

検索可能暗号を利用したブロックチェーンアドレスの生成

鈴木貴之¹ 吉野雅之¹ 長沼健¹ 佐藤尚宜¹

概要: Bitcoinをはじめとする仮想通貨はブロックチェーン(BC)技術により実現されている。BC 技術を活用することで耐障害性・改ざん不可という特徴を備えたシステムを構築でき、様々な分野で適用が検討されている。BC 技術を実装した BC システムでは参加者間の取引をトランザクション呼び、これを全員が記録する。各参加者は送受信者の匿名化や用途に応じた使い分けのためにトランザクションに指定するアドレスを複数持つ。アドレスは BC システムで利用する公開鍵情報から生成されるため、利用するアドレスが多いほど管理すべき鍵情報と検索処理における検索対象が増加し、安全性と効率性が低下する傾向にある。そこで、本稿では確率的検索可能暗号の暗号文をアドレスとして活用する方法を提案する。これにより、システム提供者が安全に管理しなければならない鍵情報の数を削減すると共に、BC に登録されたトランザクションの検索処理を効率的に行うことができる。

Generate Blockchain Address by Using Searchable Encryption

TAKAYUKI SUZUKI¹ MASAYUKI YOSHINO¹
KEN NAGANUMA¹ HISAYOSHI SATO¹

1. 概要

近年、Bitcoin[1]をはじめとする様々な仮想通貨が高騰して注目を集めると共に、その活用方法についての議論も活発になってきている。これらの仮想通貨を実現する技術であるブロックチェーン(BC)は、仮想通貨以外にも活用できることが期待されており、Ethereum[2]をはじめ、BC を実装した様々なプラットフォームが提案されている。BC は分散システムであり、BC 利用者間でネットワークを構築し(以下、このネットワークを BCN と呼ぶ)、それぞれが同じデータを共有する。参加者の誰もが全てのデータを閲覧可能であるためデータの秘匿性がなく、送受信者が特定される可能性がある。

この送受信者が特定される問題に対し、Bitcoin では送受信者・受信者が複数のアドレスを使うことで対応している。具体的には、取引毎に異なるアドレスを利用することで、取引記録から利用者を特定することを困難にしている。なお、Bitcoin では送受信者のアドレスは公開鍵から生成する。このため、アドレスから送受信者が特定されることを避けるためには、利用者は大量の公開鍵ペアを生成する必要がある。大量の鍵ペアを生成する方法として、BIP 32[3]が提案・実装されている。ただし、生成される秘密鍵は安全に扱わなければならない、鍵ペアが多くなるほど秘密鍵の管理に注意を払う必要がある。

また、アドレスの匿名化を実現するために大量の公開鍵ペアを作成すると、その管理が課題になる。特に、BCN へ

の接続手段がサービスとして提供される場合や、IoT 環境において低スペック機器の代理として BCN に接続する機器を設置した場合、この BCN 接続部は利用者や IoT 機器の鍵情報を大量に保有する必要があるため、影響が大きい。また、取引情報を検索する場合、アドレスが複数個あれば検索処理も複数回実行する必要がある。

これらの課題を解決するため、BC で利用するアドレスに検索可能暗号[4]を利用する。アドレスを生成するためのキーワードを設定し、これを入力として暗号文を生成する。この生成した暗号文をアドレスとして利用することで、アドレス利用者の匿名性を担保すると同時に、1 度の検索処理で複数のアドレスを取得可能にする。この方法により、複数の公開鍵を管理する手間がなくなって機密情報を減らすことができ、検索処理も既存手法よりシンプルに実現することができる。

以下、2 章で BC の概要を、3 章で本稿で利用する検索可能暗号について説明する。その後、4 章で検索可能暗号を BC アドレスに適用する方法とその利点を紹介し、5 章で本稿についてまとめる。

2. ブロックチェーン概要

BC とは、BCN 参加者同士でピアツーピアのネットワークを構成し、それぞれが全く同じデータを保有する分散システムである。この構成により、いずれかの場所で障害が発生してもシステム全体は問題なく動作できる特徴を持つ。

