異議の決定

異議２０１８－７００６６５

（省略）
特許権者　株式会社三菱ＵＦＪ銀行

（省略）
代理人弁理士　特許業務法人高橋・林アンドパートナーズ

（省略）
特許異議申立人　篠森 重樹

特許第６３４１４９１号発明「信号処理方法、および信号処理プログラム」の特許異議申立事件について、次のとおり決定する。

結論

特許第６３４１４９１号の特許請求の範囲を訂正請求書に添付された訂正特許請求の範囲のとおり，訂正後の請求項〔１－４〕，〔５－８〕について訂正することを認める。

特許第６３４１４９１号の請求項１，２，５，６に係る特許を維持する。

特許第６３４１４９１号の請求項３－４，７－８に係る特許についての特許異議申立てを却下する。

理由

第１　手続の経緯

特許第６３４１４９１号の請求項１乃至８に係る特許についての出願は，平成２９年２月２１日に出願され，平成３０年５月２５日にその特許権の設定登録がされ，同年６月１３日に特許掲載公報が発行された。その後，その特許について，同年８月９日に特許異議申立人篠森重樹により特許異議の申立てがされ，当審は，平成３１年２月１５日付けで取消理由を通知した。特許権者は，その指定期間内である平成３１年４月２２日に意見書の提出及び訂正の請求を行ったところ，令和元年５月８日付けで訂正請求書について手続補正指令がなされたため，同月２９日付けで訂正請求書の手続補正がなされ，その訂正の請求に対して，特許異議申立人篠森重樹は，令和元年８月１６日に意見書を提出した。

第２　訂正の適否についての判断

１　訂正の内容

本件訂正請求による訂正の内容は，以下の（１）ア乃至キ及び（２）ア乃至キのとおりである。（なお，下線は訂正箇所であり，この項において同様である。）

（１）１群の請求項１乃至４に係る訂正
ア　訂正事項１
　請求項１に係る「複数のノード」につき，「複数の通信端末」に訂正し，訂正前に「複数のノードにより構成されるグループ」とされていたものを，「互いにネットワークを介して接続される通信端末により構成されるグループ」に訂正するとともに，訂正前に「前記承認要求信号を受信した前記複数のノードのうちの一定割合に相当するノードより承認信号を受信する」とされていたものを，「前記承認要求信号を受信した前記複数の通信端末のうちの一定割合に相当する通信端末より承認信号を受信する」と訂正する。
イ　訂正事項２
　請求項１に係る「承認要求信号」の送信先につき，訂正前に「トランザクションの実行に対する承認要求信号を前記複数のノードの少なくとも一つに送信する」とされていたものを，「トランザクションの実行に対する承認要求信号を、前記複数の通信端末の少なくとも一つに送信する」に訂正する。
ウ　訂正事項３
　請求項１に係る「トランザクションを実行する手順」につき，訂正前に「受信した前記承認信号の承認に基づき」とされていたものを，「前記承認信号を受信した後」と訂正する。
エ　訂正事項４
　請求項１に係る「ブロックチェーンネットワーク」につき，訂正前に「前記トランザクション、および前記トランザクションの電子署名をブロックチェーンネットワークにブロードキャストし」とされていたものを，「前記トランザクション、および前記トランザクションの電子署名を、複数のノードで構成され、前記ネットワークに接続されたブロックチェーンネットワークにブロードキャストし」と訂正する。
オ　訂正事項５
　請求項１に係る「信号処理方法」につき，訂正前に「送信する手順」と，「受信する手順」と，「トランザクションを実行する手順」を含むとされていたものを，さらに「前記複数の通信端末のうち少なくとも一つが前記ブロックチェーンネットワークに接続され、前記ブロードキャストを実行する」と訂正する。
　カ　訂正事項６
　請求項２に係る「前記承認信号」につき，訂正前に「前記承認信号は前記ノードにおける電子署名の付加により生成される」とされていたものを，「前記承認信号は、前記承認要求信号を受信した前記通信端末において、前記トランザクションへ電子署名を付加することにより生成される」と訂正する。
キ　訂正事項７
　訂正前の請求項３及び請求項４を削除するよう訂正する。

（２）一群の請求項５乃至８に係る訂正
ア　訂正事項８

請求項５に係る「複数のノード」につき，「複数の通信端末」に訂正し，訂正前に「複数のノードにより構成されるグループ」とされていたものを，「互いにネットワークを介して接続される複数の通信端末により構成されるグループ」に訂正するとともに，訂正前に「前記承認要求信号を受信した前記複数のノードのうちの一定割合に相当するノードより承認信号を受信する」とされていたものを，「前記承認要求信号を受信した前記複数の通信端末のうちの一定割合に相当する通信端末より承認信号を受信する」と訂正する。

イ　訂正事項９

請求項５に係る「承認要求信号」の送信先につき，訂正前に「トランザクションの実行に対する承認要求信号を、前記複数のノードの一つから前記複数のノードの他の少なくとも一つに送信する」とされていたものを，「トランザクションの実行に対する承認要求信号を、前記複数の通信端末の一つから前記複数の通信端末の他の少なくとも一つに送信する」に訂正する。

ウ　訂正事項１０

請求項５に係る「トランザクションを実行する手順」につき，訂正前に「受信した前記承認信号の承認に基づき」とされていたものを，「前記承認信号を受信した後」と訂正する。

エ　訂正事項１１

請求項５に係る「ブロックチェーンネットワーク」につき，訂正前に「前記トランザクション、および前記トランザクションの電子署名をブロックチェーンネットワークにブロードキャストし」とされていたものを，「前記トランザクション、および前記トランザクションの電子署名を、複数のノードで構成され、前記ネットワークに接続されたブロックチェーンネットワークにブロードキャストし」と訂正する。

オ　訂正事項１２

請求項５に係る「信号処理プログラム」につき，訂正前に「送信する手順」と，「受信する手順」と，「トランザクションを実行する手順」を「前記複数のノードに実行させるように構成され」るとされていたものを，さらに「前記複数の通信端末のうち少なくとも一つが前記ブロックチェーンネットワークに接続され、前記ブロードキャストを実行する」と訂正する。

カ　訂正事項１３

請求項６に係る「ノード」につき，訂正前に「前記複数のノードに実行させる」とされていたものを，「前記複数の通信端末に実行させる」と訂正するとともに，電子署名が付加される対象につき，訂正前に「電子署名を付加することにより前記承認信号を生成する」とされていたものを，「電子署名を前記トランザクションへ付加することにより前記承認信号を生成する」と訂正する。

キ　訂正事項１４

訂正前の請求項７及び８を削除するよう訂正する。

２　訂正の目的の適否，新規事項の有無，及び特許請求の範囲の拡張・変更の存否

（１）訂正事項１について
　訂正事項１は，訂正前の「複数のノード」について，「複数の通信端末」と訂正する事項を含むものである。
　本件明細書の段落１６乃至２０には，次の記載が認められる。（下線は，本決定において説明のために付加したものであり，以下同様である。）

「【００１６】
　通信端末１１０はユーザの管理下に置かれ、通信機能を有する端末であり、据え付け型（デスクトップ型）コンピュータをはじめ、ノート型コンピュータや携帯電話（タブレット、スマートフォンを含む）などの携帯通信端末が例示される。通信端末１１０は、互いにネットワーク１２０を通じて通信することができる。ネットワーク１２０は、インターネットのような外部ネットワークでも良く、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）などの内部ネットワークでもよい。内部ネットワークをネットワーク１２０として用いる場合、通信端末１１０のうち少なくとも一つが外部ネットワークと接続される。図示していないが、通信端末１１０は、その一部あるいは全てが電話回線によって互いに接続されていてもよい。通信端末１１０はノードとも呼ばれる。
【００１７】
　データ１００はテキストデータ、画像データ、あるいはこれらの複合データであり、電子化されている。例えば文書、表、写真、絵、数値などである。データ１００には暗号化を施さず、ユーザグループ内においてパスワードによる保護や閲覧制限に供さなくてもよい。この場合、ユーザグループの全員が通信端末１１０を介してデータ１００を自由に閲覧することができる。
【００１８】
　データ１００は、ネットワーク１２０に接続されたサーバ１５０に格納してもよい。サーバ１５０を直接、あるいは間接的に管理する管理者（以下、単に管理者）は、管理者のサービス内容に応じてデータ１００のための様々なプラットフォームを提供する。例えばユーザグループのスケジュールデータを管理するためのプラットフォーム、ユーザの任意入力情報を時系列に表示するためのプラットフォーム、ユーザグループの共有財産に係るデータを表示するためのプラットフォームなどが提供される。ユーザは、扱うデータ１００に最適なプラットフォームを選択し、プラットフォームの環境に従ってデータ１００を扱う。
【００１９】
　ネットワーク１２０にはさらに、ブロックチェーンネットワーク１３０が接続される。ブロックチェーンネットワーク１３０は、ネットワーク１２０を介して互いに接続された複数の通信端末１３２＿１から１３２＿ｍ（ｍは自然数）で構成される。これらの通信端末１３２は、スペックの差異は存在し得るものの、権限に関しては対等であり、互いに直接通信することができ、いわゆるＰ２Ｐ（Ｐｅｅｒ－ｔｏ－Ｐｅｅｒ）ネットワークを形成する。通信端末１３２はノードとも呼ばれる。以下の記載では、通信端末１１０と区別するため、通信端末１３２をノードと呼ぶ。通信端末１１０の少なくとも一つは、ノード１

３２の少なくとも一つとネットワーク１２０を介して接続される。通信端末１１０はノード１３２として機能することも可能であり、逆に、ノード１３２が通信端末１１０を兼ねてもよい。この場合、通信端末１１０の少なくとも一つがノード１３２として機能すればよい。

【００２０】

ノード１３２は、データの送信処理または受信処理に基づく情報処理の単位であり、不特定の所有者がそれぞれ管理する通信端末であってもよく、この場合、ブロックチェーンネットワーク１３０はパブリックブロックチェーンネットワークとも呼ばれる。あるいはノード１３２のすべて、あるいは一部が管理者によって管理されるよう、ブロックチェーンネットワーク１３０を構成してもよい。例えば管理者と同じ業界内の複数の関係者によってブロックチェーンネットワーク１３０を構成する。この場合、ブロックチェーンネットワーク１３０はプライベートブロックチェーンネットワーク、あるいはコンソーシアムブロックチェーンネットワークとも呼ばれる。」

上記の記載（特に下線部）から，次の技術的事項１を読み取ることができる。

“通信端末１１０は通信機能を有する端末であって，互いにネットワーク１２０を通じて通信することができ，

前記通信端末１１０はノードとも呼ばれ，

ユーザグループの全員が前記通信端末１１０を介してデータ１００を自由に閲覧することができ，

ネットワーク１２０にはさらに，ブロックチェーンネットワーク１３０が接続され，

前記ブロックチェーンネットワーク１３０は，前記ネットワーク１２０を介して互いに接続された複数の通信端末１３２＿１から１３２＿ｍ（ｍは自然数）で構成され，

前記通信端末１１０と区別するため，前記通信端末１３２をノードと呼び，前記通信端末１１０の少なくとも一つは，前記ノード１３２の少なくとも一つと前記ネットワーク１２０を介して接続され，前記通信端末１１０は前記ノード１３２として機能することも可能であり，

前記ノード１３２が前記通信端末１１０を兼ねてもよく，この場合，前記通信端末１１０の少なくとも一つが前記ノード１３２として機能すればよく，

前記ノード１３２は，データの送信処理または受信処理に基づく情報処理の単位であり，不特定の所有者がそれぞれ管理する通信端末であってもよいこと。”

