遺言書テスト
— あるいは、あなたのブロックチェーンに意味はあるか —

斉藤 賢爾
ks91@sfc.wide.ad.jp

2019 年 2 月 10 日

概 要

現在、ブロックチェーンが何のために発明されたのか、その意味の理解に混乱が見られる。市場にあふれる、ブロックチェーンを標榜する技術の多くは単に改ざんが多少難しくなっているデータベースに過ぎないようにも見える。一方、ブロックチェーンの原点であるビットコインブロックチェーンは、デジタル署名された取引の記録が特定の (相対的な) 過去に揺るぎなく位置づけられていることが、参加する全員にとって証明可能になることを目指して設計されたと考えられる。

本テクニカルレポートでは、まずその理解に照らして現状のブロックチェーン技術の課題を整理した上で、ブロックチェーンの真価を明らかにする。そして、個別の技術がその真価を満たすものであるかどうかを判定できる「遺言書テスト」を提案し、その実施方法を解説する。

1 はじめに

2019 年 1 月で、ビットコイン [1] の稼働から 10 年が経過した。その間、様々なブロックチェーン技術が派生したが、そもそもブロックチェーンが何のために発明されたのか、その意味の理解には未だ混乱が見られる。市場にあふれる、ブロックチェーンを標榜する技術の多くは、単に改ざんが多少難しくなっているデータベースに過ぎないようにも見える。

一方、ブロックチェーンの原点はビットコインの発明であり、ビットコインは「自分が持つ金銭的資産を自分の好きに送金することを誰にも止めさせない」ために生まれたと考えられる。そのことを成就する目的で発明されたビットコインブロックチェーンは、デジタル署名された取引の記録が特定の (相対的な) 過去に揺るぎなく位置づけられている (したがって送金の事実を覆せない) ことが、参加する全員にとって証明可能になることを目指して設計されたと考えられる。証明に依らず、何らかの権威や中央に拠るのであれば、その権威ないし中央により送金は止められる恐れがあるからである。

本テクニカルレポートでは、まずそうした理解に照らして現状のブロックチェーン技術の課題を整理した上で、ブロックチェーンの真価を明らかにする。さらに、ブロックチェーンを標榜する個別の技術について、実際にブロックチェーンの真価を満たすものであるか (ブロックチェーンとして意味のあるものかどうか) を判定できる「遺言書テスト」を提案し、その実施方法を解説する。

2　ブロックチェーンの課題と真価

2.1　ブロックチェーンの課題

パブリックなレッジャー (台帳) の課題

公共のものとして参加者らにより自律的に運用されているビットコインやイーサリアム等のパブリックなレッジャーは、外因により、停止したり安全性 (特に、証明が継続できること) が損なわれたりする可能性がある。ここで外因としては、暗号技術の危殆化 (古くなり危うくなること) や、ネイティブ仮想通貨 (ブロックチェーンの維持に対する報酬となる通貨) の市場価格の暴落が挙げられる。後者は「インセンティブの不整合性」[2] として知られる課題であり、ブロックチェーンの維持に参加することの対価 (インフラの参加インセンティブ) が減額することで、インフラからの撤退が起き、ブロックチェーンにより提供される証明機能 (ユーザの参加インセンティブ) が損なわれることを意味している。

また、実時間性・秘匿性の課題や、ワンネス (参加する維持者全員がデータ全体に対して同じ処理をすること) による困難 (スケーラビリティの欠如や、新技術を実地で試せないこと) がある。

プライベートなレッジャーの課題

比較的少数の参加者により私的に運用されるプライベートな技術では、上記のパブリックな技術の課題を一通り解決することが容易だが、証明機能が外部に提供されない場合、外から見て既存のデータベースと変わらない (従ってブロックチェーン技術としては無意味) という大きな問題がある。

