ブロックチェイン技術の本質機能とその発展型について

作成：２０１６年５月２２日　http://www.patentisland.com/memo368.html
著者：　Ｐａｔｅｎｔ Ｉｓｌａｎｄ株式会社（Web: http://www.patentisland.co.jp）
代表取締役社長　久野敦司　（E-mail: atsushi_hisano@patentisland.co.jp ）

【概要】

ブロックチェイン技術の輝かしい歴史は、参考サイト１の Satoshi Nakamoto の論文から始まりました。

ブロックチェイン技術は、現代社会におけるあらゆる集団的活動の基礎となる「データ無変更の保証と、データ生成者の証明」を分散型システムにて提供できるので、 ブロックチェイン技術はＩｏＴ産業革命，知的財産システム，政治および経済のシステムにおいて根本的な発展をもたらすものとＰａｔｅｎｔ Ｉｓｌａｎｄ株式会社は考え、 その本質と発展型を考察してきました。

結論から言いますと、ブロックチェイン技術の本質機能は、「インデックスｉにおいてデータＣ（ｉ）が存在し、その後も各データＣ（ｉ）が変更されずにいることを、分散型システムにて高い信頼性で保証する」 機能であると、私は考えます。
この本質機能の発展型として、「各データＣ（ｉ）ごとにデータ生成者との信頼性の高い対応付けを分散型システムにて実現する機能」を追加したものがあります。
さらにこの発展型として、「データ提供者とデータ利用者の間の信頼性の高いデータ流通を分散型システムで行なう機能」を追加したものがあります。
（ここで、インデックスｉは事象の発生順序を示す順序番号です。インデックスｉの特殊形として、時刻を示すタイムスタンプを用いることもできます。）

ブロックチェイン技術（参考サイト１）は、異なった課題の解決のための機能を大変にエレガントに統合しているため、かえってブロックチェイン技術の本質が見えにくくなっています。
したがって、本論考ではブロックチェイン技術を課題別に、その解決のための機能を、できるだけ上位概念化して抽出します。
これによって、ブロックチェイン技術の多様な形態の発想が可能になるとともに、応用範囲の拡大も行えると考えます。

まず、なぜブロックチェイン技術が必要となったのかという背景に立ち返ってみます。

現在の産業や社会のあらゆる分野の活動は、コンピュータや通信やセンサーや記憶装置などからなるデジタル情報処理システムによって大変に高度になり便利になっています。
デジタル情報処理システムは、あらゆる情報をデジタルデータに変換して処理します。 デジタルデータは、複製，保管，変更，送信，受信，加工などの行為を他のデータから独立して容易に行なえるとともに、それらの行為の痕跡が残りにくいという特性を持っています。
そして、これらの特性がデジタル情報処理システムの大きな発展の基盤となっています。

しかし、これらの特性はその反作用として、データの信頼性や信用性を担保することが大変に困難であることの根本原因にもなっています。

そこで、ブロックチェイン技術では、「データブロックをそのデータブロックの内容によって一意に決まる値であるとともに、その値の生成に大変に大きな計算パワーを必要とするという連結データを生成し、その連結データを次のデータブロックの内容の一部にするという事を繰り返して、データブロックの列（ブロックチェイン）を形成する」という方策を 用いました。
この結果、ブロックチェインの一部を構成するデータブロックでは、そのデータブロックのデータの内容の変更を、他のデータブロックに影響を与えないで行なうことが不可能と言えるほどに困難になりました。それが、「データ無変更の保証」をもたらし、データの信頼性や信用性に大きく貢献します。

言わば、「ムカデ競争」では、各人が勝手な動きができないように前後の人と結ばれているのと等価です。

（上図の出典：
http://blog.goo.ne.jp/the-second-wind/e/ec081df786c92003a28e2db91cb4b38d　）