上記技術的事項１から，「ノード」と呼ばれる単位には，「通信端末１１０」がその中に含まれることを読み取ることができ，当該「ノード」には，「通信端末１１０」のほか，「通信端末１３２」と呼ばれるものも含まれることも読み取ることができることから，「複数のノード」を「複数の通信端末」に訂正することは，ノードを構成する複数ある通信端末のうちの一方に限定す

る事項を含むものである。
　さらに，「ユーザグループの全員が前記通信端末１１０を介してデータ１００を自由に閲覧することができ」るとともに，「通信端末１１０は通信機能を有する端末であって，互いにネットワーク１２０を通じて通信することができ」るものであることから，「複数のノードにより構成されるグループ」とされていたものを，「互いにネットワークを介して接続される通信端末により構成されるグループ」に訂正することは，ノードを構成する通信端末のうち，一方に限定する事項を含むものである。
　さらに本件明細書段落２６乃至２８には，次の記載が認められる。

「【００２６】
２．３　承認要求（Ｓ１０２）
　トランズアクションが作成されたのち、トランズアクションの承認段階へ移行する。具体的には図４に示すように、第１の通信端末１１０＿１は、承認要求信号をユーザグループ内の他のユーザが保有する通信端末１１０へ送信する（Ｓ１２０）。承認要求信号には、暗号化される前（すなわち、オリジナル）のトランズアクションＴＡ、および第１の電子署名ＥＳ１が含まれる。さらに第１の通信端末１１０＿１は、承認要求信号を送信する際、あるいは承認要求信号の送信前か送信後に公開鍵１１２＿１を、承認要求信号の送信先である通信端末１１０へ送信する。図４では、第１の通信端末１１０＿１を除く通信端末１１０のすべてに承認要求信号が送信される例が示されているが、後述するように、通信端末１１０のうちの一部に承認要求信号を選択的に送信してもよい。また、第１の通信端末１１０＿１に対して自己送信してもよい。
【００２７】
　承認要求信号を受け取ったユーザは、通信端末１１０において公開鍵１１２＿１を用いて電子署名ＥＳ１を復号化し、暗号化される前のトランズアクションと電子署名を復号化して生成したトランズアクションとを照合することで検証を行う。照合の結果、これらが同一であれば、トランズアクションが偽造、改ざんされておらず、トランズアクションの正当性が証明される。逆に、オリジナルのトランズアクションと電子署名を復号化して生成されたトランズアクションとが同一でなければ、トランズアクションが偽造、改ざんされていると判断することができる。図示していないが、正当性が証明されない場合、トランズアクションは承認されず、破棄される。
【００２８】
２．４　承認（Ｓ１０４）
　トランズアクションを受信した通信端末１１０のユーザは、トランズアクションを承認する、あるいは承認しないという行為のいずれかを選択する（Ｓ１０４）。承認が選択された場合、承認するユーザ（ここでは便宜上、第２のユーザとする）の保有する通信端末（ここでは便宜上、第２の通信端末とする）１１０＿２内で生成される秘密鍵１１４＿２によってトランズアクションが暗号化され、電子署名ＥＳ２が生成される（図３（Ｂ））。第２の通信端末１１０＿２は、第１のユーザから送信された承認要求信号に含まれるオリジナルの

トランズアクションＴＡと電子署名ＥＳ１、および第２の通信端末１１０＿２によって生成された電子署名ＥＳ２を含む承認信号を送信する（Ｓ１２２）。承認要求信号の送信と同様、承認信号の送信前、送信後、あるいは送信と同時に、秘密鍵１１４＿２に対応する公開鍵１１２＿２も送信される。図４では、第２の通信端末１１０＿１を除く通信端末１１０のすべてに承認信号が送信される例が示されているが、通信端末１１０のうちの一部に選択的に承認信号を送信してもよい。また、第２の通信端末１１０＿２に対して承認信号を自己送信してもよい。ここまでのプロセスにより、一つのトランズアクションに対応する二つの電子署名（ＥＳ１とＥＳ２）が生成される。」

上記の記載（特に下線部）から，次の技術的事項２を読み取ることができる。

“第１の通信端末１１０＿１は，承認要求信号をユーザグループ内の他のユーザが保有する通信端末１１０へ送信し，
トランズアクションを受信した通信端末１１０のユーザは，トランズアクションを承認する，あるいは承認しないという行為のいずれかを選択し，承認が選択された場合，承認するユーザの保有する第２の通信端末１１０＿２内で生成される秘密鍵１１４＿２によってトランズアクションが暗号化され，電子署名ＥＳ２が生成され，
前記第２の通信端末１１０＿２は，第１のユーザから送信された承認要求信号に含まれるオリジナルのトランズアクションＴＡと電子署名ＥＳ１，および前記第２の通信端末１１０＿２によって生成された電子署名ＥＳ２を含む承認信号を送信すること。”

上記技術的事項２より，「第１の通信端末１１０＿１」から「承認要求信号」を，「ユーザグループ」の「ユーザが保有する通信端末１１０へ送信」し，「トランズアクションを受信した通信端末１１０のユーザ」が，「トランズアクションを承認する」ことを「選択」した場合，「第２の通信端末１１０＿２によって生成された電子署名ＥＳ２を含む承認信号を送信」することを読み取ることができるから，「前記承認要求信号を受信した前記複数のノードのうちの一定割合に相当するノードより承認信号を受信する」とされていたものを，「前記承認要求信号を受信した前記複数の通信端末のうちの一定割合に相当する通信端末より承認信号を受信する」と訂正することは，承認信号が送信される対象を限定する事項を含むものである。
したがって，訂正事項１は，特許請求の範囲の減縮を目的としたものと認められる。
上記技術的事項１及び２から，訂正事項１は新規事項の追加に該当せず，また，実質的に特許請求の範囲を拡張し，又は変更するものではないことは明らかである。

（２）訂正事項２について
訂正事項２の「承認要求信号」の送信先につき，「前記複数の通信端末の少

なくとも一つに送信」する点は，上記（１）の技術的事項２の「第１の通信端末１１０＿１は，承認要求信号をユーザグループ内の他のユーザが保有する通信端末１１０へ送信」することから読み取ることができ，また，上記（１）で判断したとおり，「ノード」を「通信端末」に訂正することは，ノードを構成する複数ある通信端末のうちの一方に限定する事項を含むものである。

したがって，訂正事項２は，特許請求の範囲の減縮を目的としたものと認められる。

また上記技術的事項２から，訂正事項２は新規事項の追加に該当せず，また，実質的に特許請求の範囲を拡張し，又は変更するものではないことは明らかである。

（３）訂正事項３について

訂正事項３によって，訂正前に「受信した前記承認信号の承認に基づき」とされていたものを，「前記承認信号を受信した後」と訂正することは，平成３１年２月１５日付け取消理由通知の理由１（特許法３６条６項２号）の（１）において，「請求項１の「受信した前記承認信号の承認」との記載は，何を表しているのかが明確でない」旨の取消理由を解消するためになされたものであり，明りょうでない記載の釈明を目的とするものと認められる。

また本件明細書段落２８乃至２９及び段落３９乃至４１には，次の記載が認められる。

「【００２８】
２．４　承認（Ｓ１０４）
トランズアクションを受信した通信端末１１０のユーザは、トランズアクションを承認する、あるいは承認しないという行為のいずれかを選択する（Ｓ１０４）。承認が選択された場合、承認するユーザ（ここでは便宜上、第２のユーザとする）の保有する通信端末（ここでは便宜上、第２の通信端末とする）１１０＿２内で生成される秘密鍵１１４＿２によってトランズアクションが暗号化され、電子署名ＥＳ２が生成される（図３（Ｂ））。第２の通信端末１１０＿２は、第１のユーザから送信された承認要求信号に含まれるオリジナルのトランズアクションＴＡと電子署名ＥＳ１、および第２の通信端末１１０＿２によって生成された電子署名ＥＳ２を含む承認信号を送信する（Ｓ１２２）。承認要求信号の送信と同様、承認信号の送信前、送信後、あるいは送信と同時に、秘密鍵１１４＿２に対応する公開鍵１１２＿２も送信される。図４では、第２の通信端末１１０＿１を除く通信端末１１０のすべてに承認信号が送信される例が示されているが、通信端末１１０のうちの一部に選択的に承認信号を送信してもよい。また、第２の通信端末１１０＿２に対して承認信号を自己送信してもよい。ここまでのプロセスにより、一つのトランズアクションに対応する二つの電子署名（ＥＳ１とＥＳ２）が生成される。
【００２９】
承認信号を受け取った通信端末１１０では、二つの電子署名を対応する公開鍵１１２＿１、１１２＿２を用いて復号化し、トランズアクションの検証を行

うことができる（図３（Ｂ）参照）。これにより、どのユーザが承認したかを把握することができる。」

「【００３９】
２．６　ブロードキャスト（Ｓ１１０）
　トランズアクションが承認されると、トランズアクションの実行が開始される。具体的には、最初にトランズアクションはネットワーク１２０を介してブロックチェーンネットワーク１３０へブロードキャストされる（Ｓ１１０）。
【００４０】
　例えば第１の通信端末１１０＿１は、受信した承認信号に含まれる電子署名の数が承認条件を満たすか否かを判断する。承認条件が満たされたと判断された場合、トランズアクション、電子署名ＥＳ１、および受けとった電子署名をブロックチェーンネットワーク１３０へブロードキャストする（Ｓ１２８）。なお、ブロードキャストを行う通信端末１１０は第１の通信端末１１０＿１に限られず、任意に設定することができる。例えば、あらかじめ決められた通信端末１１０からブロードキャストしても良く、承認条件を満たすために必要な電子署名を最後に生成した通信端末１１０がブロードキャストを行ってもよい。
２．７　ブロックチェーンの更新
【００４１】
　ブロードキャストが行われたのち、トランズアクションの検証が行われる。図５（Ａ）に示すように、ブロックチェーンネットワーク１３０の各ノード１３２の記憶装置には、これまでにブロードキャストされた過去のトランズアクションをまとめたブロック１４０が格納されている。これらのブロック１４０は生成順に連結されて時系列を作る。新たなトランズアクションはブロックチェーンネットワーク１３０内で検証され、トランズアクションの正当性が確認されると、このトランズアクションを含む新たなブロック１４０が生成される。新たにに生成されたブロック（図５（Ａ）ではブロック１４０＿３）は、これまでに生成されたブロック（ブロック１４０＿１、ブロック１４０＿２）に連結され、これによりブロックチェーンの更新が行われ、トランズアクションが実行される。」

　上記の記載（特に下線部）から，次の技術的事項３を読み取ることができる。

“トランズアクションを受信した通信端末１１０のユーザは，トランズアクションを承認する，あるいは承認しないという行為のいずれかを選択し，承認が選択された場合，承認するユーザの保有する通信端末１１０＿２内で生成される秘密鍵１１４＿２によってトランズアクションが暗号化され，電子署名ＥＳ２が生成され，
　前記通信端末１１０＿２は，トランズアクションＴＡと電子署名ＥＳ１，および前記通信端末１１０＿２によって生成された電子署名ＥＳ２を含む承認信号を送信し，
　承認信号を受け取った通信端末１１０では，二つの電子署名を対応する公開

鍵１１２＿１，１１２＿２を用いて復号化し，トランズアクションの検証を行うことができ，
　トランズアクションが承認されると，トランズアクションの実行が開始され，
　トランズアクションはブロックチェーンネットワーク１３０内で検証され，トランズアクションの正当性が確認されると，このトランズアクションを含む新たなブロック１４０が生成され，新たに生成されたブロックは，これまでに生成されたブロックに連結され，これによりブロックチェーンの更新が行われ，トランズアクションが実行されること。”