2.2　ブロックチェーンの真価

ブロックチェーンが、記録が覆っていないことの証明のために発明されたとすれば、その真価とは、「記録が改ざんされていないことを証明できる」ことだと考えられるし、より具体的には、「過去に位置づけられたデジタル署名を、何の権威にも依らずに正しいまたは正しくないと証明できる」ことだと考えられる。このことの実現は、特にブロックチェーン以前では不十分であり、また社会において要求がある。一般に、暗号技術が危殆化したり、秘密鍵が漏洩している場合を考慮すれば、過去に施されたデジタル署名を無条件に正しいと見なすことはできないからである。

このことを、デジタル化された遺言書を例にして考えると、次のようになる。

現行法では、直筆の署名があり公証役場の承認を得られなければ、遺言書は公的なものとして扱われないが、「電子文書としての遺言書へのデジタル署名が本人のものであり、内容が改ざんされていないことを証明」できれば、デジタルファースト化の波に乗って遺言書もデジタルにできる。

ただし、一般に本人の死後は秘密鍵が秘密に保たれている保証がない。また、遺言書が公証人 (遺言書を保存しその正当性を保証する誰か) に預けられ、本人の生前に署名があったことを証言してもらえたとしても、相続人と公証人は共謀するかも知れない (例えば、本人の秘密鍵を取得し、遺言書の改ざんにより莫大な遺産を相続できる可能性をもつ相続人が、分け前をちらつかせて、公証人に偽証をけしかけるかも知れない)。よって、単に文書に本人がデジタル署名を施すだけではデジタルな遺言書は有効なものとして作成できない。

一方、もしデジタル署名された遺言書のデータ、またはそのダイジェストが、ブロックチェーンに書き込まれたとすれば、そのブロックチェーンが先に真価として挙げた機能を満たし続ける限りにおいて、遺言書は (論理的な意味で) 有効と見なせる。

このことは、逆に「有効な遺言書を作れるか」という問いが、「誰かがブロックチェーンだと言って売り込んで来たものが、採用に値するかどうかをテストする問い」として使えることを示している。もし、解きたい問題が (変形を経て) このテストの形になる場合は、テストに不合格な技術は使えないことになる。また、もし解きたい問題がこのテストの形にならない場合は、そもそもブロックチェーンと呼ばれる技術を使うことの意味がない。最も不幸なケースは、解きたい問題は無いのに、このテストに合格しない技術を使って「ブロックチェーンを用いた実証実験に成功した」等と謳うことだが、残念ながらこのケースが巷に蔓延しているようである (不名誉なことだと思うので、あえて例示しない)。

ところで、多くの研究者は、ビットコインが解きたかった問題の中核は「デジタルコインの二重消費を検出すること」[1]だと考えていると思う。そのためにはコインの消費を特定の過去に揺るぎなく位置づける必要があり、変形により、有効な遺言書は作れるかという問いと同型となる。

さて、このテストに合格する技術は実際的に作られているだろうか。暗号技術の危殆化や仮想通貨暴落による停止の可能性まで考慮すると、この問いはビットコイン等のブロックチェーンでも解けていないと言える。また、秘密鍵が漏洩したとしても過去のデジタル署名が有効であることは、コインによる送金の事実が安定して覆らないことに大きく寄与するが、ビットコイン等では「秘密鍵」イコール「コインの所持者」であるので、漏洩が資産そのものを失うことに直結するという大きな問題を抱えた設計となっている。

3 遺言書テスト

ここで「遺言書テスト」を改めて次のように整理する。

> あなたのブロックチェーンでは「遺言書」を作れますか？すなわち、本人が生前に署名したままのかたちで遺言書が保存されていることを、保存しているシステムを (本人の秘密鍵を取得した悪意の相続人との共謀の可能性があるので) 信用せずに、利害関係のあるすべての相続人に対して証明できますか？

端的には、この問いは「システム内部で改ざんされていないことの証明」と「デジタル署名の事後 (永年) 証明」を要求している。これはあくまで問いの雛形であり、遺言書に限らず、アプリケーションに応じた具体的な問いを立てることが重要となる。