以下、ブロックチェイン技術の本質機能を、参考サイト１の内容を起点として順番に説明していきます。

１．　「データ無変更を分散型システムにて高い信頼性で保証する」という課題を解決するための機能について

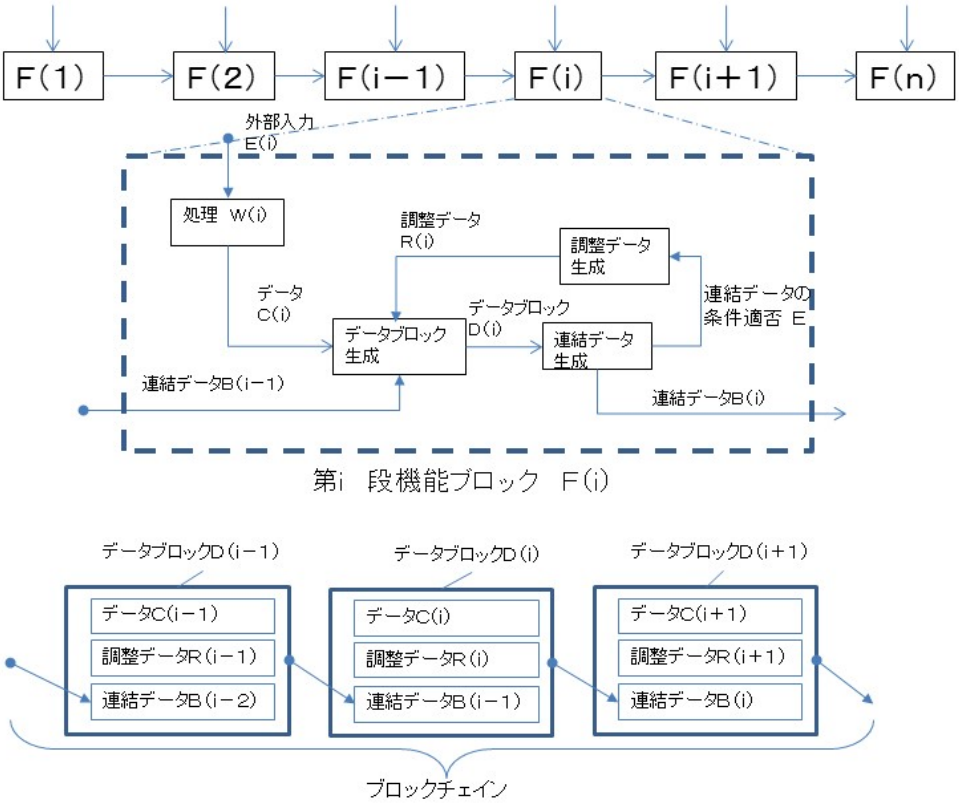
参考サイト１では、ビットコインの実現のためのブロックチェイン技術を説明しているためもあり、 参考サイト２においてもブロックチェインを「不正が難しい取引台帳」であるとしていますが、ブロックチェイン技術は取引データの処理にだけ使用されるものではないと考えます。

そこで、ブロックチェイン技術の本質を説明するために、下記の図１では取引データとは言わず、Ｃを単にデータとしました。
また、参考サイト１でいうハッシュは、前段と後段の連結機能に本質があるのであり、ハッシュ関数はその連結機能の耐改ざん性を大幅に増すものであると考え、 下記の図１では、ハッシュと呼ばず「連結データ」と呼びました。
さらに、参考サイト１では、電子署名を用いていましたが、電子署名はデータＣが取引データである場合のように、取引対象の提供者を特定するためには必要なものですが、 「データ無変更を分散型システムにて保証する」ための特徴機能ではないと考え、下記の図１では省略しました。

本論考では、ブロックチェインに組み込まれたブロック内のデータＣ（ｉ）の内容を、そのブロックチェイン内の他のブロックに影響を及ぼさずには変更することができないし、ネットワークを構成する他の多数のノードがデータが勝手には変更されていないことを保証するという「データ無変更の分散型保証」を実現する仕組みを、 特徴機能として抽出しました。
特徴機能は、次の３つです。