　上記技術的事項３より，「トランズアクションＴＡ」を含む「承認信号」が「通信端末１１０＿２」によって「送信」された後に，「トランズアクションが実行される」ことを読み取ることができるから，訂正事項３は新規事項の追加に該当せず，また，実質的に特許請求の範囲を拡張し，又は変更するものではないことは明らかである。

（４）訂正事項４について
　訂正事項４にかかる，「前記トランザクション、および前記トランザクションの電子署名をブロックチェーンネットワークにブロードキャストし」とされていたものを，「前記トランザクション、および前記トランザクションの電子署名を、複数のノードで構成され、前記ネットワークに接続されたブロックチェーンネットワークにブロードキャストし」と訂正することは，「ブロックチェーンネットワーク」につき，「複数のノードで構成され」ること，及び「前記ネットワークに接続され」ることを限定する事項を含むものである。
　そして，訂正事項４に係る，「ブロックチェーンネットワーク」，及び「ブロードキャスト」につき，本件明細書の段落１９及び３９乃至４０には，次の記載が認められる。

「【００１９】
　ネットワーク１２０にはさらに、ブロックチェーンネットワーク１３０が接続される。ブロックチェーンネットワーク１３０は、ネットワーク１２０を介して互いに接続された複数の通信端末１３２＿１から１３２＿ｍ（ｍは自然数）で構成される。これらの通信端末１３２は、スペックの差異は存在し得るものの、権限に関しては対等であり、互いに直接通信することができ、いわゆるＰ２Ｐ（Ｐｅｅｒ－ｔｏ－Ｐｅｅｒ）ネットワークを形成する。通信端末１３２はノードとも呼ばれる。以下の記載では、通信端末１１０と区別するため、通信端末１３２をノードと呼ぶ。通信端末１１０の少なくとも一つは、ノード１３２の少なくとも一つとネットワーク１２０を介して接続される。通信端末１１０はノード１３２として機能することも可能であり、逆に、ノード１３２が通信端末１１０を兼ねてもよい。この場合、通信端末１１０の少なくとも一つがノード１３２として機能すればよい。」

「【００３９】

２．６　ブロードキャスト（Ｓ１１０）

トランズアクションが承認されると、トランズアクションの実行が開始される。具体的には、最初にトランズアクションはネットワーク１２０を介してブロックチェーンネットワーク１３０へブロードキャストされる（Ｓ１１０）。

【００４０】

例えば第１の通信端末１１０__１は、受信した承認信号に含まれる電子署名の数が承認条件を満たすか否かを判断する。承認条件が満たされたと判断された場合、トランズアクション、電子署名ＥＳ１、および受けとった電子署名をブロックチェーンネットワーク１３０へブロードキャストする（Ｓ１２８）。なお、ブロードキャストを行う通信端末１１０は第１の通信端末１１０__１に限られず、任意に設定することができる。例えば、あらかじめ決められた通信端末１１０からブロードキャストしても良く、承認条件を満たすために必要な電子署名を最後に生成した通信端末１１０がブロードキャストを行ってもよい。」

上記の記載（特に下線部）から，次の技術的事項４を読み取ることができる。

“ネットワーク１２０にはブロックチェーンネットワーク１３０が接続され，
前記ブロックチェーンネットワーク１３０は，前記ネットワーク１２０を介して互いに接続された複数の通信端末１３２__１から１３２__ｍ（ｍは自然数）で構成され，前記通信端末１３２はノードとも呼ばれ，
トランズアクションは前記ネットワーク１２０を介して前記ブロックチェーンネットワーク１３０へブロードキャストされ，
前記トランズアクション，電子署名ＥＳ１，および受けとった電子署名は前記ブロックチェーンネットワーク１３０へブロードキャストされること。”

上記技術的事項４のうち，「ネットワーク１２０にはブロックチェーンネットワーク１３０が接続」されること，及び「前記ブロックチェーンネットワーク１３０は，前記ネットワーク１２０を介して互いに接続された複数の通信端末１３２__１から１３２__ｍ（ｍは自然数）で構成され」ることから，「ブロックチェーンネットワーク」が「複数のノードで構成され」ることを読み取ることができる。また，「前記トランズアクション，電子署名ＥＳ１，および受けとった電子署名は前記ブロックチェーンネットワーク１３０へブロードキャストされること」から，“前記トランザクション、および前記トランザクションの電子署名を、複数のノードで構成され、前記ネットワークに接続されたブロックチェーンネットワークにブロードキャスト”することを読み取ることができる。

したがって，訂正事項４は，特許請求の範囲の減縮を目的としたものと認められ，上記技術的事項４から，訂正事項４は新規事項の追加に該当せず，また，実質的に特許請求の範囲を拡張し，又は変更するものではないことは明らかである。

（５）訂正事項５について
訂正事項５に係る，「前記複数の通信端末のうち少なくとも一つが前記ブロックチェーンネットワークに接続され、前記ブロードキャストを実行する」との事項は，訂正前の「受信した前記承認信号の承認に基づき、前記トランザクション、および前記トランザクションの電子署名をブロックチェーンネットワークにブロードキャストし、前記トランザクションに関する情報を含むブロックをブロックチェーンに追加することによって前記トランザクションを実行する手順」のうち，「前記トランザクション、および前記トランザクションの電子署名をブロックチェーンネットワークにブロードキャスト」する構成について，さらに限定するものと認められ，訂正事項５は，特許請求の範囲の減縮を目的としたものと認められる。
そして，上記（１）の技術的事項１から，「前記通信端末１１０の少なくとも一つは，前記ノード１３２の少なくとも一つと前記ネットワーク１２０を介して接続され，前記通信端末１１０は前記ノード１３２として機能することも可能」であること，及び「ネットワーク１２０を介して互いに接続された複数の通信端末１３２__１から１３２__ｍ（ｍは自然数）で構成され」るところの，「ブロックチェーンネットワーク１３０」において，「前記ノード１３２が前記通信端末１１０を兼ねてもよく，この場合，前記通信端末１１０の少なくとも一つが前記ノード１３２として機能すればよ」いことを読み取ることができるから，訂正事項５は，新規事項の追加に該当せず，また，実質的に特許請求の範囲を拡張し，又は変更するものではないことは明らかである。

（６）訂正事項６について
訂正事項６は，訂正前の「前記承認信号は前記ノードにおける電子署名の付加により生成される」のうち，「前記承認信号」を，「前記承認要求信号を受信した前記通信端末」において，「前記トランザクションへ電子署名を付加することにより」生成されると限定するものであって，訂正事項６は特許請求の範囲の減縮を目的としたものと認められる。
そして上記（１）の技術的事項２より，「第２の通信端末１１０__２内で生成される秘密鍵１１４__２によってトランズアクションが暗号化され，電子署名ＥＳ２が生成」され，「前記第２の通信端末１１０__２」によって，「トランズアクションＴＡと電子署名ＥＳ１，および前記第２の通信端末１１０__２によって生成された電子署名ＥＳ２を含む承認信号を送信する」ことを読み取ることができるから，訂正事項６は新規事項の追加に該当せず，また，実質的に特許請求の範囲を拡張し，又は変更するものではないことは明らかである。

（７）訂正事項７について
訂正事項７は，訂正前の請求項３及び４を削除するものであるから，特許請求の範囲の減縮を目的とするものである。
訂正事項７は，新規事項の追加に該当せず，また，実質的に特許請求の範囲を拡張し，又は変更するものではないことは明らかである。

（８）訂正事項８について
訂正事項８は，訂正事項１と同じ訂正事項を含むものであり，上記（１）のとおり，特許請求の範囲の減縮を目的としたものと認められる。
また上記技術的事項１及び２から，訂正事項８は新規事項の追加に該当せず，また，実質的に特許請求の範囲を拡張し，又は変更するものではないことは明らかである。

（９）訂正事項９について
訂正事項９は，実質的に訂正事項２と同様な訂正事項を含むものであり，上記（２）のとおり，特許請求の範囲の減縮を目的としたものと認められる。
また上記技術的事項２から，訂正事項９は新規事項の追加に該当せず，また，実質的に特許請求の範囲を拡張し，又は変更するものではないことは明らかである。

（１０）訂正事項１０について
訂正事項１０は，訂正事項３と同じ訂正事項を含むものであり，上記（３）のとおり，明りょうでない記載の釈明を目的とするものと認められる。
また上記技術的事項３より，訂正事項３は新規事項の追加に該当せず，また，実質的に特許請求の範囲を拡張し，又は変更するものではないことは明らかである。

（１１）訂正事項１１について
訂正事項１１は，訂正事項４と同じ訂正事項を含むものであり，上記（４）のとおり，特許請求の範囲の減縮を目的としたものと認められ，上記技術的事項４から，訂正事項１１は新規事項の追加に該当せず，また，実質的に特許請求の範囲を拡張し，又は変更するものではないことは明らかである。

（１２）訂正事項１２について
訂正事項１２は，実質的に訂正事項５と同様な訂正を含むものであり，上記（５）のとおり，特許請求の範囲の減縮を目的としたものと認められる。
また上記技術的事項１から，訂正事項１２は新規事項の追加に該当せず，また，実質的に特許請求の範囲を拡張し，又は変更するものではないことは明らかである。

（１３）訂正事項１３について
訂正事項１３は，実質的に訂正事項６と同様な訂正を含むものであり，上記（６）のとおり，特許請求の範囲の減縮を目的としたものと認められる。
また上記技術的事項２から，訂正事項１３は新規事項の追加に該当せず，また，実質的に特許請求の範囲を拡張し，又は変更するものではないことは明らかである。

（１４）訂正事項１４について

訂正事項１４は，訂正前の請求項７及び８を削除するものであるから，特許請求の範囲の減縮を目的とするものである。
訂正事項１４は，新規事項の追加に該当せず，また，実質的に特許請求の範囲を拡張し，又は変更するものではないことは明らかである。

３　小括
以上のとおりであるから，本件訂正請求による訂正は，特許法１２０条の５第２項ただし書１号及び３号に掲げる事項を目的とするものであり，かつ，同条９項において準用する同法１２６条５項及び６項の規定に適合する。
したがって，特許請求の範囲を，訂正請求書に添付された訂正特許請求の範囲のとおり，訂正後の請求項〔１－４〕，〔５－８〕について訂正することを認める。

第３　訂正後の本件発明
本件訂正請求により訂正された請求項１，２，５及び６に係る発明（以下それぞれ「本件発明１」，「本件発明２」，「本件発明５」及び「本件発明６」という。）は，訂正特許請求の範囲の請求項１，２，５及び６に記載された次の事項により特定されるとおりのものである。

本件発明１：
「互いにネットワークを介して接続される複数の通信端末により構成されるグループにおいて共有されるデータに対するトランザクションの実行に対する承認要求信号を、前記複数の通信端末の少なくとも一つに送信する手順と、
前記承認要求信号を受信した前記複数の通信端末のうちの一定割合に相当する通信端末より承認信号を受信する手順と、
前記承認信号を受信した後、前記トランザクション、および前記トランザクションの電子署名を、複数のノードで構成され、前記ネットワークに接続されたブロックチェーンネットワークにブロードキャストし、前記トランザクションに関する情報を含むブロックをブロックチェーンに追加することによって前記トランザクションを実行する手順とを含み、
前記複数の通信端末のうち少なくとも一つが前記ブロックチェーンネットワークに接続され、前記ブロードキャストを実行する、信号処理方法。」