また、BCN に登録される取引データであるトランザクションは、ブロックという構造に格納されて保持される。ブロックのサイズには上限があり、入りきらないトランザク

¹ (株)日立製作所 研究開発グループ システムイノベーションセンタ,
〒244-0817 横浜市中区吉田町 292 番地

ションは以降のブロックに格納される。各トランザクションは、参加者もしくは参加者の代表が検証した上でブロックに格納し、各ブロックには1つ前のブロックから算出したハッシュ値を含める。ブロックが生成されるごとに過去のデータから生成されるハッシュ値を含む構造になっているため、データの改ざんが困難なシステムとなっている。また、生成したブロックは BCN 参加者に送信し、参加者全員が同じデータを保有する。

また、BCN に登録するトランザクションも、トランザクション発行者が署名をつけた上で処理を依頼する。このため、登録者が確実に処理を依頼したことが保証される。その一方で、署名から送信者が特定される可能性が高まる。利用者が、宛先情報であるアドレスに常に同じ物を利用している場合も同様である。アドレスから利用者が特定されることを防ぐために、アドレスを使い捨てにする方法が利用されている。つまり、利用者は送信時や受取時において都度アドレスを生成し、それを使って取引を行う。なお、Bitcoin や Ethereum ではアドレスは公開鍵から生成される。このため、常に異なるアドレスを生成することで匿名性を担保できる一方、大量の公開鍵が必要になる。この鍵生成をルール化して大量の鍵情報の移行を容易にするために BIP 32 が提案・実装されている。BIP 32 ではマスタシードからマスタとなる秘密鍵(マスタノード)を生成し、ここから子供・孫の秘密鍵を作成してそれらに対応する公開鍵を作成する。送受信者の匿名化だけでなく、取引額や回数、取引先などに応じて利用する秘密鍵を割り当てて、セキュリティレベルに応じて各鍵を安全に管理するために鍵を分ける用途にも活用できる[5]。

BC 技術を提供するプラットフォームには、大きくパーミッションレス型とパーミッション型の2種類の構成がある。パーミッションレス型は誰でも参加できるものであり、Bitcoin や Ethereum がこれに相当する。パーミッション型は許可を与えられた者だけが参加できるもので、例えば Hyperledger Fabric[6]や Corda[7]がこれに相当する。

3. 検索可能暗号

検索可能暗号とは、データが暗号化された状態で検索を可能にする暗号技術である。近年、利用者のデータが手元の機器ではなく企業やクラウドに構築されたストレージに格納されることが多い。このような環境に適用することで、ストレージ・サービス提供者から利用者データの保護を実現する。検索可能暗号を利用した際の処理イメージを図1に示す。

検索可能暗号は、柔軟な鍵管理ができる公開鍵暗号を利用するものと、高速に処理できる共通鍵暗号を利用するものの2種類に大別できる。本稿では処理時間を重視し、共通鍵暗号を使った検索可能暗号[4]を利用する。この暗号方式は暗号状態で完全一致を判別でき、確率的暗号、つまり

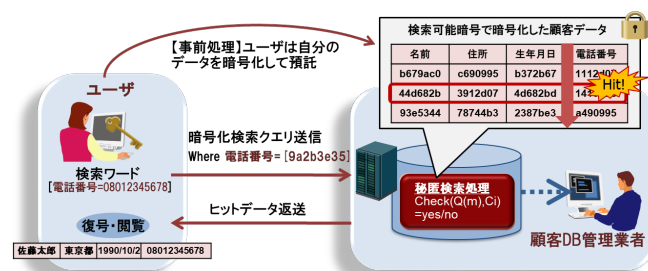


図1 検索可能暗号概要

Fig. 1 Overview of Searchable Encryption

同じ入力データから異なる暗号データを生成するという特徴を持つ。

また、暗号データの検索処理にも暗号化したクエリを利用する。これは、平文クエリを送信することで、データ検索者からの情報漏洩を防ぐためである。暗号クエリも確率的暗号であるため、暗号データと暗号クエリからはデータ間の関係性がつかめず、安全性が高い。暗号クエリの生成には秘密鍵を利用するが、検索処理に秘密鍵は不要である。このため、検索処理の実行場所に制約はない。検索処理では、暗号データと暗号クエリを入力とする独自処理を使って一致判定する。

