【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】令和1年12月5日(2019.12.5)

【公表番号】特表2018-537022(P2018-537022A)
【公表日】平成30年12月13日(2018.12.13)
【年通号数】公開・登録公報2018-048
【出願番号】特願2018-519754(P2018-519754)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｆ　21/64　(2013.01)
Ｇ０６Ｆ　21/62　(2013.01)
Ｇ０６Ｑ　10/06　(2012.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｚ
Ｇ０６Ｆ　21/64
Ｇ０６Ｆ　21/62　３４５
Ｇ０６Ｑ　10/06　３２６

【手続補正書】
【提出日】令和1年10月28日(2019.10.28)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
コンピュータ実施方法であって、
ポインタを用いて、分散台帳システムから、アイデンティティ所有者の少なくとも１つの属性について、少なくとも１つの証明にアクセスすることであって、前記少なくとも１つの証明は、前記分散台帳システムの少なくとも２つの状態の間で移動可能であり、前記少なくとも２つの状態は、ＶＥＲＩＦＩＥＤ状態を含み、前記少なくとも１つの証明は、暗号学的証明を含む、ことと、
前記少なくとも１つの属性に対応する値を受信することと、
前記少なくとも１つの属性についての前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあるか否かを判断することと、
前記少なくとも１つの証明を照合する責任を持つ実体を信用するかどうかを判断することと、
前記少なくとも１つの証明における前記暗号学的証明が前記少なくとも一つの属性に対応する前記受信した値の有効な証明であるか否かを判断することと、
前記少なくとも１つの証明が前記少なくとも１つの証明を照合する責任を持つ実体により電子署名されているか否かを判断することと、
前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあると判断したことに応答して、前記少なくとも１つの証明を照合する責任を持つ実体は、信用されるべきものであること、前記暗号学的証明は、前記受信した値の有効な証明であること、及び前記少なくとも１つの証明が前記少なくとも１つの証明を照合する責任を持つ実体により電子署名されていることを判断することと、
前記アイデンティティ所有者と取引を進めることと、
を含むコンピュータ実施方法。

【請求項２】
請求項１に記載のコンピュータ実施方法であって、前記分散台帳システムは、少なくとも１つのブロックチェーンを用いて実装される、コンピュータ実施方法。
【請求項３】
請求項１に記載のコンピュータ実施方法であって、前記少なくとも１つの証明は、前記アイデンティティ所有者に関連するバッジに格納され、前記ポインタは、前記バッジへの参照を含む、コンピュータ実施方法。
【請求項４】
請求項３に記載のコンピュータ実施方法であって、前記バッジは、バッジについての複数のスキーマから選択されたスキーマに従って生成され、前記スキーマは、複数の属性を含み、前記複数の属性は、前記少なくとも１つの属性を含む、コンピュータ実施方法。
【請求項５】
請求項１に記載のコンピュータ実施方法であって、前記少なくとも１つの証明の前記少なくとも２つの状態は、ＰＥＮＤＩＮＧ状態を含み、
前記コンピュータ実施方法は、前記少なくとも一つの属性に対応する前記値が前記少なくとも１つの証明を照合する責任を持つ実体により照合されたときに、前記少なくとも１つの証明を前記ＰＥＮＤＩＮＧ状態から前記ＶＥＲＩＦＩＥＤ状態に遷移させることを更に含む、コンピュータ実施方法。
【請求項６】
請求項１に記載のコンピュータ実施方法であって、前記少なくとも１つの証明の前記少なくとも２つの状態は、ＥＸＰＩＲＥＤ状態を含み、
前記コンピュータ実施方法は、前記少なくとも一つの属性に対応する前記値が最後に照合されたときに設定されたタイマーの期限切れ後に、前記少なくとも１つの証明を前記ＶＥＲＩＦＩＥＤ状態から前記ＥＸＰＩＲＥＤ状態に遷移させることを更に含む、コンピュータ実施方法。
【請求項７】
請求項１に記載のコンピュータ実施方法であって、前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあるときに限り、前記少なくとも１つの証明における前記暗号学的証明へのアクセスが許可される、コンピュータ実施方法。
【請求項８】
請求項１に記載のコンピュータ実施方法であって、前記アイデンティティ所有者は、ユーザである、コンピュータ実施方法。
【請求項９】
請求項１に記載のコンピュータ実施方法であって、前記少なくとも１つの証明は、前記分散台帳システムに格納されているデジタルアイデンティティ表現からアクセスされ、前記デジタルアイデンティティ表現は、前記アイデンティティ所有者に関連し、且つ、証明についての規則を実装するプログラムコードを含む、コンピュータ実施方法。
【請求項１０】
請求項１に記載のコンピュータ実施方法であって、前記少なくとも一つの属性に対応する前記値は、前記分散台帳システムの外部のチャンネルを介して受信される、コンピュータ実施方法。
【請求項１１】
システムであって、
少なくとも１つのプロセッサと、
少なくとも１つの非一時的なコンピュータ読み取り可能な媒体であって、前記少なくとも１つのプロセッサによって実行されたときに、前記少なくとも１つのプロセッサに、
ポインタを用いて、分散台帳システムから、アイデンティティ所有者の少なくとも１つの属性について、少なくとも１つの証明にアクセスすることであって、前記少なくとも１つの証明は、前記分散台帳システムの少なくとも２つの状態の間で移動可能であり、前記少なくとも２つの状態は、ＶＥＲＩＦＩＥＤ状態を含み、前記少なくとも１つの証明は、