本件発明２：
「前記承認信号は、前記承認要求信号を受信した前記通信端末において、前記トランザクションへ電子署名を付加することにより生成される、請求項１に記載の信号処理方法。」

本件発明５：
「互いにネットワークを介して接続される複数の通信端末により構成されるグループにおいて共有されるデータに対するトランザクションの実行に対する承認要求信号を、前記複数の通信端末の一つから前記複数の通信端末の他の少な

くとも一つに送信する手順と、
　前記承認要求信号を受信した前記複数の通信端末のうちの一定割合に相当する通信端末より承認信号を受信する手順と、
　前記承認信号を受信した後、前記トランザクション、および前記トランザクションの電子署名を、複数のノードで構成され、前記ネットワークに接続されたブロックチェーンネットワークにブロードキャストし、前記トランザクションに関する情報を含むブロックをブロックチェーンに追加することによって前記トランザクションを実行する手順を前記複数のノードに実行させるように構成され、
　前記複数の通信端末のうち少なくとも一つが前記ブロックチェーンネットワークに接続され、前記ブロードキャストを実行する、信号処理プログラム。」

　本件発明６：
「電子署名を前記トランザクションへ付加することにより前記承認信号を生成することを前記複数の通信端末に実行させるように構成される、請求項５に記載の信号処理プログラム。」

第４　取消理由通知に記載した取消理由について
１　取消理由の概要
　訂正前の請求項１乃至８に係る特許に対して，当審が平成３１年２月１５日に特許権者に通知した取消理由の要旨は，次のとおりである。

ア．請求項１乃至８に係る特許は，特許請求の範囲の記載が特許法３６条６項２号に規定する要件を満たしていない特許出願に対してされたものであり，取り消されるべきものである。

イ．請求項１乃至８に係る発明は，甲第１号証及び甲第３号証に記載された発明に基いて，当業者が容易に想到することができたものであって，請求項１乃至８に係る特許は，特許法２９条２項の規定に違反してされたものであり，取り消されるべきものである。

２　甲号証の記載
（１）甲第１号証に記載された事項及び引用発明
　甲第１号証（アンドレアス・Ｍ・アントノプロス，今井崇也，鳩貝淳一郎，「ビットコインとブロックチェーン 暗号通貨を支える技術」，初版，ＮＴＴ出版株式会社，２０１６年７月２１日，ｐ．１－２９６頁）には，次の事項が記載されている。

Ａ　「ビットコインとは
　ビットコインは，デジタルマネーのエコシステムの基礎となるコンセプトと技術の集合体です。ビットコインという名の通貨によって，ビットコインネットワークの参加者の間で，価値の保有と移転が行われます。ユーザ間のやり取

りは，主にビットコインプロトコルに基づいてインターネットを通じて行われますが，他のネットワークを使うこともできます。ビットコインのプロトコルスタックはオープンソースソフトウェアとして利用可能であり，ノートパソコンからスマートフォンまでさまざまなデバイス上で動作し，この技術を簡単に使えるようにしています。」（１ページ１乃至８行）

Ｂ　「

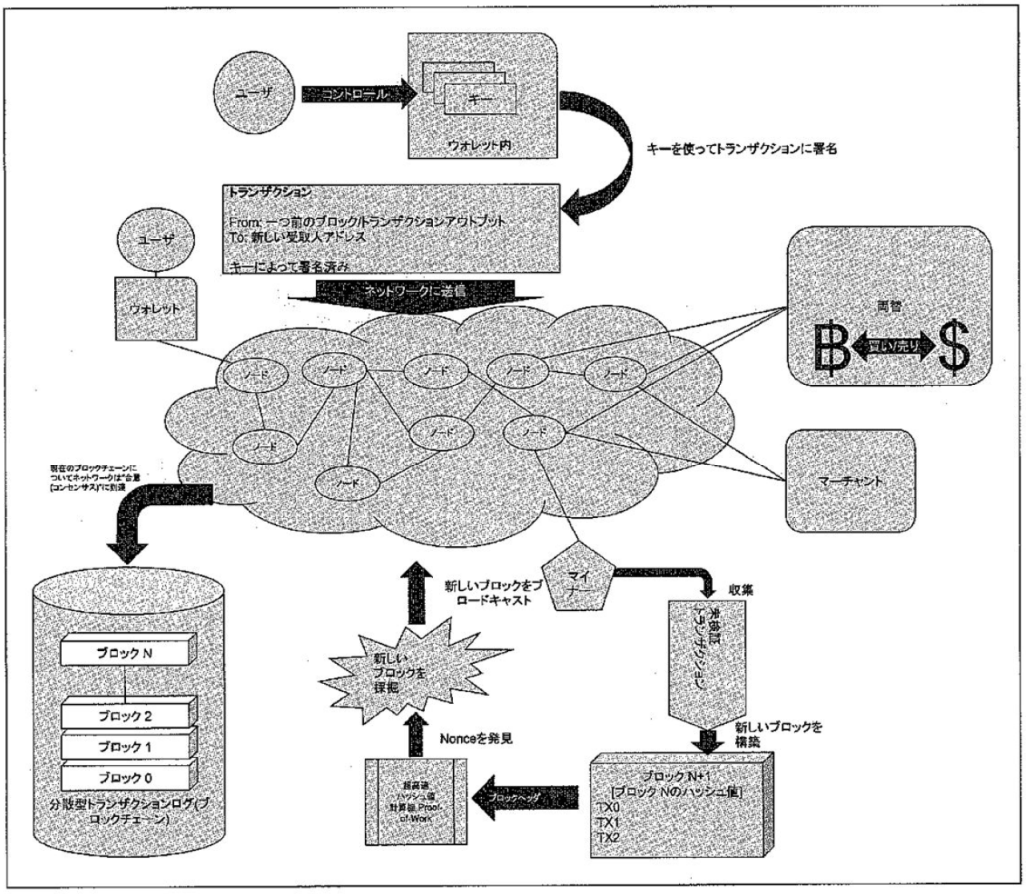

図2－1　ビットコイン概観

図２－１」（１６ページ）

Ｃ　「一言で言うと，トランザクションとはビットコインの所有者が他の人にビットコインを送ったと認めたことをビットコインネットワークに示すことです。このため，新しい所有者が受け取ったビットコインを使うには，新しい所有者が他の人にビットコインを送ったと認めたことを示す別のトランザクションを作らなければなりません。

…（中略）…

トランザクションは，それぞれのインプットごとにビットコインの所有権の証明も含んでいます。この所有権の証明はデジタル署名の形になっており，この

署名は所有者とは独立に他人によって検証されるようになっています。ビットコインの用語でビットコインを「使う」とは，トランザクションに署名することです。」（１８ページ１８乃至３３行）

Ｄ　「トランザクションはトランザクションインプットからトランザクションアウトプットに価値を移転します。インプットはどこからビットコインが来たかを示し，通常は前のトランザクションのアウトプットになります。トランザクションアウトプットは，このビットコインを鍵と紐づけることで新しい所有者にこのビットコインを割り当てます。この鍵は解除条件と呼ばれるものです。解除条件は，資金を将来トランザクションで使用するときに必要とされる署名に対する必要条件になります。１つのトランザクションからのアウトプットは新しいトランザクションの中でインプットとして使用され，これにより，アドレスからアドレスに価値が移転するときに所有の連鎖が作られるのです（図２－４参照）。」（１９ページ１乃至８行）

Ｅ　「

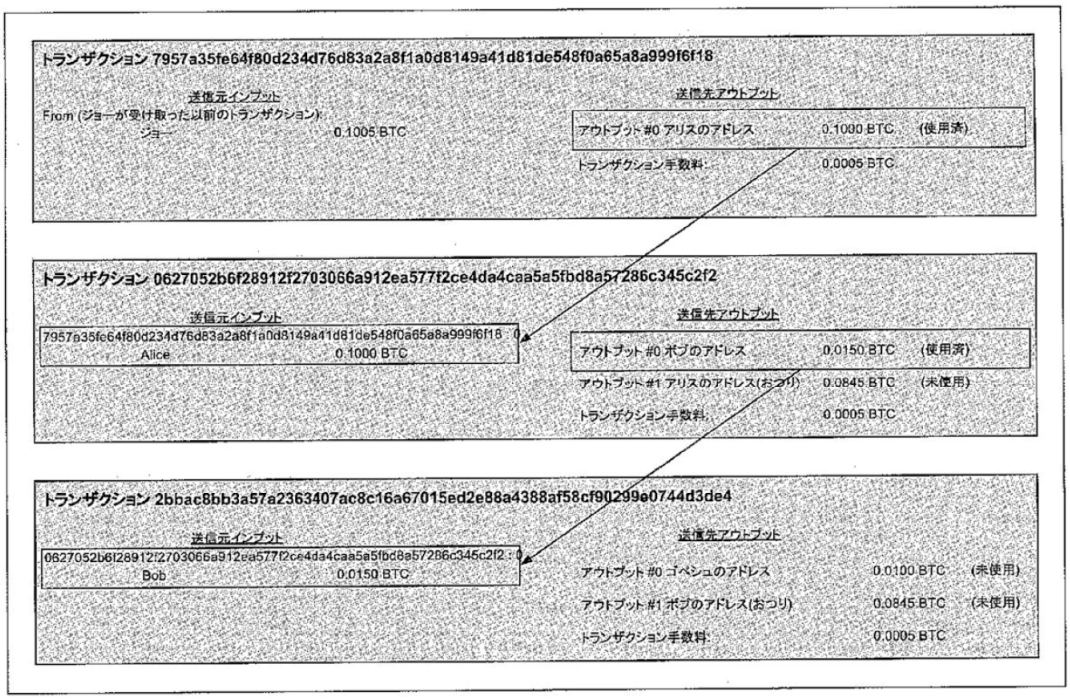

図2－4　トランザクションの連鎖。あるトランザクションのアウトプットは次のトランザクションのインプットになる。

図２－４」（２０ページ）

Ｆ　「アリスがボブのカフェで支払いをするときは，ジョーからアリスへのトランザクションを，このトランザクションのインプットとして用います。前の章で，アリスは現金と引き換えにジョーからビットコインを受け取りました。このトランザクションは，アリスの秘密鍵でロックされています。アリスからボブへの新しいトランザクションは，ジョーからアリスへのトランザクション

の内容をインプットとして参照し，コーヒー代の支払いとおつりの受け取りのトランザクションアウトプットを作成します。トランザクションはチェーンの形を取っていて，最新のトランザクションのインプットは前のトランザクションのアウトプットに対応しています。アリスの秘密鍵は前のトランザクションのアウトプットを解錠し，それによってこのアウトプットにある資金がアリスのものであるとビットコインネットワークに示すのです。アリスは，コーヒー代の支払いをボブのビットコインアドレスに紐づけます。このことによって，このアウトプットを使うためには，ボブは署名を生成しなければならなくなります。このことは，この価値の移転かアリスとボブの間のものであるということを表しています。図２－４が，ジョー，アリス，ボブの一連のトランザクションの連鎖を説明しています。」（２０ページ１乃至１４行）

Ｇ　「アウトプットの作成
　トランザクションアウトプットはスクリプトの形で作成されます。このスクリプトは，資金を使用する際の解除条件であり，これに対する解を導入することでのみ解除されます。要するに，このスクリプトが意味しているのは，「ボブのパブリックアドレスに対応する秘密鍵から作られた署名を提示する人であれば誰でも，このアウトプットが支払われる」ということです。ボブのみが，対応する秘密鍵を含むウォレットを持っているため，このウォレットのみがこのアウトプットを復号する署名を示すことができます。従って，アリスがアウトプットを復号しようとしても，ボブの署名を要求され，邪魔されてしまいます。」（２４ページ４乃至１１行）