（１）データの変更の困難性を実現するために、前段および後段との連結データによる連鎖を利用する機能
（２）所定条件を満足するブロックをブロードキャストして、他の十分な範囲のノードからブロックチェインへの追加の承認を得る機能
（３）各ノードでの自己が保有するブロックチェイン内のブロック間の連結性および他のノードの有する連結データとの一致性を検査する機能

図1　データブロックが所定条件を満たす連結データで結合してチェーンを形成する仕組み



特徴機能１．　データの変更の困難性を実現するために、前段および後段との連結データによる連鎖を利用する機能

まず、ブロックチェイン技術を実行するシステムの構造は、時系列の順序番号である「ｉ」ごとにデータを獲得する処理W（ｉ）を内蔵する機能ブロックＦ（ｉ）が、 一列に連結した多段処理システムであり、各段の間は情報が流れていると、します。
そして、機能ブロックＦの動作を、次のようなプロセスＰ１，Ｐ２の組み合わせとして記述します。

Ｐ１：　前段である機能ブロックＦ（ｉ－１）が保持するデータブロックＤ（ｉ－１）によって一意に決定される連結データＢ（ｉ－１）と、 処理W（ｉ）で獲得したデータＣ（ｉ）と調整データＲ（ｉ）と組み合わせて、データブロックＤ（ｉ）を形成します。

Ｐ２：　前記のデータブロックＤ（ｉ）によって一意に決定される連結データＢ（ｉ）が

所定条件を満足しなければ、調整データＲ（ｉ）を変更して、 前記Ｐ１に処理を戻します。
連結データＢ（ｉ）が所定条件を満足していれば、Ｅの値に成功フラグを設定し、 Ｂ（ｉ）を後段の機能ブロックＦ（ｉ＋１）に与えます。

ここで、「機能ブロックＦ（ｉ）がデータＣ（ｉ）を確定させる」とは、前記のプロセスＰ１によって形成されたデータブロックＤ（ｉ）から生成されるとともに、 所定条件を満足する連結データＢ（ｉ）を生成して外部に出力することであるとします。所定条件を連結データＢ（ｉ）が満足するようにするために、調整データＲ（ｉ） が調整手段となります。
次に、データＣ（ｉ）の確定の後にＣ（ｉ）を変更することの困難性を説明します。
データＣ（ｉ）は、調整データＲ（ｉ）および連結データＢ（ｉ－１）と組み合わされてデータブロックＤ（ｉ）を形成しています。
そのため、Ｃ（ｉ）の変更は、データブロックＤ（ｉ）によって一意に決まる連結データＢ（ｉ）以降の各連結データの変更が必要という形で影響を後段にもたらします。
もし、後段の機能ブロックＦ（ｉ＋１）以降に気付かれないように、機能ブロックＦ（ｉ）においてＣ（ｉ）を変更しようとするならば、 Ｃ（ｉ）を変更しても連結データＢ（ｉ）を変更しなくても済むようにしなければならないことになります。

連結データＢ（ｉ）は、データＣ（ｉ）と前段からの連結データＢ（ｉ－１）と調整データＲ（ｉ）の組み合わせからなるデータブロックＤ（ｉ）から生成されますので、 データＣ（ｉ）の変更の影響が連結データＢ（ｉ）以降の後段に発生しないようにしようとするならば、適切な連結データＢ（ｉ－１）の値を探索して発見し、 そのような値に連結データＢ（ｉ－１）を変更することが必要となります。
連結データＢ（ｉ－１）の変更は、さらにその前段の連結データの変更を必要とするというように、前段方向に変更の影響が波及します。
すなわち、データブロックがプロセスＰ１とＰ２で実現されるチェインを構成しているという枠組みのもとでは、データＣ（ｉ）の変更は、 前段または後段の連結データに影響を与えてしまうので、その影響の存在を検知するプロセスと組み合わせるならば、データＣ（ｉ）の変更が困難となります。