4. 検索可能暗号を使った BC アドレス

BC に対して処理を依頼する際、そのトランザクションには依頼者の署名をつける。このため、BC 利用者は署名をつけるために公開鍵と秘密鍵の鍵ペアを保有する必要がある。また、秘密鍵は自身で安全に管理しなければならない。しかし、BC が様々な分野で利用されるようになると、鍵の重要性を強く意識しない利用者や、鍵管理を煩わしく思う利用者も増加することが想定される。そのほか、組み込み機器などのリソースが限られた環境における機器では、鍵情報の保持や署名実行が難しい状況がありうる。このような背景を考慮すると、利用者や低リソース機器の代わりに秘密鍵管理と BC へのトランザクションの送信と検索を代理実行するサービスや機器が現れる。以下、この代理処理機能部を BCN 接続部と呼ぶ。BCN 接続部では複数の鍵を管理する必要がある。鍵は秘密情報であるため、安全に管理しなくてはならないが、その数が多くなると管理コスト及び安全性において課題が発生する。また、自分の取引を匿名化するために BIP 32 のような仕組みを使って大量の鍵を生成していた場合は、管理対象の鍵の数がさらに多くなるため、この課題が複雑化する。

このような BCN 接続部の課題を解決する一つの方法として、検索可能暗号として生成された暗号文を BCN のアドレスとして利用することを提案する。以下、具体的な利用方法とその結果得られる利点について説明する。

4.1 検索可能暗号の BC アドレスへの適用

本稿で利用する検索可能暗号は、1つの入力値に対して

1つの暗号文を出力する。しかし、同じ入力値を何度設定しても、異なる暗号文を出力する特徴を持つ。生成された暗号文は、入力情報と暗号鍵を知らない人からは乱数にしか見えないため、BCNにおいても送受信者を一意に特定できないアドレスとして利用できる。図2にBIP 32による鍵とアドレスを生成した場合と、本方式でのアドレス生成の違いを示す。なお、図2ではBCN接続部が複数の利用者の情報を保持している状況を表している。図2上に示すBIP 32では、マスタシードからマスタノードを生成し、ここから任意個の子供・孫の鍵ペアを生成して利用する[3]。このため、BCN接続部はマスタシードを起点として生成される複数個の鍵ペアを管理する必要がある。図2下は提案方式であり、検索可能暗号を生成する機能部と、この機能用の鍵情報が存在する。BCN接続部は利用者毎に鍵ペアを管理するが、アドレスには、例えばIDなどの利用者を特定する情報を入力として生成された検索可能暗号文を利用する。このため、1利用者の鍵ペアに対して複数個のアドレスを関連付けることが可能になる。以下、アドレスに検索可能暗号を適用した際に得られる利点について説明する。

4.1.1 秘匿対象データの削減

図2上に示すように、従来方式では利用者の特定を防ぐために大量のアドレスが必要になるため、生成するアドレス数に対応する鍵ペアを生成しなければならない。一方、提案方式では1つの入力情報から複数個のアドレスを生成できる。このため、提案方式は従来方式に比べて厳重に管理すべき秘密鍵の個数を減らすことができる。図2のようなシンプルな例では、利用者が n 人、一人当たりのアドレス数を m 個とすると、従来手法は $n(m+2)$ 個、提案手法では $n+1$ 個の秘密情報を管理すればよく、個数を約 $1/m$ に減らすことができる。なお、従来手法の「+2」は鍵ペアを生成する際に利用するマスタシードとマスタノードの数であり、提案手法の「+1」は検索可能暗号を生成するための暗号鍵の数である。

4.1.2 アドレス情報管理の改善

複数個のアドレスを生成する別の理由として、家族間での送金、少額決済、得意先への支払いなど、利用先や用途に応じてアドレスを使い分ける使い方がある。用途に応じて使い分けるためには、それぞれの用途毎に鍵ペアを作成する必要があり、「どの鍵ペアをどの用途に利用したか」を管理しなくてはならない。鍵情報そのものは、見た目だけの区別は難しく、アプリケーションやサービス側でこれらの情報を管理する仕組みが必要になる。

これに対し、検索可能暗号を利用すると、暗号生成時に入力する情報で区別することが可能になる。つまり、アドレスとして利用する暗号文を生成する際に、利用用途の情報を入力として暗号文を生成できる。例えば「母」「孫」のような宛先や「通信費」などの利用用途をキーワードとして入力し、出力される暗号文をアドレスとして利用するこ