Ｈ　「ビットコインネットワークへのトランザクションの送信トランザクションはブロックチェーンに取り込まれるための情報をすべて持っているため，どこで，どのようにビットコインネットワークに送信されても構いません。ビットコインネットワークはｐｅｅｒ－ｔｏ－ｐｅｅｒネットワークであり，個々のビットコインクライアントは，いくつかの他のビットコインクライアントと繋がることで，ビットコインネットワークに参加しています。ビットコインネットワークの目的は，トランザクションとブロックをすべてのビットコインクライアントに伝えることです。」（２５ページ１０乃至１６行）

Ｉ　「ビットコイントランザクションに関するよくある誤解は，「承認」のために新しいブロックが生成されるまで１０分間待たなければならないとか，完全な６回の承認のために６０分間待たなければならないといったことです。承認は，トランザクションがビットコインネットワーク全体に受け入れられたことを保証しますが，このように待つことはコーヒー一杯のような少額の商品には必要ありません。店舗側は，承認がない場合でも，いつも彼らが受け入れている個人ＩＤや署名がないクレジットカードよりリスクが大きくないなら，有効な少額のトランザクションを受け入れるでしょう。」（２６ページ１９乃至２５行）

Ｊ　「ビットコインマイニング

トランザクションはビットコインネットワークに伝えられました。しかし，マイニングと呼ばれるプロセスを通して検証されブロックに取り込まれるまで，共有されている元帳であるブロックチェーンの一部になることはできません。詳細な説明は第８章を参照してください。

ビットコインにおける信用の仕組みは，計算によって成り立っています。トランザクションがブロックの中に取り込まれるためには膨大な計算を必要としますが，取り込まれていることを検証するにはわずかな計算しか必要ありません。このマイニングは，以下の２つの目的のために行うものです。

・マイニングは，それぞれのブロックの中に新しいビットコインを作り出します。これは，あたかも中央銀行が新しいお金を印刷するようなものです。ブロックごとに作り出されるビットコインの量は決められており，時間とともに減少していきます。

・マイニングは，信用を作り出します。マイニングは，「トランザクションを含むブロックに十分な計算量がつぎ込まれた場合にのみ，そのトランザクションが承認される」ことを保証することによって，信用を作り出します。より多くのブロックがあるということは，より多くの計算量を要したことを意味し，従って，より多くの信用を得ていることを意味するのです。」（２６ページ２６行乃至２７ページ７行）

Ｋ　「Ｐａｙ－ｔｏ－Ｓｃｒｉｐｔ　Ｈａｓｈ　（Ｐ２ＳＨ）とマルチシグネチャアドレス

ご存知の通り，初期から使われているビットコインアドレスは「１」から始まり，秘密鍵から導出される公開鍵から作られます。誰もがビットコインを「１」から始まるビットコインアドレスに送れますが，このビットコインは，対応する秘密鍵署名と公開鍵ハッシュを示すことでのみ使用できます。

「３」から始まるビットコインアドレスはｐａｙ－ｔｏ－ｓｃｒｉｐｔ　ｈａｓｈ（Ｐ２ＳＨ）アドレスであり，ときどき誤ってマルチシグネチャアドレスまたはマルチシグアドレスと呼ばれます。これらではビットコイントランザクションの受取人を，公開鍵の所有者の代わりにｓｃｒｉｐｔのハッシュを使って指定します。この特徴は，２０１２年にＢｉｔｃｏｉｎ　Ｉｍｐｒｏｖｅｍｅｎｔ　Ｐｒｏｐｏｓａｌ　１６（〔ｂｉｐ００１６〕参照）で導入され，幅広く採用されています。というのは，この特徴により，アドレス自体に機能を追加することができるようになったためです。「１」から始まるビットコインアドレスに資金を「送る」トランザクション（ｐａｙ－ｔｏ－ｐｕｂｌｉｃ－ｋｅｙ－ｈａｓｈ〔Ｐ２ＰＫＨ〕とも呼ばれる）と違って，「３」で始まるビットコインアドレスに送った資金は，その所有権を示すために，１つの公開鍵ハッシュと１つの秘密鍵署名以上のものの提示が要求されます。要求されるものはビットコインアドレスを作ったときにｓｃｒｉｐｔの中で指定され，このビットコインアドレスへの入金にはすべて同じ要求が課されます。ｐａｙ－ｔｏ－ｓｃｒｉｐｔ　ｈａｓｈ アドレスはトランザクションｓｃｒｉｐｔから生

成され，トランザクションアウトプットを誰が使えるかということを定義しています（詳細については，第５章「Ｐａｙ－ｔｏ－Ｓｃｒｉｐｔ Ｈａｓｈ（Ｐ２ＳＨ）」節参照）。ｐａｙ－ｔｏ－ｓｃｒｉｐｔ ｈａｓｈアドレスのエンコードはビットコインアドレスを生成するときに使われる二重ハッシュ関数と同じ関数を使って行われ，公開鍵の代わりにｓｃｒｉｐｔにのみ適用されます。

…（中略）…

マルチシグネチャアドレスとＰ２ＳＨ

現在，Ｐ２ＳＨの最も一般的な実装は，マルチシグネチャアドレスｓｃｒｉｐｔです。この名前が示しているように，ｓｃｒｉｐｔは所有権を証明し資金を利用するために１つ以上の署名を要求します。ビットコインマルチシグネチャは，Ｎ個の鍵から作られるＭ個の署名（「ｔｈｒｅｓｈｏｌｄ」とも呼ばれます）を要求し，これはＭ－ｏｆ－Ｎ ｍｕｌｔｉ－ｓｉｇと呼ばれています。ここで，ＭはＮと等しいか小さい数です。例えば，第１章に出てきたカフェのオーナーのボブは，彼の鍵と彼の奥さんの鍵から作られる１－Ｏｆ－２シグネチャを要求するマルチシグネチャアドレスを使うことができ，このアドレスに紐づいたトランザクションアウトプットを使うには彼または奥さんのどちらか一方の鍵で署名すればよいのです。ゴペッシュ（ボブのウェブサィトを作ったウェブデザイナー）がビジネス用に２－ｏｆ－３マルチシグネチャアドレスを持っていたとすると，少なくともビジネスパートナーの２人がトランザクションに署名しなければ，このアドレスに紐づく資金を使うことができません。」（１０５ページ下から５行乃至１０７ページ上から８行）

Ｌ　「トランザクションのライフサイクル

トランザクションのライフサイクルは，まず組成（ｏｒｉｇｉｎａｔｉｏｎ）とも呼ばれるトランザクションの生成過程から始まります。このとき，トランザクションには署名がされますが，これはトランザクションが参照する資金を使う許可がなされたことを意味します。署名の後で，トランザクションは，ビットコインネットワークにブロードキャストされ，個々のネットワークノード（ビットコインネットワークの参加者）によって検証されながらビットコインネットワーク内を伝搬し，（ほぼ）すべてのノードに行き渡ります。最後に，トランザクションはマイニングノードによって検証され，ブロックチェーンの中のブロックに記録されます。」（１１７ページ１１乃至１８行）

Ｍ　「ビットコインネットワークへのトランザクションのブロードキャスト

ブロックチェーンに記録されるために，トランザクションはまず，ビットコインネットワークに届けられる必要があります。ビットコイントランザクションは３００～４００バイトのデータを持ち，数万ものビットコインノードのうち，どれか１つにたどり着かなければなりません。送信者は複数のビットコインノードにブロードキャストするので，ビットコインノードを信用する必要は

ありません。ノードも送信者を信用する必要がなく，また送信者が誰なのかを特定する必要もありません。トランザクションは署名されており，また一切の機密情報（秘密鍵や証明書）も含まれていないため，どのようなオープンな転送手段を使ってブロードキャストしても構いません。例えば，暗号化されたネットワークでしか送れない，機密情報が含まれるクレジットカードとは異なり，ビットコインでは，トランザクションをどのようなネットワークでも送れます。トランザクションが，どれか１つビットコインノードにたどり着ければ，送る方法は何でもよいのです。このためビットコイントランザクションは，ＷｉＦｉやＢｌｕｅｔｏｏｔｈ，ＮＦＣ，光通信，バーコード，ビットコインアドレスのウェブフォームへのコピー＆ペーストのような，安全でないネットワークを通してでも送ることかできます。」（１１８ページ１８乃至３２行）

Ｎ　「トランザクションアウトプットとインプット

ビットコイントランザクションの基本的な構成要素は，未使用トランザクションアウトプット（ＵＴＸＯ：ｕｎｓｐｅｎｔ　ｔｒａｎｓａｃｔｉｏｎ　ｏｕｔｐｕｔ）です。ＵＴＸＯは，特定の所有者にロックされた分割不可能なビットコインの固まりです。これはブロックチェーンに記録されており，ビットコインネットワーク全体により通貨の単位として認識されているものです。ビットコインネットワークは，すべての利用可能（未使用）なＵＴＸＯを把握しており，その数は現在数百万に達します。ユーザがビットコインを受け取るときはいつでも，ＵＴＸＯとしてブロックチェーンに記録されます。このため，ユーザのビットコインは，数百のトランザクションとブロックの中に，ＵＴＸＯとして散らばっています。ビットコインは，実際には，ビットコインアドレスまたは口座の残高として記録されているわけではないのです。あるのはただ，散らばって特定の所有者のみが利用できるよう設定 されたＵＴＸＯだけです。ユーザのビットコイン残高という概念は，ウォレットによって作り上げられたものにすぎません。ウォレットは，ブロックチェーンをスキャンしてユーザに属しているすべてのＵＴＸＯを掻き集め，残高を計算しているのです。」（１２０ページ下から１４行乃至末行）

Ｏ　「マルチシグネチャ

マルチシグネチャｓｃｒｉｐｔは，Ｎ個の公開鍵と，解除条件を解放する少なくともＭ個の署名が入っている条件を設定しています。これはＭ－ｏｆ－Ｎスキームとしても知られており，Ｎはキーの総数，Ｍは検証に必要な署名数です。例えば２－ｏｆ－３マルチシグネチャでは，あらかじめ登録しておいた署名者の３つの公開鍵があり，これらのうち２つを使って有効なトランザクションに対する署名を作らなければなりません。このとき，標準的なマルチシグネチャｓｃｒｉｐｔは最大でも１５個の公開鍵だけが使用できるように制限されており，これは１－ｏｆ－ｌから１５－ｏｆ－１５までのマルチシグネチャ，またはそれぞれの組み合わせを使用できるということを示しています。この制限は本書が出版されるまでに引き上げられるかもしれません。ビットコインネットワークによって現在何が許可されているかを見るために，ｉｓＳｔａｎｄ