暗号学的証明を含む、ことと、
前記少なくとも１つの属性に対応する値を受信することと、
前記少なくとも１つの属性についての前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあるか否かを判断することと、
前記少なくとも１つの証明を照合する責任を持つ実体を信用するかどうかを判断することと、
前記少なくとも１つの証明における前記暗号学的証明が前記少なくとも一つの属性に対応する前記受信した値の有効な証明であるか否かを判断することと、
前記少なくとも１つの証明が前記少なくとも１つの証明を照合する責任を持つ実体により電子署名されているか否かを判断することと、
前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあると判断したことに応答して、前記少なくとも１つの証明を照合する責任を持つ実体は、信用されるべきものであること、前記暗号学的証明は、前記受信した値の有効な証明であること、及び前記少なくとも１つの証明が前記少なくとも１つの証明を照合する責任を持つ実体により電子署名されていることを判断することと、
前記アイデンティティ所有者と取引を進めることと、
を実行させる複数の命令を記憶している、少なくとも１つの非一時的なコンピュータ読み取り可能な媒体と、
を備えるシステム。
【請求項１２】
請求項１１に記載のシステムであって、前記分散台帳システムは、少なくとも１つのブロックチェーンを用いて実装される、システム。
【請求項１３】
請求項１１に記載のシステムであって、前記少なくとも１つの証明は、前記アイデンティティ所有者に関連するバッジに格納され、前記ポインタは、前記バッジへの参照を含む、システム。
【請求項１４】
請求項１３に記載のシステムであって、前記バッジは、バッジについての複数のスキーマから選択されたスキーマに従って生成され、前記スキーマは、複数の属性を含み、前記複数の属性は、前記少なくとも１つの属性を含む、システム。
【請求項１５】
請求項１１に記載のシステムであって、前記少なくとも１つの証明の前記少なくとも２つの状態は、ＰＥＮＤＩＮＧ状態を含み、
前記複数の命令は、前記少なくとも１つのプロセッサによって実行されたときに、前記少なくとも１つのプロセッサに、前記少なくとも一つの属性に対応する前記値が前記少なくとも１つの証明を照合する責任を持つ実体により照合されたときに、前記少なくとも１つの証明を前記ＰＥＮＤＩＮＧ状態から前記ＶＥＲＩＦＩＥＤ状態に遷移させることを更に実行させる、システム。
【請求項１６】
請求項１１に記載のシステムであって、前記少なくとも１つの証明の前記少なくとも２つの状態は、ＥＸＰＩＲＥＤ状態を含み、
前記複数の命令は、前記少なくとも１つのプロセッサによって実行されたときに、前記少なくとも１つのプロセッサに、前記少なくとも一つの属性に対応する前記値が最後に照合されたときに設定されたタイマーの期限切れ後に、前記少なくとも１つの証明を前記ＶＥＲＩＦＩＥＤ状態から前記ＥＸＰＩＲＥＤ状態に遷移させることを更に実行させる、システム。
【請求項１７】
請求項１１に記載のシステムであって、前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあるときに限り、前記少なくとも１つの証明における前記暗号学的証明へのアクセスが許可される、システム。