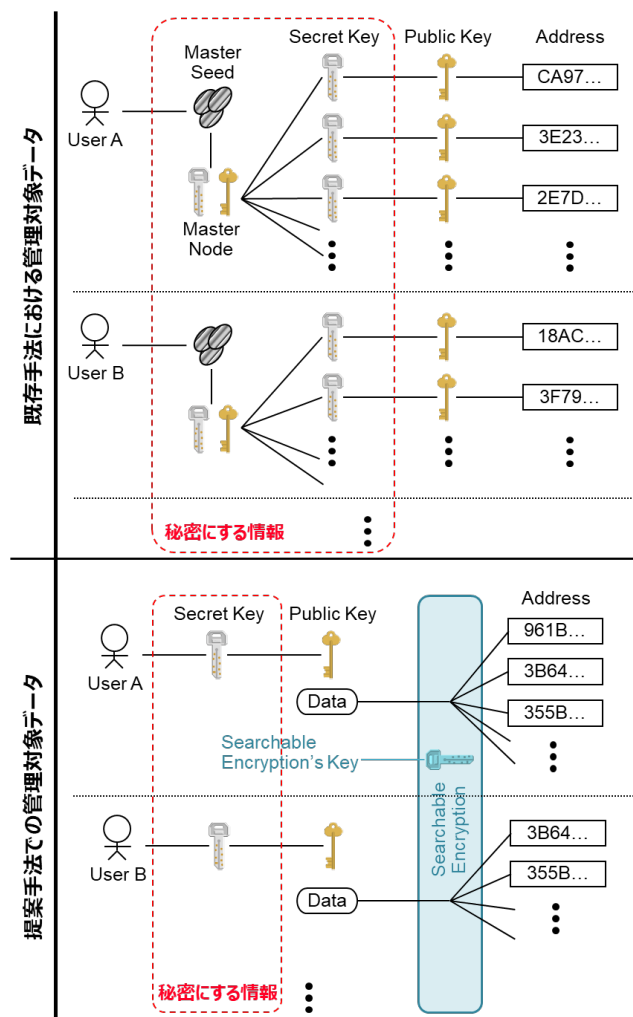


図2 従来手法と本手法における管理情報の違い

Fig. 2 Difference of Existing Method and Proposed Method

とができる。このように、検索可能暗号を活用することで利用者からは直感的に、サービス提供者も余計な管理情報を保有することなく、アドレスを使い分けることが可能になる。

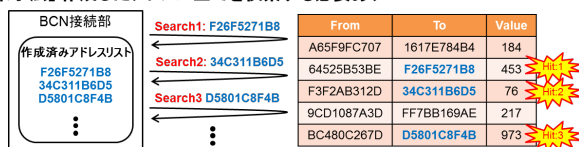
4.1.3 トランザクション検索の効率化

検索可能暗号を利用することで、BCに登録されたトランザクションの検索も効率的に処理できる。既存方式と提案方式におけるトランザクションの検索方法の違いについて、図3に処理イメージを示す。

図3上のように、既存方式では、利用者が生成した大量のアドレスに対して、BCN接続部が何度も検索処理を実行する必要がある。これに対しアドレスを検索可能暗号化し場合は、図3下に示すように利用者のトランザクションを取得するための検索クエリを作成し、このクエリとのマッチング処理を実行して検索処理を実施する。利用した検索可能暗号の特徴から、作成した検索クエリに対応する複数のトランザクションが1度の検索処理で取得できる。

このため、トランザクションを検索するためにアドレス情報を複数保有する必要がなく、検索処理自体のシンプル

【従来手法】作成したアドレス全てを検索する必要あり



【提案手法】暗号クエリを生成し、検索指示は1回

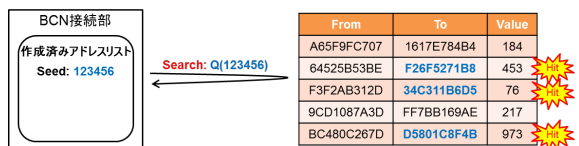


図 3 提案方式による検索方法の違い

Fig. 3 Difference of Existing Method and Proposed Method

に実装することができる。用途や宛先に応じてアドレス生成用の情報を複数個持つ場合でも、従来方式に比べて管理する情報を削減することが可能になる。

なお、トランザクションはブロックに格納される。このため、まずトランザクションが格納されているブロックを特定し、ブロック内を検索することでより効率的に検索できるが、本稿ではこの検索については対象外とする。