ａｒｄ（）関数をチェックしてみてください。」（１３８ページ下から５行乃至１３９ページ上から６行）

Ｐ　「Ｐａｙ－ｔｏ－Ｓｃｒｉｐｔ－Ｈａｓｈ　（Ｐ２ＳＨ）
　ｐａｙ－ｔｏ－ｓｃｒｉｐｔ－ｈａｓｈ（Ｐ２ＳＨ）は２０１２年に導入されたもので，複雑なトランザクションｓｃｒｉｐｔをはるかに単純化した，新しい種類のトランザクションです。Ｐ２ＳＨを説明するために，実用的な例を見てみましょう。第１章で，ドバイで電子機器の輸入業を営んでいるムハンマドを紹介しました。ムハンマドの会社は，口座管理のためにビットコインのマルチシグネチャ機能を利用しています。マルチシグネチャｓｃｒｉｐｔは，ビットコインの先進的なＳｃｒｉｐｔ言語の主要な使い方の１つで，とても強力な機能です。ムハンマドの会社は，すべての顧客からの支払い（会計用語で「売掛金」）にマルチシグネチャを使っています。マルチシグネチャスキームを使い，顧客によるすべての支払いは次のような方法で安全性を担保しています。支払いを実行するには少なくとも２つの署名が必要であり，登録されている人はムハンマド，彼のパートナーのうちの１人，バックアップキーを持っている彼の代理人です。このようなマルチシグネチャスキームはコーポレートガバナンスをサポートし，盗難，横領，または紛失を防ぐ役割があります。

…（中略）…

　ｐａｙ－ｔｏ－ｓｃｒｉｐｔ－ｈａｓｈ　（Ｐ２ＳＨ）は，これらの実用的な難点を解決するために開発され，ビットコインアドレスでの支払いと同じくらい簡単に複雑なｓｃｒｉｐｔを使えるようにしたのです。Ｐ２ＳＨでの支払いで，複雑なｌｏｃｋｉｎｇ　ｓｃｒｉｐｔは暗号学的なハッシュに置き換えられます。ＵＴＸＯを使おうとするトランザクションがのちに作られたとき，このトランザクションはｕｎｌｏｃｋｉｎｇｓｃｒｉｐｔだけでなくこのハッシュとマッチするｓｃｒｉｐｔを含んでいなければなりません。簡単に言って，Ｐ２ＳＨは「このハッシュとマッチするｓｃｒｉｐｔに対して支払い，このｓｃｒｉｐｔはのちほどこのアウトプットが使用されるときに与えられます」という意味です。」（１４１ページ下から９行乃至１４２ページ下から１２行）

　以上によれば，甲第１号証は，以下の発明（以下「引用発明」という。）を開示していると認められる。

「ビットコインは，デジタルマネーのエコシステムの基礎となるコンセプトと技術の集合体であり，ユーザ間のやり取りは，主にビットコインプロトコルに基づいてインターネットを通じて行われ，ノートパソコンからスマートフォンまでさまざまなデバイス上で動作し，
　トランザクションとは，ビットコインの所有者が他の人にビットコインを送ったと認めたことをビットコインネットワークに示すことであり，それぞれのインプットごとにビットコインの所有権の証明も含み，この所有権の証明はデ

ジタル署名の形になっており，この署名は所有者とは独立に他人によって検証されるようになっていて，トランザクションインプットからトランザクションアウトプットに価値を移転し，トランザクションアウトプットは，このビットコインを鍵と紐づけることで新しい所有者にこのビットコインを割り当て，この鍵は解除条件と呼ばれ，

アリスがボブのカフェで支払いをするときは，ジョーからアリスへのトランザクションを，このトランザクションのインプットとして用い，アリスからボブへの新しいトランザクションは，ジョーからアリスへのトランザクションの内容をインプットとして参照し，コーヒー代の支払いとおつりの受け取りのトランザクションアウトプットを作成し，

最新のトランザクションのインプットは前のトランザクションのアウトプットに対応し，アリスの秘密鍵は前のトランザクションのアウトプットを解錠し，それによってこのアウトプットにある資金がアリスのものであるとビットコインネットワークに示し，

トランザクションアウトプットはスクリプトの形で作成され，このスクリプトは，資金を使用する際の解除条件であり，「ボブのパブリックアドレスに対応する秘密鍵から作られた署名を提示する人であれば誰でも，このアウトプットが支払われる」という意味のスクリプトであり得，

ビットコインネットワークはｐｅｅｒ－ｔｏ－ｐｅｅｒネットワークであり，個々のビットコインクライアントは，いくつかの他のビットコインクライアントと繋がることで，ビットコインネットワークに参加しており，

承認は，トランザクションがビットコインネットワーク全体に受け入れられたことを保証するものであり，

トランザクションはビットコインネットワークに伝えられ，マイニングと呼ばれるプロセスを通して検証されブロックに取り込まれるまで，共有されている元帳であるブロックチェーンの一部になることはできず，

「３」から始まるビットコインアドレスはｐａｙ－ｔｏ－ｓｃｒｉｐｔ ｈａｓｈ（Ｐ２ＳＨ）アドレスであり，ときどき誤ってマルチシグネチャアドレスまたはマルチシグアドレスと呼ばれ，これらではビットコイントランザクションの受取人を，公開鍵の所有者の代わりにｓｃｒｉｐｔのハッシュを使って指定し，

「３」で始まるビットコインアドレスに送った資金は，その所有権を示すために，１つの公開鍵ハッシュと１つの秘密鍵署名以上のものの提示が要求され，要求されるものはビットコインアドレスを作ったときにｓｃｒｉｐｔの中で指定され，このビットコインアドレスへの入金にはすべて同じ要求が課され，ｐａｙ－ｔｏ－ｓｃｒｉｐｔ ｈａｓｈ アドレスはトランザクションｓｃｒｉｐｔから生成され，トランザクションアウトプットを誰が使えるかということを定義しており，

ｓｃｒｉｐｔは所有権を証明し資金を利用するために１つ以上の署名を要求し，ビットコインマルチシグネチャは，Ｎ個の鍵から作られるＭ個の署名（「ｔｈｒｅｓｈｏｌｄ」とも呼ばれます）を要求し，これはＭ－ｏｆ－Ｎ ｍｕｌｔｉ－ｓｉｇと呼ばれ，

彼の鍵と彼の奥さんの鍵から作られる１－Ｏｆ－２シグネチャを要求するマルチシグネチャアドレスを使うことができ，このアドレスに紐づいたトランザクションアウトプットを使うには彼または奥さんのどちらか一方の鍵で署名すればよく，

２－ｏｆ－３マルチシグネチャアドレスを持っていたとすると，少なくともビジネスパートナーの２人がトランザクションに署名しなければ，このアドレスに紐づく資金を使うことができず，

トランザクションのライフサイクルは，まず組成（ｏｒｉｇｉｎａｔｉｏｎ）とも呼ばれるトランザクションの生成過程から始まり，このとき，トランザクションには署名がされ，これはトランザクションが参照する資金を使う許可がなされたことを意味し，署名の後で，トランザクションは，ビットコインネットワークにブロードキャストされ，個々のネットワークノード（ビットコインネットワークの参加者）によって検証されながらビットコインネットワーク内を伝搬し，（ほぼ）すべてのノードに行き渡り，最後に，トランザクションはマイニングノードによって検証され，ブロックチェーンの中のブロックに記録され，

ブロックチェーンに記録されるために，トランザクションはまず，ビットコインネットワークに届けられる必要があり，

トランザクションは署名されており，また一切の機密情報（秘密鍵や証明書）も含まれていないため，どのようなオープンな転送手段を使ってブロードキャストしても構わなく，

ビットコイントランザクションの基本的な構成要素は，未使用トランザクションアウトプット（ＵＴＸＯ：ｕｎｓｐｅｎｔ ｔｒａｎｓａｃｔｉｏｎ ｏｕｔｐｕｔ）であり，ＵＴＸＯは，特定の所有者にロックされた分割不可能なビットコインの固まりであってブロックチェーンに記録され，

マルチシグネチャｓｃｒｉｐｔは，Ｎ個の公開鍵と，解除条件を解放する少なくともＭ個の署名が入っている条件を設定しており，これはＭ－ｏｆ－Ｎスキームとしても知られており，Ｎはキーの総数，Ｍは検証に必要な署名数であり，例えば２－ｏｆ－３マルチシグネチャでは，あらかじめ登録しておいた署名者の３つの公開鍵があり，これらのうち２つを使って有効なトランザクションに対する署名を作らなければならず，

ｐａｙ－ｔｏ－ｓｃｒｉｐｔ－ｈａｓｈ（Ｐ２ＳＨ）は，複雑なトランザクションｓｃｒｉｐｔをはるかに単純化した，新しい種類のトランザクションであり，

すべての顧客からの支払い（会計用語で「売掛金」）にマルチシグネチャを使った，顧客によるすべての支払いは，支払いを実行するに少なくとも２つの署名が必要であり，登録されている人はムハンマド，彼のパートナーのうちの１人，バックアップキーを持っている彼の代理人とし，コーポレートガバナンスをサポートし，盗難，横領，または紛失を防ぐ役割があり，

Ｐ２ＳＨは「このハッシュとマッチするｓｃｒｉｐｔに対して支払い，このｓｃｒｉｐｔはのちほどこのアウトプットが使用されるときに与えられます」という意味をもつ，

信号処理方法。」

（２）甲第３号証に記載された事項

甲第３号証（「マルチシグ関連トランザクション」，［ｏｎｌｉｎｅ］，２０１７年１月１２日，ＧｉｔＨｕｂ，［２０１８年７月２６日検索］，インターネット ＜ｈｔｔｐｓ：／／ｇｉｔｈｕｂ．ｃｏｍ／ＮＥＭＪＰＭａｎｕａｌ／ＮＥＭ＿Ｔｅｃｈｎｉｃａｌ＿ｒｅｆｅｒｅｎｃｅ＿ＪＡ／ｂｌｏｂ／ｅｃｃｆ８ｂ１ａ６ｂ３９１４ｆ２ｃｄｆ１ｅ１３４１６ｂ１７４ｃ５ｅ６３ａ６６ｆ５／Ｔｒａｎｓａｃｔｉｏｎｓ／４．３．ｍｄ＞）には，次の事項が記載されている。

Ｑ 「現時点で、NEM は n 人の内 m 人（m of n）の署名が必要なマルチシグ（多重署名）アカウントをネイティブにサポートしています。

NEM のマルチシグトランザクションはフレキシビリティを念頭にデザインされています。
他のいかなるトランザクション（現時点では重要度委任トランザクション、送金トランザクション、マルチシグ変更トランザクション）
であろうともマルチシグトランザクションに変更できます。」（１ページ目「マルチシグ関連トランザクション」の項）

Ｒ 「前述のように、任意のトランザクションは、マルチシグトランザクションにラッピングすることができます。

マルチシグアカウントから別のアカウントに XEM を送信するには、送金トランザクションをラップする必要があります。
このラップによるマルチシグ化には追加で 6XEM の手数料がかかります。

以下の例では、その際の更に詳細な手順を説明しています:
前提として、マルチシグアカウント$$(M)$$は 1000XEM の残高と連署人$$(A,B,C)$$を持ち、そこから 100XEM をアカウント$$X$$に送るとします。

どの連署人も、100XEM の送金を開始する権限を持ちます。B が送金開始を提案し、A,C がそれに連署するというケースを考えてみましょう。トランザクションが受理されるまでに以下の手順が発生します。
1.「署名者」がマルチシグアカウントになっている以外は通常と変わらない、100XEM の送金トランザクションを B が作成する。
2.B が署名されていない送金トランザクションをマルチシグトランザクションにラップする
3.B はこのマルチシグトランザクションに署名し、NEM ネットワークに送る。
4.一時停止中のマルチシグトランザクションがあるという通知が A、C に対して来る。
5.そのトランザクションに対して、A はハッシュ値を計算し署名することで、

マルチシグ署名トランザクションを作成し、ネットワークに送る。
6.A と同様のことを C が行う。
7.全連署人が署名を完了したので、トランザクションはネットワークに受理され M から X へ 100XEM が送られる。

