

FinTech・ブロックチェーン特許紹介(13)
～ブロックチェーンを用いた認証方法～

2018年4月2日

河野特許事務所

所長 弁理士 河野 英仁

デジタルアイデンティティを管理するためのシステムおよび方法

米国特許 US9,667,427

特許権者 Cambridge Blockchain LLC

本特許は2016年10月14日に出願され2017年5月30日に登録された。本発明はブロックチェーン上でバッジを発行して認証を行い、当該バッジを用いて企業間・個人間のセキュアな取引を実行するアイデアである。

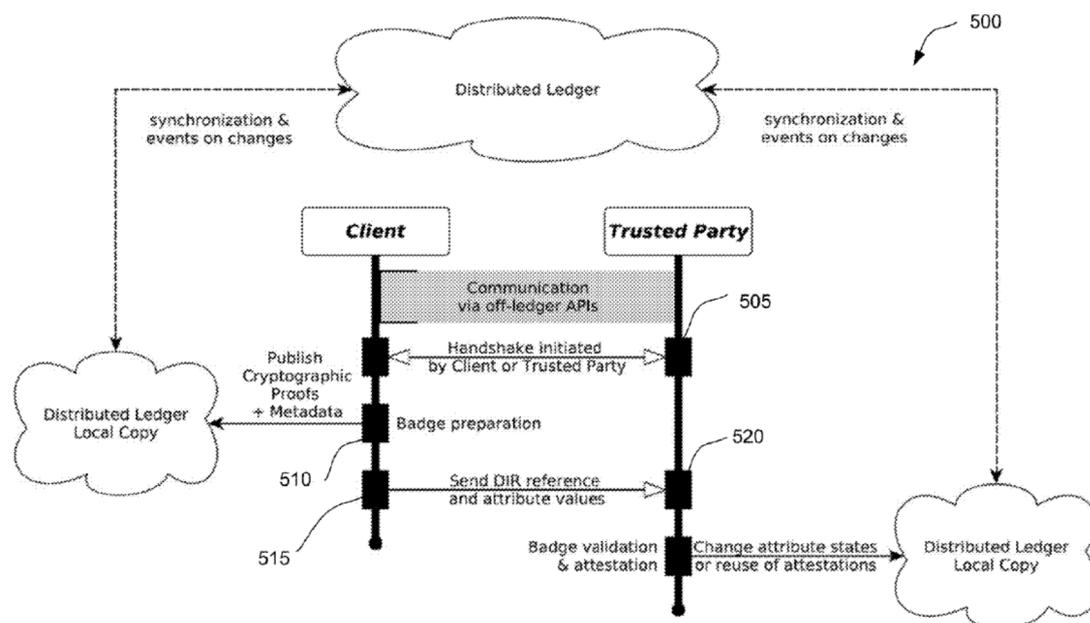
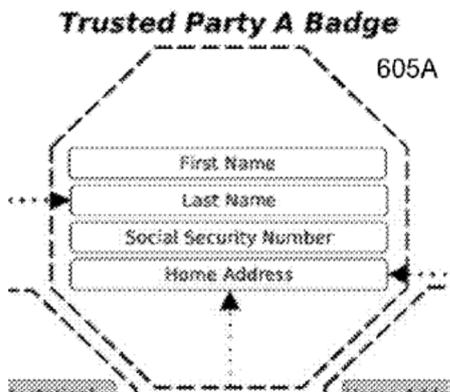