ここで、データＣ（ｉ）の確定後にデータＣ（ｉ）を変更し、Ｃ（ｉ）の変更に応じて連結データＢ（ｉ）も変更し、連結データＢ（ｉ）を後段の機能ブロックＦ（ｉ＋１）に 与えていない状態を想定します。
その状態では、機能ブロックＦ（ｉ）が保有する連結データＢ（ｉ）と、後段の機能ブロックＦ（ｉ＋１）が前段から受け取ったものとして保有する連結データの値が相違 しますが、どちらが正しいのかの判別がつきません。

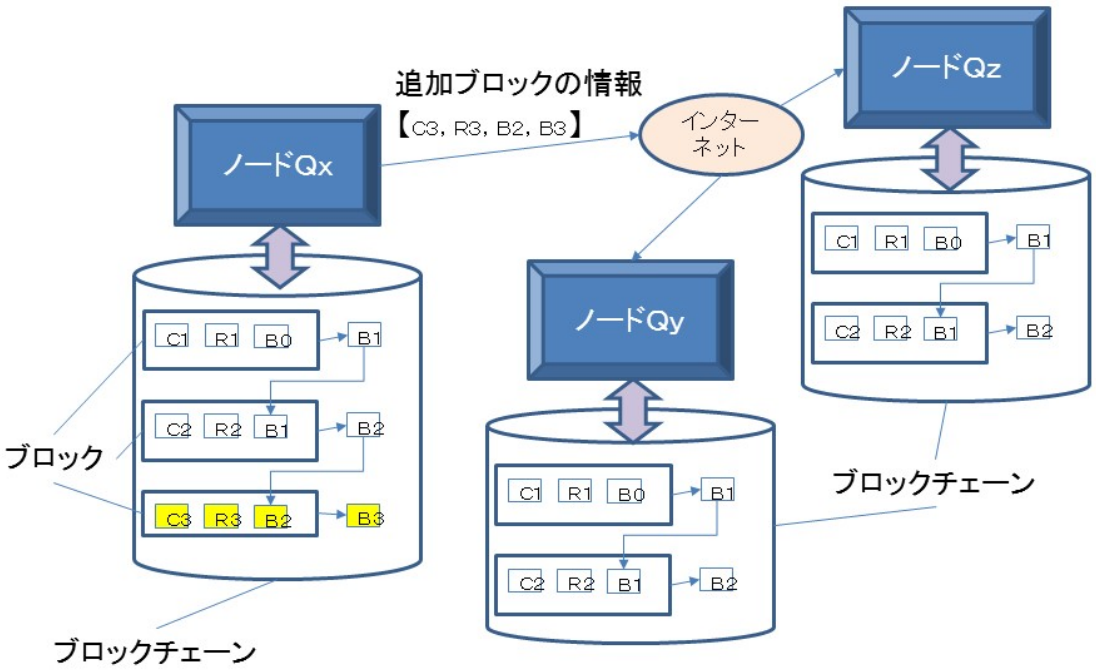
そこで、連結データＢが満足すべき条件であって、そのような条件が成立するデータブロックＤの内容は滅多に見つからないものを設けることで、データＣの確定後に データＣを変更しにくくしています。
すなわち、図１に示すように、調整データＲ（ｉ）を内部で自動生成してデータブロックＤ（ｉ）の内容を自動調整して、データブロックＤ（ｉ）に対応する連結データＢ（ｉ） が大変に多大な計算パワーを用いて初めて適切な調整データＲ（ｉ）が発見できるような難度の高い所定条件を満たす内部構造を持たせることで、 機能ブロックＦのチェインによって、データの変更がされにくいという信頼性の高いシステムを実現できることがわかります。

特徴機能２． 所定条件を満足するブロックをブロードキャストして、他の十分な範囲のノードからブロックチェインへの追加の承認を得る機能

ブロックチェインは、連結データによって連結されたブロックの列です。このブロックの列は、図１に示すような機能ブロックのチェインを内蔵するノードによって 生成されるだけでなく、そのようなノードがインターネットを介してつながっています。（図２）
各ノードは同じブロックチェインを保有するように連携しています。そのため、１つのノードがブロックチェインにブロックを追加したい場合には、他のノードにも そのブロック（追加ブロック）をブロードキャストします。ブロードキャストによって追加ブロックを受領した他のノードは、 受領した追加ブロックが所定条件を満たすかどうかを、各自で検査します。 この検査の結果、十分な範囲のノードが検査合格とした場合、そのブロックはブロックチェインの末尾に追加されます。
すなわち、ネットワークにつながった各ノードが保有するブロックチェインに新たなブロックが追加されるということです。