もし A または C のいずれかがマルチシグ送金トランザクションの〆切の前にマルチシグ署名トランザクションを送信しなかった場合、その送金トランザクションは無効と判断されネットワークから拒否されます。
$$M$$から$$X$$への XEM の送金は行われません。」（１ページ目最終行乃至２ページ目最終行「４．３．３マルチシグトランザクション」の項）

以上によれば，甲第３号証は，以下の技術的事項（以下，「甲３記載事項」という。）を開示していると認められる。

「n 人の内 m 人（m of n）の署名が必要なマルチシグ（多重署名）アカウントをネイティブにサポートしている NEM において，
B が送金開始を提案し，A,C がそれに連署するケースの場合，
100XEM の送金トランザクションを B が作成し，
B が署名されていない送金トランザクションをマルチシグトランザクションにラップし，
B はこのマルチシグトランザクションに署名し，NEM ネットワークに送り，
そのトランザクションに対して，A はハッシュ値を計算し署名することで，マルチシグ署名トランザクションを作成し，ネットワークに送り，
全連署人が署名を完了したので，トランザクションはネットワークに受理され M から X へ 100XEM が送られ，
もし A または C のいずれかがマルチシグ送金トランザクションの〆切の前にマルチシグ署名トランザクションを送信しなかった場合，その送金トランザクションは無効と判断されネットワークから拒否され，
$$M$$から$$X$$への XEM の送金が行われないこと。」

３　当審の判断
（１）特許法２９条２項（理由２）について

ア　本件発明１について
（ア）対比
本件発明１と引用発明とを対比する。

１）引用発明の「トランザクション」，「ｐｅｅｒ－ｔｏ－ｐｅｅｒネットワーク」，「ビットコインネットワーク」，「ネットワークノード（ビットコインネットワークの参加者）」，「ブロードキャスト」及び「信号処理方法」はそれぞれ，本件発明１の「トランザクション」，「ネットワーク」，「ブロックチェーンネットワーク」，「ノード」，「ブロードキャスト」及び「信号処

理方法」に相当する。

２）引用発明は，「デジタルマネーのエコシステムの基礎となるコンセプトと技術の集合体であ」るところの「ビットコイン」を，「ユーザ間のやり取り」を「主にビットコインプロトコルに基づいてインターネットを通じて行」い，「ノートパソコンからスマートフォンまでさまざまなデバイス上で動作」するものである。また，「ビットコインネットワークはｐｅｅｒ－ｔｏ－ｐｅｅｒネットワークであり，個々のビットコインクライアントは，いくつかの他のビットコインクライアントと繋がることで，ビットコインネットワークに参加して」いて，当該「ビットコインクライアント」を構成する上記「ノートパソコン」や「スマートフォン」などの「さまざまなデバイス」は，「互いにネットワークを介して接続される複数の通信端末」ということができる。
　そして当該「デジタルマネーのエコシステムの基礎となるコンセプトと技術の集合体であ」るところの「ビットコイン」は，複数の「ビットコインクライアント」により「構成されるグループにおいて共有されるデータ」と言い得る。
　さらに，「ビットコイン」に係る「トランザクション」についてみるに，「まず組成（ｏｒｉｇｉｎａｔｉｏｎ）とも呼ばれるトランザクションの生成過程から始まり，このとき，トランザクションには署名がされ，これはトランザクションが参照する資金を使う許可がなされたことを意味し，署名の後で，トランザクションは，ビットコインネットワークにブロードキャストされ」ることから，所定の「ビットコインクライアント」からは，「ビットコイン」に対する「トランザクション」に対する信号，すなわち「データに対するトランザクションの実行に対する」信号が，「複数の通信端末の少なくとも一つに送信」されているといえる。
　以上総合すると，引用発明と本件発明１とは，下記相違点１において異なるものの，“互いにネットワークを介して接続される複数の通信端末により構成されるグループにおいて共有されるデータに対するトランザクションの実行に対する信号を，前記複数の通信端末の少なくとも一つに送信する手順”を有する点で一致するといえる。

３）引用発明において，「トランザクション」は，「まず組成（ｏｒｉｇｉｎａｔｉｏｎ）とも呼ばれるトランザクションの生成過程から始まり，このとき，トランザクションには署名がされ」ることから，本件発明１の「トランザクションの電子署名」に相当するものが生成されていることは明らかである。さらに引用発明は，「署名の後で，トランザクションは，ビットコインネットワークにブロードキャストされ」ることから，上記１）の認定を踏まえれば，トランザクション及びトランザクションの電子署名が「ブロックチェーンネットワークにブロードキャスト」されることも明らかである。
　そして，引用発明の「ビットコインネットワーク」は，「トランザクション」が「個々のネットワークノード（ビットコインネットワークの参加者）によって検証されながら」当該「ビットコインネットワーク内を伝搬し，（ほぼ）すべてのノードに行き渡」るから，本件発明１の「複数のノードで構成され、前

記ネットワークに接続されたブロックチェーンネットワーク」であるといえ，以上総合して引用発明と本件発明１とは，“トランザクション，および前記トランザクションの電子署名を，複数のノードで構成され，ネットワークに接続されたブロックチェーンネットワークにブロードキャスト”する点で一致するといえる。

４）引用発明は，「トランザクションは，ビットコインネットワークにブロードキャストされ，個々のネットワークノード（ビットコインネットワークの参加者）によって検証されながらビットコインネットワーク内を伝搬し，（ほぼ）すべてのノードに行き渡り，最後に，トランザクションはマイニングノードによって検証され，ブロックチェーンの中のブロックに記録され」ることから，上記３）の認定と併せ，引用発明と本件発明１とは，“前記トランザクション，および前記トランザクションの電子署名を，複数のノードで構成され，前記ネットワークに接続されたブロックチェーンネットワークにブロードキャストし，前記トランザクションに関する情報を含むブロックをブロックチェーンに追加することによって前記トランザクションを実行する手順”を含む点で一致する。（なお，引用発明は，「「３」から始まるビットコインアドレスはｐａｙ－ｔｏ－ｓｃｒｉｐｔ ｈａｓｈ（Ｐ２ＳＨ）アドレスであり，ときどき誤ってマルチシグネチャアドレスまたはマルチシグアドレスと呼ばれ，これらではビットコイントランザクションの受取人を，公開鍵の所有者の代わりにｓｃｒｉｐｔのハッシュを使って指定し，

「３」で始まるビットコインアドレスに送った資金は，その所有権を示すために，１つの公開鍵ハッシュと１つの秘密鍵署名以上のものの提示が要求され，要求されるものはビットコインアドレスを作ったときにｓｃｒｉｐｔの中で指定され，このビットコインアドレスへの入金にはすべて同じ要求が課され，ｐａｙ－ｔｏ－ｓｃｒｉｐｔ ｈａｓｈ アドレスはトランザクションｓｃｒｉｐｔから生成され，トランザクションアウトプットを誰が使えるかということを定義しており，

ｓｃｒｉｐｔは所有権を証明し資金を利用するために１つ以上の署名を要求し，ビットコインマルチシグネチャは，Ｎ個の鍵から作られるＭ個の署名（「ｔｈｒｅｓｈｏｌｄ」とも呼ばれます）を要求し，これはＭ－ｏｆ－Ｎｍｕｌｔｉ－ｓｉｇと呼ばれ」るものであって，「彼の鍵と彼の奥さんの鍵から作られる１－Ｏｆ－２シグネチャを要求するマルチシグネチャアドレス」を使って，「このアドレスに紐づいたトランザクションアウトプットを使うには彼または奥さんのどちらか一方の鍵で署名すればよ」いようにしたり，「２－ｏｆ－３マルチシグネチャアドレスを持っていたとすると，少なくともビジネスパートナーの２人がトランザクションに署名しなければ，このアドレスに紐づく資金を使うことができ」なくするようなものであるが，これらの「署名」は，「トランザクションに関する情報を含むブロックをブロックチェーンに追加する」ことによって「トランザクションを実行する」こととは直接関係しないものである。）

５）引用発明の「ビットコインクライアント」は，「いくつかの他のビットコインクライアントと繋がることで，ビットコインネットワークに参加して」いて，「トランザクションは，ビットコインネットワークにブロードキャストされ」るものであることから，当該「トランザクション」を「ビットコインネットワーク」に「ブロードキャスト」する，「ノートパソコンからスマートフォンまでさまざまなデバイス」などの通信端末が存在することは明らかであり，したがって引用発明と本件発明１とは，“前記複数の通信端末のうち少なくとも一つが前記ブロックチェーンネットワークに接続され，前記ブロードキャストを実行する”点で一致するといえる。

６）以上上記１）乃至５）で検討した内容を踏まえると，本件発明１と引用発明とは，次の点で一致し，また相違する。

〈一致点〉
　互いにネットワークを介して接続される複数の通信端末により構成されるグループにおいて共有されるデータに対するトランザクションの実行に対する信号を，前記複数の通信端末の少なくとも一つに送信する手順と，
　前記トランザクション，および前記トランザクションの電子署名を，複数のノードで構成され，前記ネットワークに接続されたブロックチェーンネットワークにブロードキャストし，前記トランザクションに関する情報を含むブロックをブロックチェーンに追加することによって前記トランザクションを実行する手順を含み，
　前記複数の通信端末のうち少なくとも一つが前記ブロックチェーンネットワークに接続され，前記ブロードキャストを実行する，信号処理方法。

〈相違点１〉
　「互いにネットワークを介して接続される複数の通信端末により構成されるグループにおいて共有されるデータに対するトランザクションの実行に対する」信号が，本件発明１は「承認要求信号」であるのに対し，引用発明は，「トランザクションには署名がされ」，さらに当該「トランザクションは，ビットコインネットワークにブロードキャストされ，個々のネットワークノード（ビットコインネットワークの参加者）によって検証されながらビットコインネットワーク内を伝搬し，（ほぼ）すべてのノードに行き渡」るものであるが，「承認要求信号」であることが特定されていない点。

〈相違点２〉
　本件発明１は，「前記承認要求信号を受信した前記複数の通信端末のうちの一定割合に相当する通信端末より承認信号を受信する手順」を有し，「トランザクションを実行する」のは，「前記承認信号を受信した後」であるのに対し，引用発明は，「複数の通信端末のうちの一定割合に相当する通信端末より承認信号を受信する手順」を有することが特定されていない点。

（イ）判断

上記相違点１及び２をまとめて検討する。

まず本件発明１の「承認要求信号」についてみるに，本件明細書段落２４乃至２６によれば，第１のユーザによって，データ処理の内容とデータ処理の開始に必要な承認条件などが含まれるトランズアクションが作成され（段落２４），当該トランズアクションは，該トランズアクションを送信する第１の通信端末１１０__１において秘密鍵１１４__１が生成され，該トランズアクションＴＡを当該秘密鍵１１４__１によって暗号化した第１の電子署名（ＥＳ１）が生成され（段落２５），該第１の通信端末１１０__１によって暗号化される前（すなわち，オリジナル）のトランズアクションＴＡおよび第１の電子署名ＥＳ１が含まれる信号が「承認要求信号」である（段落２６）。

次に，本件発明１の「承認信号」についてみるに，本件明細書段落２８によれば，トランズアクションを受信した通信端末１１０のユーザによって，まずトランズアクションを承認する，あるいは承認しないという行為のいずれかが選択され，承認が選択された場合，承認する第２のユーザの保有する第２の通信端末１１０__２内で生成される秘密鍵１１４__２によってトランズアクションが暗号化され，電子署名ＥＳ２が生成され，該第２の通信端末１１０__２によって，第１のユーザから送信された承認要求信号に含まれるオリジナルのトランズアクションＴＡと電子署名ＥＳ１，および第２の通信端末１１０__２によって生成された電子署名ＥＳ２が含まれる信号が「承認信号」である。