FIG. 5

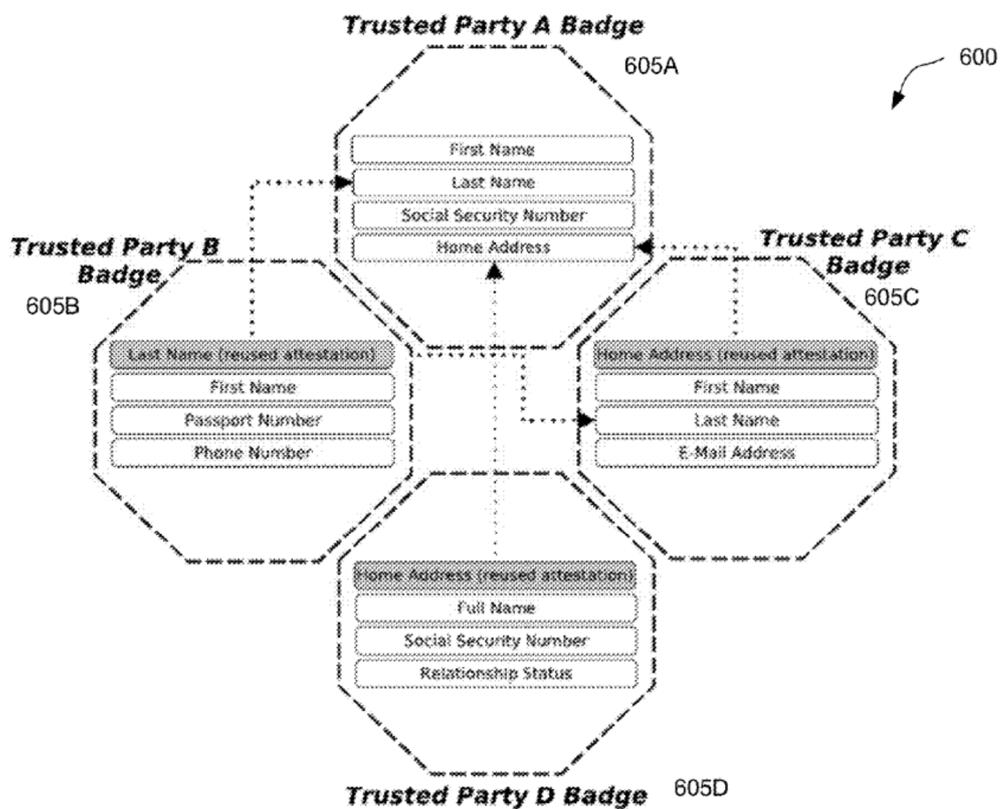
最初にユーザは、オフブロックチェーン環境において認証機関と通信を確立する(505)。次いでユーザは認証機関が発行した GUII (Globally Unique Identity Identifier) 及び特定のアルゴリズムを用いて、ユーザの属性値(名前、姓、ソーシャルセキュリティ番号、住所等のハッシュ値)を含むバッジを発行する(510)。このバッジには検証時に用いる当該アルゴリズムの種類も記述されている。



ユーザは DIR (Digital Identity Representation) を指定してバッジをブロックチェーン上へブロードキャストする (510)。次いでユーザは、認証機関に当該 DIR 及び認証を希望する属性値をオフブロックチェーンで送信する (515)。

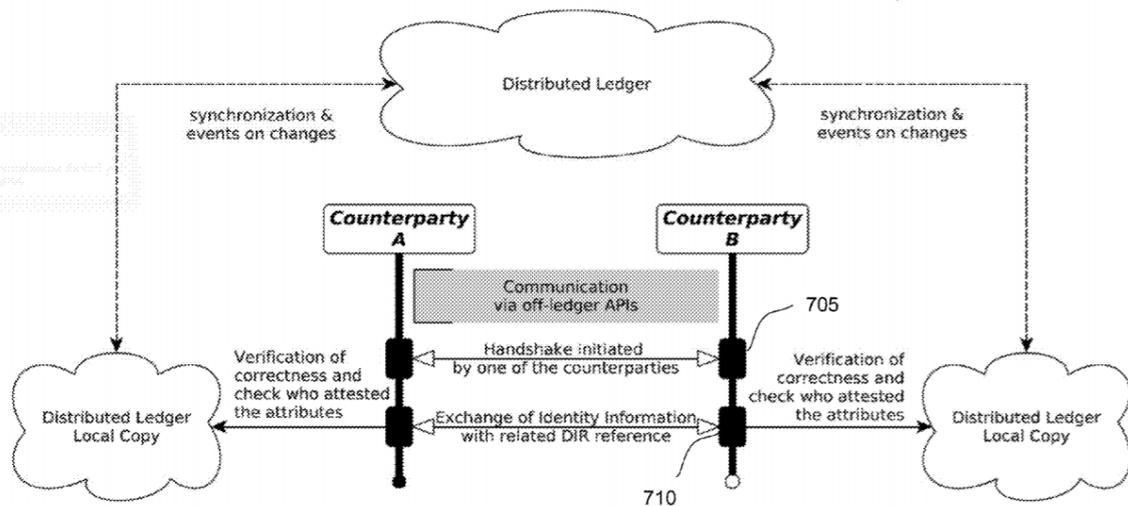
認証機関は DIR を参照してブロックチェーン上からバッジを取得する。そして認証機関はバッジ内に記述されたアルゴリズムに従い、ユーザから送信された属性値とバッジ内の属性値との検証を行う (520)。