4.2 検索可能暗号化したアドレスから鍵ペア導出

検索可能暗号をアドレスに利用することで、アドレスと対応した公開鍵を生成する必要がなくなるため、不要な鍵ペアやアドレスを管理する必要がなくなる。しかし、4.1節で説明した方法ではアドレスは複数個持てるが、公開鍵は一つである。このため、アドレスを複数個使い分けても同じ公開鍵を利用することになるため、送受信者の匿名化は実現できない。そこで、検索可能暗号で生成されたアドレスが乱数とみなせる特徴を使い、このアドレスから鍵ペアを生成する。BC 接統部に、任意の情報を入力して鍵ペアを生成するための機構を備えることでこれを実現できる。鍵ペア生成部には、利用者毎に異なる暗号鍵を用意する。この生成処理イメージを図 4 に示す。

BC 接統部にこの機構を備えることで、生成済みのアドレスから動的に鍵ペアを生成することが可能になる。このため、システムで安全に管理しなければならない情報を大幅に減らすことができる。具体的には検索可能暗号を生成するために利用する鍵と、アドレスから鍵ペアを導出する際に利用する鍵のみを持てばよい。鍵ペア導出時に生成した秘密鍵も安全に扱う必要はあるが、あくまで署名時などの特定処理実行時のみ必要な情報であり、恒常的に保持する必要はない。

このような機構を備えることで、管理コストをより一層抑えると共に、よりセキュアな BC 接統部を構築することができる。

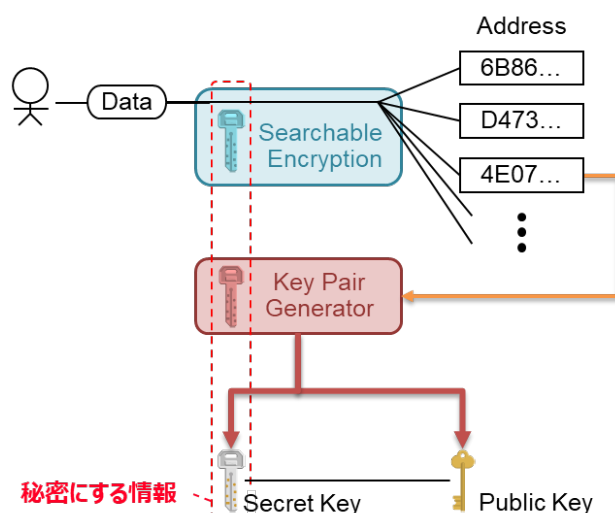


図 4 アドレスからの鍵情報導出

Fig. 4 Derivation Key Pair from Address

5. まとめ

本稿では、検索可能暗号により生成される暗号文を BCN のアドレスとして活用する方法を提案した。アドレスに確率的検索可能暗号化された暗号文を利用することで、安全に管理する必要がある秘密鍵情報を削減するとともに、トランザクション検索処理における処理効率化を実現できる。また、アドレスは利用者が指定するキーワードから生成できるため、アドレスの使い分けが容易になる。さらに、検索可能暗号化された暗号文を入力として鍵ペアを作成する仕組みを備えることで、秘匿すべき鍵情報を 2 個まで削減できる。これらの特徴により、よりセキュアで検索が容易な BC システムの実現が可能になる。

一方で、実際には Bitcoin や Ethereum のアドレスは公開鍵から生成したハッシュ値となっているため、既存環境へ本方式をそのまま適用するのは難しい。今後広まるであろうパーミッション型の BC には十分利用可能と考える。なお、ブロック単位での検索については今後の課題である。

参考文献

- [1] Bitcoin. <https://bitcoin.org/ja/>, (参照 2018-05-07)
- [2] Ethereum. <https://ethereum.org/>, (参照 2018-05-07)
- [3] “BIP 32: Hierarchical Deterministic Wallets”. <https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki>, (参照 2018-05-07).
- [4] Yoshino, M., Naganuma, K. and Sato, H.. Symmetric Searchable Encryption for Database Applications. Network-Based Information Systems (NBIS), pp.657-662. DOI:10.1109/NBIS.2011.110.
- [5] 山崎重一郎, 安土 茂亨, 田中 俊太郎. “ブロックチェーン・プログラミング 仮想通貨入門”. 講談社, 2017
- [6] Hyperledger Fabric. <https://www.hyperledger.org/projects/fabric/>, (参照 2018-05-07)
- [7] Corda. <https://www.corda.net/>, (参照 2018-05-07)