以上から，「承認信号」は，暗号化される前（すなわち，オリジナル）のトランズアクションＴＡおよび第１の電子署名ＥＳ１が含まれる信号である「承認要求信号」が受信された通信端末において，トランズアクションの承認か非承認かの選択がなされた後生成される信号であることが読み取れる一方，引用発明においては，「トランザクション」に「署名がされ」ることや，「署名の後で，トランザクションは，ビットコインネットワークにブロードキャストされ，個々のネットワークノード（ビットコインネットワークの参加者）によって検証されながらビットコインネットワーク内を伝搬し，（ほぼ）すべてのノードに行き渡り，最後に，トランザクションはマイニングノードによって検証され」るものであるほか，「「３」で始まるビットコインアドレスに送った資金」が「その所有権を示すために，１つの公開鍵ハッシュと１つの秘密鍵署名以上のものの提示が要求され，要求されるものはビットコインアドレスを作ったときにｓｃｒｉｐｔの中で指定され」，該「ｓｃｒｉｐｔは所有権を証明し資金を利用するために１つ以上の署名を要求し，ビットコインマルチシグネチャは，Ｎ個の鍵から作られるＭ個の署名（「ｔｈｒｅｓｈｏｌｄ」とも呼ばれます）を要求」する，「Ｍ－ｏｆ－Ｎ ｍｕｌｔｉ－ｓｉｇと呼ばれ」ることや，「マルチシグネチャｓｃｒｉｐｔ」が，「Ｎ個の公開鍵と，解除条件を解放する少なくともＭ個の署名が入っている条件を設定しており，これはＭ－ｏｆ－Ｎスキームとしても知られており，Ｎはキーの総数，Ｍは検証に必要な署名数であり，例えば２－ｏｆ－３マルチシグネチャでは，あらかじめ登録しておいた署名者の３つの公開鍵があり，これらのうち２つを使って有効なトランザクションに対する署名を作らなければなら」ないことなどが特定されて

いるものの，上記に示したような承認要求信号を受信した通信端末のユーザによる，承認，非承認の選択及び当該選択に基づく承認信号の受信等については，なんら特定されておらず，また甲第１号証の上記第４　２（１）で引用した箇所以外にも，そのことを示す事項は記載されていない。さらに，このような「承認要求信号」及び「承認信号」の送受信手順は，その他甲３記載事項にも開示がなく，また本願出願前の周知技術とはいえず，本件発明１は，甲第１号証及び甲第３号証に基づいて当業者が容易になし得たものとすることはできない。

（ウ）小括
　以上のとおり，本件発明１は，甲第１号証及び甲第３号証に記載された事項に基づいて当業者が容易に発明することができたものとはいえない。

イ　本件発明２について
　本件発明２は，本件発明１を引用するものであるから，本件発明１と同じ理由により，甲第１号証及び甲第３号証に記載された事項に基づいて当業者が容易に発明することができたものとはいえない。

ウ　本件発明５について
　本件発明５は，本件発明１と概ねそのカテゴリー表現のみ異なるものであって，本件発明１と同じ理由により，甲第１号証及び甲第３号証に記載された事項に基づいて当業者が容易に発明することができたものとはいえない。

エ　本件発明６について
　本件発明６は，本件発明５を引用するものであって，本件発明５と同じ理由により，甲第１号証及び甲第３号証に記載された事項に基づいて当業者が容易に発明することができたものとはいえない。

オ　小括
　以上判断したとおり，本件発明１，本件発明２，本件発明５及び本件発明６は，甲第１号証及び甲第３号証に記載された事項に基づいて当業者が容易に発明することができたものとはいえない。

（２）特許法３６条６項２号（取消理由通知に係るもの）について
　取消理由通知において，「請求項１の「受信した前記承認信号の承認」との記載」が明確でないとする点は，上記第２　１（１）ウに示す訂正事項３によって訂正された結果，明確となった。
　取消理由通知において，「請求項２の「前記承認信号は前記ノードにおける電子署名の付加により生成される」との特定事項について，「前記ノード」は，請求項２が引用する請求項１に記載された「複数のノード」のうちいずれを示すものであるのか」が明確でないとする点は，上記第２　１（１）ア，イ及びカに示す訂正事項１，２及び６によって訂正された結果，明確となった。

取消理由通知において，「請求項３の「前記承認信号を受信する手順において受信される前記承認信号が、前記複数のノードのうちの一定割合に満たない場合」との特定事項」及び「請求項４の「前記承認は，受信した前記承認信号に含まれる前記電子署名の総数によって判断される」との特定事項」について明確でないとする点は，上記第２　１（１）キに示す訂正事項７によって訂正された結果，明確となった。

取消理由通知において，訂正前の請求項５乃至８に関し明確でないとする点は，第２　１（２）に示す訂正事項８乃至１０及び１３乃至１４によって訂正された結果，明確となった。

よって，特許請求の範囲の記載は明確である。

（３）特許異議申立人の意見について

特許異議申立人篠森重樹は，訂正の請求により，訂正前の「複数のノード」を「複数の通信端末」に訂正し，「訂正請求書と同日提出の意見書」の４ページ５行「（ｂ）相違点の検討」の項において特許権者が主張する，「訂正発明１のようにトランザクションの承認をブロックチェーンネットワークに参加していない通信端末間で行うという構成により、通信端末には、ノードにかかる大きな負荷（段落［００４１］）やブロックチェーンネットワークによって規定される条件を満たすためのハッシュ値計算（段落［００４５］など）が要求されない。このため、段落［００１０］に記載されているように、データを共有する複数のユーザの利便性が確保され、かつ、共有されるデータを安全に管理・利用することが可能となる。」といった効果を奏することが，本件明細書に記載が無く，訂正事項１及び６は，「訂正前請求項１－８発明の技術的意義を実質上拡張し，又は変更するもの」であることを主張する。（令和元年８月１６日提出の意見書（以下単に「異議申立人意見書」という。）１乃至９ページ）

しかしながら，通信端末がブロックチェーンネットワークに参加していない通信端末間でトランザクションの承認を行うことによって，「通信端末には、ノードにかかる大きな負荷（段落［００４１］）やブロックチェーンネットワークによって規定される条件を満たすためのハッシュ値計算（段落［００４５］など）が要求され」ないことは，本件明細書に記載が無く，また，訂正前の「複数のノード」を「複数の通信端末」に訂正することは，上記第２の２で示したとおり，訂正の要件に違反するものとはいえないので，上記主張は採用しない。

また，特許異議申立人篠森重樹は，異議申立人意見書において，「（理由２）」として，新たな証拠となる甲第９号証を示し，本件特許１，２，５及び６は，特許法２９条の２の規定により，取り消されるべきものである旨主張するが，異議申立書における申立ての理由に新たな理由を付加するものであって，採用の限りで無い。

また，異議申立人篠森重樹は，異議申立人意見書において，「（理由３）」として，新たに甲第１１号証を追加して本件特許１，２，５及び６が，特許法２９条２項の規定により取り消されるべきものである旨主張するが，該甲第１

１号証にも，上記第４の３（１）ア（ア）に示す相違点１及び２に係る構成を開示するものではなく，採用の限りでは無い。

（４）小括
　よって，本件発明１，２，５及び６は，甲第１号証及び甲第３号証が開示する発明から，当業者が容易に想到し得るものとはいえない。

第５　取消理由通知において採用しなかった特許異議申立理由について
１　特許法２９条１項３号（理由１）について
　特許異議申立人篠森重樹は，特許異議申立書において，訂正前の特許請求の範囲の請求項１乃至８に係る発明は，甲第１号証に記載された発明であるから，特許法２９条１項３号の規定により特許を取り消されるべきものであると主張する。
　しかしながら，上記第４の３（１）で示したとおり，本件発明１，２，５及び６は，甲第１号証に記載された発明とはいえず，特許異議申立人篠森重樹のかかる主張は，採用することができない。

２　特許法３６条６項２号（理由３）について
　特許異議申立人篠森重樹は，特許異議申立書において，訂正前の特許請求の範囲の請求項５乃至８に係る発明は不明確である旨を主張しているが，情報処理方法として特定される，請求項１及び２に記載の方法における各手順については，本件明細書の段落１４乃至５２に「第１実施形態」として説示される内容によって，当業者が把握することが可能であり，またこれを実施するためのプログラムに関しても，当業者であれば具体的なフローチャートやハードウェアとの関連について記載が無くても理解できるものであって，本件発明５及び６は明確であり，特許請求の範囲の記載は，特許法３６条６項２号の要件を満たす。
　したがって，特許異議申立人篠森重樹のかかる主張は，採用することができない。

３　特許法３６条４項１号（理由４）について
　特許異議申立人篠森重樹は，特許異議申立書において，本件明細書の発明の詳細な説明の記載が，訂正前の特許請求の範囲の請求項５乃至８に係る発明を当業者が実施することができる程度に明確かつ十分に記載されていない旨を主張しているが，上記２と同じく，明細書段落１４乃至５２の記載に接した当業者であれば，本件発明５及び６を容易に実施することができるといえ，本件明細書の記載は，特許法３６条４項１号の要件を満たす。
　したがって，特許異議申立人篠森重樹のかかる主張は，採用することができない。

４　特許法１７条の２第３項（理由５）について

特許異議申立人篠森重樹は，特許異議申立書において，訂正前の特許請求の範囲の請求項５に記載された，「前記トランザクション、および前記トランザクションの電子署名をブロックチェーンネットワークにブロードキャストし、前記トランザクションに関する情報を含むブロックをブロックチェーンに追加することによって前記トランザクションを実行する」点は，願書に最初に添付した明細書，特許請求の範囲及び図面（以下，「当初明細書等」という。）の記載からみて，新たな技術的事項を加えるものである旨を主張する。

しかしながら，その主張の主旨は，当該補正の根拠とされる，当初明細書等の段落３９乃至５１並びに図４及び５には，具体的なプログラムの構成が開示されていないことに依拠するものであるが，上記３及び４でも指摘したとおり，具体的なプログラムやその実装態様を示すまでもなく，当業者であれば当初明細書等の段落３９乃至５１並びに図４及び５に記載の事項をプログラムによって実現することは容易に実施し得るものであり，またプログラムの具体的内容の明示がなかったからといって，当初明細書等に新たな技術的事項を加えるものであるとすることはできない。

したがって，特許異議申立人篠森重樹のかかる主張は，採用することができない。

第６　むすび

以上のとおりであるから，取消理由通知に記載した取消理由及び特許異議申立書に記載した特許異議申立理由によっては，本件請求項１，２，５及び６に係る特許を取り消すことはできない。

また，他に本件請求項１，２，５及び６に係る特許を取り消すべき理由を発見しない。

また，請求項３及び４並びに請求項７及び８に係る特許は，上記のとおり，訂正により削除された。これにより，特許異議申立人篠森重樹による特許異議の申立てについて，請求項３及び４並びに請求項７及び８に係る申立ては，申立ての対象が存在しないものとなったため，特許法１２０条の８第１項で準用する同法１３５条の規定により却下する。

よって，結論のとおり決定する。

令和１年１１月２７日

審判長　特許庁審判官　仲間 晃
特許庁審判官　山崎 慎一
特許庁審判官　松平 英

〔決定分類〕Ｐ１６５１．１１３－ＹＡＡ（Ｇ０６Ｆ）
１２１
５３６

５３７
５５

審判長　特許庁審判官　仲間　晃 8834
特許庁審判官　松平　英 3146
特許庁審判官　山崎　慎一　9174