【請求項１８】
請求項１１に記載のシステムであって、前記アイデンティティ所有者は、ユーザである、システム。
【請求項１９】
請求項１１に記載のシステムであって、前記少なくとも１つの証明は、前記分散台帳システムに格納されているデジタルアイデンティティ表現からアクセスされ、前記デジタルアイデンティティ表現は、前記アイデンティティ所有者に関連し、且つ、証明についての規則を実装するプログラムコードを含む、システム。
【請求項２０】
請求項１１に記載のシステムであって、前記少なくとも一つの属性に対応する前記値は、前記分散台帳システムの外部のチャンネルを介して受信される、システム。
【請求項２１】
少なくとも１つのプロセッサにより実行されたときに、方法を実行する複数の命令が符号化された非一時的なコンピュータ読み取り可能な媒体であって、前記方法は、
ポインタを用いて、分散台帳システムから、アイデンティティ所有者の少なくとも１つの属性について、少なくとも１つの証明にアクセスすることであって、前記少なくとも１つの証明は、前記分散台帳システムの少なくとも２つの状態の間で移動可能であり、前記少なくとも２つの状態は、ＶＥＲＩＦＩＥＤ状態を含み、前記少なくとも１つの証明は、暗号学的証明を含む、ことと、
前記少なくとも１つの属性に対応する値を受信することと、
前記少なくとも１つの属性についての前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあるか否かを判断することと、
前記少なくとも１つの証明を照合する責任を持つ実体を信用するかどうかを判断することと、
前記少なくとも１つの証明における前記暗号学的証明が前記少なくとも一つの属性に対応する前記受信した値の有効な証明であるか否かを判断することと、
前記少なくとも１つの証明が前記少なくとも１つの証明を照合する責任を持つ実体により電子署名されているか否かを判断することと、
前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあると判断したことに応答して、前記少なくとも１つの証明を照合する責任を持つ実体は、信用されるべきものであること、前記暗号学的証明は、前記受信した値の有効な証明であること、及び前記少なくとも１つの証明が前記少なくとも１つの証明を照合する責任を持つ実体により電子署名されていることを判断することと、
前記アイデンティティ所有者と取引を進めることと、
を含む、非一時的なコンピュータ読み取り可能な媒体。
【請求項２２】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記分散台帳システムは、少なくとも１つのブロックチェーンを用いて実装される、非一時的なコンピュータ読み取り可能な媒体。
【請求項２３】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記少なくとも１つの証明は、前記アイデンティティ所有者に関連するバッジに格納され、前記ポインタは、前記バッジへの参照を含む、非一時的なコンピュータ読み取り可能な媒体。
【請求項２４】
請求項２３に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記バッジは、バッジについての複数のスキーマから選択されたスキーマに従って生成され、前記スキーマは、複数の属性を含み、前記複数の属性は、前記少なくとも１つの属性を含む、非一時的なコンピュータ読み取り可能な媒体。
【請求項２５】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記少なく

とも１つの証明の前記少なくとも２つの状態は、ＰＥＮＤＩＮＧ状態を含み、
前記方法は、前記少なくとも一つの属性に対応する前記値が前記少なくとも１つの証明を照合する責任を持つ実体により照合されたときに、前記少なくとも１つの証明を前記ＰＥＮＤＩＮＧ状態から前記ＶＥＲＩＦＩＥＤ状態に遷移させることを更に含む、非一時的なコンピュータ読み取り可能な媒体。
【請求項２６】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記少なくとも１つの証明の前記少なくとも２つの状態は、ＥＸＰＩＲＥＤ状態を含み、
前記方法は、前記少なくとも一つの属性に対応する前記値が最後に照合されたときに設定されたタイマーの期限切れ後に、前記少なくとも１つの証明を前記ＶＥＲＩＦＩＥＤ状態から前記ＥＸＰＩＲＥＤ状態に遷移させることを更に含む、非一時的なコンピュータ読み取り可能な媒体。
【請求項２７】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあるときに限り、前記少なくとも１つの証明における前記暗号学的証明へのアクセスが許可される、非一時的なコンピュータ読み取り可能な媒体。
【請求項２８】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記アイデンティティ所有者は、ユーザである、非一時的なコンピュータ読み取り可能な媒体。
【請求項２９】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記少なくとも１つの証明は、前記分散台帳システムに格納されているデジタルアイデンティティ表現からアクセスされ、前記デジタルアイデンティティ表現は、前記アイデンティティ所有者に関連し、且つ、証明についての規則を実装するプログラムコードを含む、非一時的なコンピュータ読み取り可能な媒体。
【請求項３０】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記少なくとも一つの属性に対応する前記値は、前記分散台帳システムの外部のチャンネルを介して受信される、非一時的なコンピュータ読み取り可能な媒体。