図2　追加ブロックのブロードキャスト

インターネットで接続された各ノードは、同一の内容のブロックチェーンを保有している。
現在のブロックチェーンに接続するブロックを追加したいノードは、所定条件を満足する
ブロックをインターネットを用いて他のノードにブロードキャストする。



特徴機能３．　各ノードでの自己が保有するブロックチェイン内のブロック間の連結性および他のノードの有する連結データとの一致性を検査する機能

この特徴機能３が必要な背景をまず、説明します。
ブロックチェインに登録済みのどれかのブロック内のデータＣを変更しようとすると、参考サイト１２の第１７ページに記載のように、変更対象のデータを有するブロックでの 連結データが変化します。しかし、その変化は連結データが所定条件（例：連結データの上位の数桁が０の連続である）を満足するというものでなければなりません。
所定条件を満足するためには、そのブロックでの調整データＲの適切な値を探索するという膨大な計算労力の消費が必要となります。
このような膨大な計算労力を費やして、そのブロックでの連結データが所定条件を満足したとしても、ブロックチェイン内のブロック間の連結性の維持のためには、 後続のブロックに与えていた連結データを変更することがさらに必要となります。そうなると、後続のブロックにおいても同様に適切な調整データＲを探索して、さらに後続に 与えるべき連結データを生成することが必要となります。

このような処理が１つのノード内で必要となるだけでなく、他のノードが保有しているブロックチェインとの一致性も保たねばならないので、 他のノードにおいても同期してブロックチェインのデータの変更を行なうことが必要となります。
ネットワークを構成する過半数を超える所定割合以上のノードにおいて、同期したブロックチェインの作り替えが行なえたならば、 ブロックチェインに登録済みのどれかのブロック内のデータＣを変更することは可能ですが、ノードが別々に管理されていることや計算能力などがばらついていることを考えると、 そのような「多数のノード間で同期したブロックチェインの作り替え」は大変に困難と言えます。

「多数のノード間で同期したブロックチェインの作り替え」に比して、ブロックチェイン内におけるブロック間の連結性の検査や、他のノードの有する連結データとの一致性の 検査は大変に小さな計算労力で実行できますので、そのような検査機能を各ノードで常時、周期的に実行することは簡単です。
そして、その周期が「多数のノード間で同期したブロックチェインの作り替え」に必要な最低時間よりも十分に短いならば、「多数のノード間で同期したブロックチェインの作り替え」 は、その途中段階で発見されて阻止でき、ブロックチェインを原状復帰させることができます。

２．　「データとデータ生成者の信頼性の高い対応付けを分散型システムで行なう」という課題の解決のための機能について

ブロックチェイン技術の説明の中では、電子署名および公開鍵暗号方式による暗号化と復号化の機能が出てきます。(参考サイト２の第１５ページ, 参考サイト１０の第１０ページ)
図１でいう機能ブロックＦ（ｉ）を実行する者であるＬが、外部からデータＥ（ｉ）を、例えばセンサーから得たり自分でキーボードなどから入力して得て、Ｃ（ｉ）を生成したとします。 その場合、Ｌをデータ Ｃ（ｉ）の生成者として、データＣ（ｉ）に対応付けるとともに、その対応付けを維持する必要があります。
それは、データＣ（ｉ）が知的財産や契約情報や個人情報や価値情報や取引情報や、データ所有権の対象としたいマシン生成情報のような、権利主体を伴なった情報である場合です。