多くのいわゆるプライベート/コンソーシアムの台帳技術は (少なくとも素のままでは) このテストに合格できない。かといってパブリックなものは外因により停止してしまい、動かしたい人々の意思だけでは継続できない恐れがある[2]。

4 おわりに

読者は、上で整理した真価や「遺言書テスト」に、ブロックチェーンの特徴としてよく言われる「分散」「共有」や「非中央集権」が入っていないという疑問を抱くかも知れない。だが、「遺言書テスト」に合格するために

[1] 検出した上で互いに矛盾する取引のどちらを採用するかは実は別の問題で、ビットコインブロックチェーンではこれに対してナカモト・コンセンサスを採用した。

[2] 例えば、作業証明を用いるシステムの場合、作業証明のコストが巨大であることは、それだけの作業を想定される時間内にこなせるだけの大量な計算資源の存在を示唆する。仮想通貨の価格の暴落後、撤退によりシステムが停止したとして、大量な計算資源は依然として市場に存在しているのだから、システムを動かしたい人々が仮に乏しい計算資源しか持たない場合 (大量な計算資源が投入されればいつでも記録は覆せうるのだから)、安全性を確保しつつシステムを再び運用することは困難である。

は、「中央」にトラストを置けないことは明らかである。中央に位置づけられてきた機能の内部で改ざんが行われてないことの「証明」を、外部から行えることが重要だからである。また、このことを満たすためには、改ざんを (侵入者にとって)「難しくする」だけでは不十分である。

加えて、上で整理した真価を満たす以外に、解きたい問題を解くのに必要な要素技術は、ブロックチェーン以前から存在しているという認識も大事ではないだろうか。例えば、可用性・耐障害性のための複製および分散合意技術、自律性のための P2P(Peer-to-Peer) など、ブロックチェーンについて巷で騒がれている部分の多くは単に「分散システムの性質」であり、必要に応じて既存の技術を適用できることは、設計者としては理解しておく必要があるだろう。

さて、パブリックに動作するブロックチェーンでも不十分だとすれば、遺言書テストに満足いくかたちで合格できる技術は作れるのだろうか。

このレポートにてブロックチェーンの真価と捉えた「過去に位置づけられたデジタル署名を、何の権威にも依らずに正しいまたは正しくないと証明できる」かどうかは、新しい問題ではなく、前世紀から意識されており、例えば [3] にてデジタル署名の課題として整理されている。それに拠れば、課題はデジタル署名の「経時証明問題」(過去のデジタル署名が正しいことの証明) と「アリバイ証明問題」(過去にあったとされるデジタル署名が正しくないことの証明) に分解される。その上で [3] は、無関係な履歴の中に互いに証拠を残していく「履歴交差」のアイデアを提案している。筆者らは、この履歴交差のアイデアにもとづく「コンテキスト証明 (Proof of Context)」を備える技術を開発中である (https://github.com/beyond-blockchain)。

このレポートにて提案した「遺言書テスト」は、直感的には「経時証明問題」として整理されるが、「アリバイ証明問題」も暗に含んでいる。偽造された遺言書が出てきた際には、それを否定できる必要があるからである。

謝辞

「遺言書テスト」を整理し提案するにあたり、その考案の機会を提供し、議論に参加してくださった株式会社ブロックチェーンハブの皆様、および慶應義塾大学 環境情報学部・総合政策学部 SBI ホールディングス寄附講座「ビヨンドブロックチェーン (2018 年度秋)」の参加者の皆様に、ここで感謝の意を表します。

参考文献

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Available electronically at http://bitcoin.org/bitcoin.pdf.

[2] Kazuyuki Shudo, Reiki Kanda, and Kenji Saito. Towards Application Portability on Blockchains. In *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, 2018.

[3] 岩村充, 宮崎邦彦, 松本勉, 佐々木良一, 松木武. 電子署名におけるアリバイ証明問題と経時証明問題—ヒステリシス署名とデジタル古文書の概念. コンピュータサイエンス誌 bit, Vol. 32, No. 11, pp. 42–48, 2000.