrees with the examining division

(decision, point 18.5) that recording product damage on blockchain (seventh auxiliary request, feature 1.3.6) merely concerns the non-technical question of what information to store and, therefore, lacks technical character. The Board also agrees with the examining division that, using the Comvik approach again, the use of a sensor (e.g. a camera) to capture the damage (feature 1.3.5) is an obvious implementation of the non-technical requirement to record the evidence of it, see decision, points 18.2 to 18.4. Not only does the Board agree with the division that sensor-based monitoring architectures were commonly known at the priority date (decision, point 18.1), but it also considers that applying sensors to monitor the integrity of shipped products would have been obvious in view of documents D3 and D5, in particular D5, paragraphs 16 to 20.

The appellant argued that the features in question enabled generating and recording automatic alerts on the blockchain, indicating when and where conditions adverse to the product's integrity occurred. However, this is not claimed and, apart from that, constitutes an obvious implementation of the business requirement to automatically detect and record the occurrence of such adverse conditions.

5. Main request, admittance

5.1 The Board accepts the appellant’s argument (see section XV above) that the introduction of the new closest prior art, D4, may indeed constitute an exceptional circumstance which, potentially, could justify the admission of this request despite its late filing (Article 13(2) RPBA). The Board also accepts the appellant’s view that this request shifts the invention

from the use of a distributed blockchain to a centralised database, apparently in an attempt to address the objection under Article 56 EPC starting from D4.

5.2 However, the presence of such an exceptional circumstance is a necessary condition, but not in itself sufficient, for a new claim to be admissible at this procedural stage. The appellant must also demonstrate, *inter alia*, that this claim does not give rise to new objections, in particular those under Article 123(2) EPC.

5.3 The Board notes that almost all features of the main request's only claim differ from those in the previous claims. Although the appellant indicated a basis in the description and drawings, a number of the claim features paraphrase the indicated basis passages rather than being literally disclosed in them.

5.4 In particular, the Board judges that the following amended features, which are the representative examples of this paraphrasing, introduce added subject-matter:

-vi. sending a change of status notice, by at least one of said plurality of electronic user interface devices, to said at least one host compute device, for each change in status of said asset or group of assets or each change in status of said agent identifier, according to the system rules;

-vii. transforming said change of status notice into at least one second transaction record, by said at least one host compute device, for each change in status of said asset or group of assets or each change in status of said agent identifier, and recording said at least

one second transaction, according to the system rules.

The Board is not convinced by the appellant's assertion that these features are derivable from the passages listed at section XV above. These passages are limited to the generation of shipping manifests recording the transfer of assets between custodians ("*agents*" in the claim) and to recording these precise transfers. By contrast, the features in question specify sending and recording any change in the status of either an asset or an agent identifier.

The added subject-matter is particularly evident in the part specifying the sending and recording of "*each change in status of said agent identifier*", which introduces a concept that is entirely absent from the allegedly supporting passages. Furthermore, although less evident, the part reciting the sending and recording of "*each change in status of said asset*" likewise contains added subject-matter, as it generalises the disclosed concept of notifying and recording the transfer of assets between agents to the much broader one of notifying and recording any conceivable change in status of an asset.

- *where said at least one asset identifier is created or obtained ... upon rules provided by at least one source exogenous to said at least one host compute device, and according to the system rules*" (feature iii)

The Board accepts the argument that the description discloses the use of external policies that may be considered equivalent to the rules in claim 1. Although not argued by the appellant, page 15, second paragraph, which appears to provide the most plausible basis for

the above wording, discloses that: "*such policies or rules may be recognized as necessary standards or regulations to be implemented by various supply chains in order for the supply chain to be compliant with the policies of standards organizations. Such organizations may be, by way of example, the International Standards Organization ("ISO") or other similar standards-setting associations, or regulatory authorities such as the Federal Drug Administration.*"

However, here again, the claim wording significantly paraphrases this passage and, as a result, extends beyond it; the expression "*source exogenous to said at least one host compute device*" encompasses virtually any type of source for rules, whereas the passage mentions in this respect only standard-setting organisations and regulatory authorities.

5.5 Hence, since the late-filed main request gives rise to new objections under Article 123(2) EPC, the Board does not admit it into the proceedings pursuant to Article 13(2) RPBA.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek W. Chandler

Decision electronically authenticated