特徴機能４．　電子署名を付随させた連結データによって、連結データのもととなったデータとデータ生成者を対応付ける機能

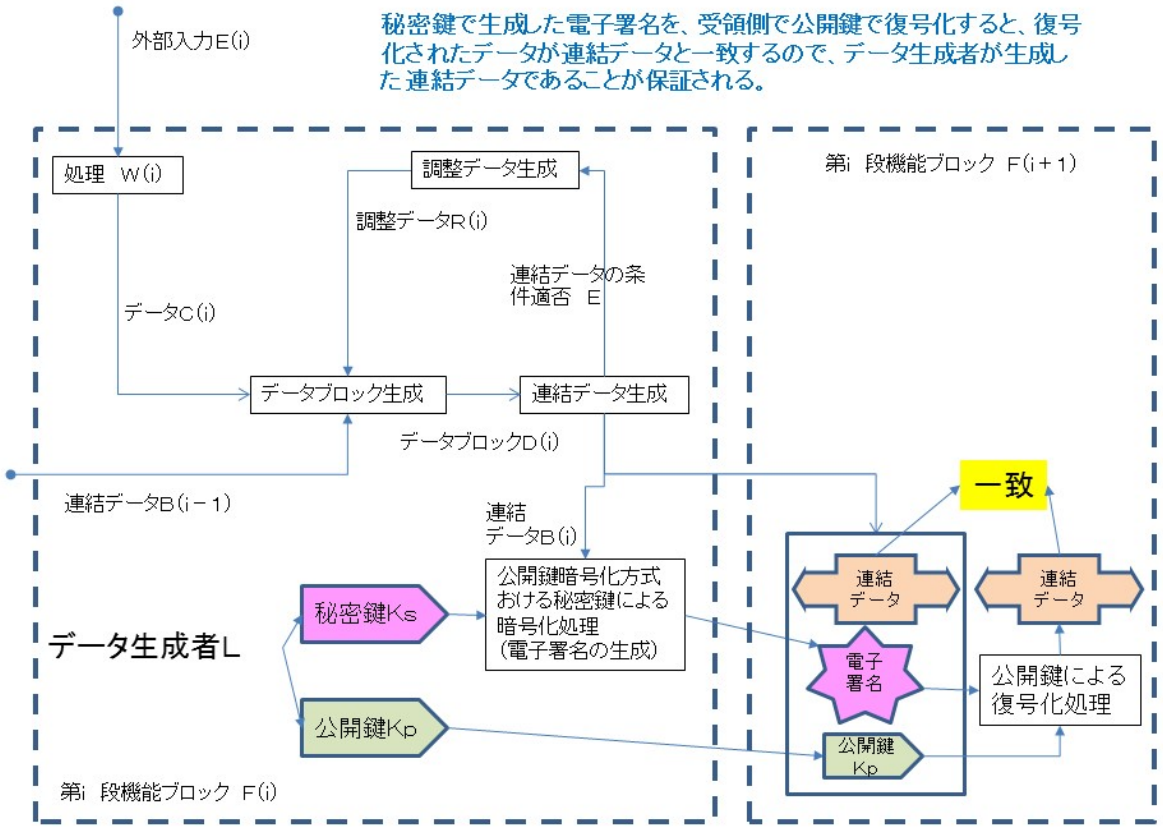
このことを、図３を用いて説明します。

（１）　まず、データ生成者Ｌは、自己を特定するものとして、公開鍵暗号化方式における秘密鍵Ｋｓと公開鍵Ｋｐの組を生成します。

（２）　データＣ（ｉ）と連結データＢ（ｉ－１）と調整データＲ（ｉ）を組み合わせたデータであるデータブロックＤ（ｉ）から得られる連結データＢ（ｉ）を、 公開鍵暗号化方式における秘密鍵Ｋｓで暗号化して、電子署名ＤＳを作成します。そして、この電子署名ＤＳと公開鍵Ｋｐと連結データＢ（ｉ）を組にして、 機能ブロックＦ（ｉ＋１）に与えます。