認証機関は問題がなければバッジに VERIFIED のステータスを付与し、バッジを再びブロックチェーン上にブロードキャストする。認証機関による認証が否定された場合、バッジには INVALID とのステータスが付与される。また認証機関による認証待ちの場合、バッジには PENDING のステータスが付与される。



6

認証機関はバッジ内の名前、姓、ソーシャルセキュリティー番号及び住所の全ての属性について検証を行うほか、他の認証機関にて認証済みの項目が存在すれば、それを利用する。例えば認証機関Bについてみれば、姓 (Last Name) に関しては認証機関Aにより既に認証済みである。認証機関Bは認証機関Aにより認証されたバッジ内の姓は認証済みであるとして検証を省略することもできる。



以下に認証済みバッジを用いた活用方法を解説する。例えば上図のように不動産バイヤー(Counterparty A)と売り手(Counterparty B)とが取引を行う場合、最初に両社の間でオフブロックチェーンにて通信を確立し、氏名等の各種情報及び双方の DIR を交換する。不動産バイヤーは、売り手の DIR を参照し、ブロックチェーンから売り手の認証済みバッジを取得する。不動産バイヤーは取得した売り手のバッジが VERIFIED ステータスか否かを判断する。

そして VERIFIED ステータスである場合、不動産バイヤーはバッジに記述されたアルゴリズムに従い、バッジに記憶された属性値と、売り手の情報とを比較し検証を行う。売り手側も同様の手法により検証を行う。

個人情報を秘匿しつつ暗号化及びブロックチェーン技術を用いることでシームレス・シンプルな認証を実現している。またバッジを発行することで、取引のたびに異なる認証機関による認証を経ることなく、複数の取引においてバッジによる共通化した認証が可能となる。

ABOUT SOLUTION TEAM INVESTORS More



Cambridge Blockchain

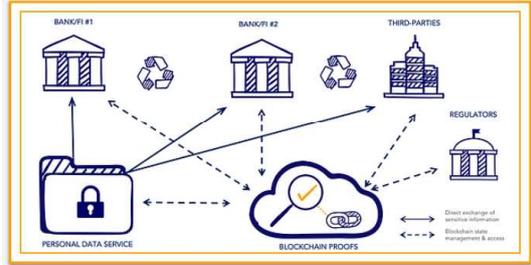
Identity compliance, simplified

Cambridge Blockchain puts control of personal identity data back in the hands of the end user. Our platform allows financial institutions to meet the strictest new data privacy rules, eliminate redundant identity compliance checks and improve the customer experience.

Cambridge Blockchain 社¹はブロックチェーンを用いた認証技術を提供する 2015 年設立の米国マサチューセッツ州の企業である。

OUR SOLUTION

Streamlining digital identity



- User control of personal identity services
- Reusable multi-platform governance efficiency
- Trust assurance for customer privacy
- Enables regulatory compliance for financial institutions, corporate clients & identity partners

Cambridge Blockchain's distributed architecture resolves the competing challenges of transparency and privacy, leading to stronger regulatory compliance, lower costs and a seamless customer experiences.

¹ Cambridge Blockchain 社 HP より 2018 年 3 月 29 日 <https://www.cambridge-blockchain.com/>



上述した特許に関わるブロックチェーンを用いた認証技術を金融機関及び企業に提供している。

以上