（３）　機能ブロックＦ（ｉ＋１）では、公開鍵Ｋｐを用いて電子署名ＤＳを復号化します。電子署名ＤＳがデータ生成者によって作成された真正なものであれば、 ＤＳの復号化によって連結データＢ（ｉ）と一致するデータが出現し、機能ブロックＦ（ｉ＋１）においても、 連結データＢ（ｉ）が公開鍵Ｋｐで示されるデータ作成者Ｌに対応付けられます。

図3　データCと、データ生成者Lを対応付ける仕組み



３．　「データ提供者とデータ利用者の間の信頼性の高いデータ流通を分散型システムで行なう」という課題の解決のための機能について

データ提供者とデータ利用者の間のデータ流通を実行するためには、分散型システムで行なう場合でも、そうでない場合でも、次の機能が必要となります。
（Ｆ１）データ提供者が提供可能なデータの属性と提供条件を示した提供側メタデータを用意する機能
（Ｆ２）データ利用者が利用を希望するデータの属性と利用条件を示した利用側メタデータを用意する機能
（Ｆ３）提供側メタデータと利用側メタデータに基づいて、データ提供者からデータ利用者に提供する対象データとデータ提供者とデータ利用者を決定する機能
（Ｆ４）対象データをデータ提供者からデータ利用者に送るデータ移転機能
（Ｆ５）データ移転の実績データを記録する機能
（Ｆ６）データ移転の実績データに基づいて、データ移転に伴う対価の支払いなどの精算をする機能

対象データが、センシングデータ等のデータであって、Ｆ３とＦ４を自動実行するシステムが、Ｓｅｎｓｅｅｋであると考えます。
対象データが「価値情報」であって、Ｆ４とＦ５を自動実行するシステムが、ビットコインシステムであると考えます。

ブロックチェイン技術を用いてデータ流通の信頼性を上げるには、次の特徴機能５の実現が有効であると考えます。

特徴機能５．　対象データの連結データをデータ利用者の公開鍵で暗号化たものと、前記の連結データにデータ提供者の電子署名を付与したものを、 データ利用者に送る機能

【参考サイト】
１．　Bitcoin: A Peer-to-Peer Electronic Cash System
http://bitcoin.peryaudo.org/vendor/bitcoin.pdf
２．　ブロックチェインの基本的な仕組み
http://www.slideshare.net/cookle/5-58379474
３．　ブロックチェイン
https://ja.wikipedia.org/wiki/%E3%83%96%E3%83%AD%E3%83%83%E3%82%AF%E3%83%81%E3%82%A7%E3%83%BC%E3%83%B3

４．　ブロックチェーンの仕組みとその可能性
http://fis.nri.co.jp/ja-JP/publication/kinyu_itf/backnumber/2015/10/201510_07.html
５．　平成２７年度 我が国経済社会の情報化・サービス化に係る基盤整備（ブロックチェーン技術を利用したサービスに関する国内外動向調査）報告書
http://www.meti.go.jp/press/2016/04/20160428003/20160428003-2.pdf
６．　ブロックチェーンをもう一段深く理解する
http://wazanova.jp/items/1314
７．　ブロックチェーンの正体
http://jp.techcrunch.com/2015/10/19/blockchain/
８．　ブロックチェーンでどこまでできるの? その可能性と課題を探る
http://news.mynavi.jp/articles/2016/04/19/blockchain_nttd/
９．　Bitcoin の仕組み
http://bitcoin.peryaudo.org/design.html
１０．　ブロックチェーン技術の基本と応用の可能性
http://www.slideshare.net/ks91020/ss-58535780
１１．サルでも分かるビットコイン ?Bitcoin の仕組みを理解しよう?
http://kivantium.hateblo.jp/entry/20140228/p1
１２．深読みビットコイン (2) コンセンサスの行方
http://www.slideshare.net/ks91020/ks91-consensusebisu20150227

１３．Bitcoin を技術的に理解する
http://www.slideshare.net/kenjiurushima/20140602-bitcoin1-201406031222
１４．電子署名の仕組み
http://esac.jipdec.or.jp/intro/shikumi.html