連載

5分で分かる!? 有名論文ナナメ読み

松尾真一郎（ジョージタウン大学）

Satoshi Nakamoto :
Bitcoin : A Peer-to-Peer Electronic Cash System

cryptography mailing list at metzdowd.com

ナナメ読み？　ご無体な

まずはじめに，いくら旧知の仲といえ，この論文を5分でナナメ読みできるような解説を依頼した会誌編集長は控えめに言って頭がおかしい．それは使っている技術が高度であるからではない．むしろ，Bitcoinを構成する要素技術は，提案から10年以上経過したものばかりで，枯れている技術である．しかし，それらが精巧なガラス細工のように組み合わさって生まれたエコシステムの価値を5分のナナメ読みで理解ができると考えているとすれば，本当に頭がおかしい．

Bitcoin以前の技術は，なぜソレを実現できなかったのか

この論文において，Bitcoinは以下のように記述されている（訳：崎村夏彦氏）[1]．

— 同意している二者が信頼できる第三者を必要とせず，直接取引が可能な，トラストの代わりに暗号的証明に依拠する電子支払いシステム
— 分散されたピア・ツー・ピアのタイムスタンプサーバを使って，トランザクションの時間的順序の計算機的証明を生成することによる，二重支払い問題を解決するシステム

この記述から分かるように，Bitcoinは二重支払いを防止する電子支払いシステムが目的である．その目的だけなら，昔から実現可能だった．それを信頼できる第三者を必要とせずに実現できそうな，初めての現実的な方式であるというのが，暗号研究者にとって「ヤラレタ」と思わされたところだ．しかし，この偉業を5分で分かった気になれと思うのは，やはり頭がおかしい．

元々，もしある人が信頼できる（秘密を守ってくれるし，嘘もつかない，言われたことをやってくれる）というのであれば，システムのセキュリティ確保は非常に簡単である．決められた処理を確実に，かつセキュアに実行してくれる第三者が存在して，その第三者と相互認証した上で暗号通信をすれば，システム全体のセキュリティは保たれる．しかし，皆さんも実体験しているように，世の中に「ここだけの話」は存在しないし，裏切る人は多いし，信頼できる第三者が機能しなくなることもある．暗号プロトコルの研究者は信頼できる第三者という仮定がなくても，数式だけで安全な世界を作ることを夢見て研究をしている．だからこそ，この論文はエポックメイキングなのだ．

二重支払いを防止するシステムなら，ATMを使った銀行送金は古くからすでに実現されている．通貨を発行する中央銀行が存在し，通貨は完全に信頼可能で，ATMが置かれている銀行と銀行間のネットワークが完全に信頼できれば，容易に目的を達成することができる．では，ATMや銀行間ネットワークをPCやインターネットに置き換えたらどうなるだろうか．この状況での支払いを実現する電子マネーの研究は1990年代から存在する．たとえば，日本銀行とNTTによる電子現金プロトコルは，現金を模擬して100円なら"100"というデータを中央銀行が発行し，そのデータそのものを現金同様として扱えるようにした．もち

ろん，単純に 100 というデータだけなら誰でも作ることができるので，二重支払いどころかお金は作りたい放題になるので，Bitcoin と同じく偽造や二重支払いを防止するために送金の意思表明を電子署名を用いて実現している．別の方法として，スマートカードの物理的セキュリティを完全に信頼した上で，支払いのときの残高管理をスマートカード，銀行口座，そして通貨を発行する中央銀行の間で齟齬なく行えばいいとする方式もあった．この際にも，電文に矛盾が起きないように，暗号技術が使われていた．これを 5 分で理解することを要求するのは控えめに言って頭がおかしいので，文献 2)，3）などの論文をじっくりあたってほしい．

ただ，1990 年代のこれらの試みでは，前述の暗号技術者の夢は実現されていない．中央銀行や銀行は信頼できる第三者のままだ．お金としての帳簿を管理する主体（中央銀行，銀行）が，系全体の信頼点になっているからである．暗号プロトコルの研究において，信頼できる第三者を減らす伝統的な手法として，暗号処理に必要な秘密情報を複数の主体に分割し，その複数の主体の一部が不正したとしても処理が行える手法がある．分散復号，分散署名，マルチパーティー計算などがその例である．しかし，これらの権限分割はあらかじめ決められた人の間でなされるだけで，悪い人を排除して，新しい良い人を加えるなどの自由度はなかった．これを 5 分で理解することを要求するのは控えめに言って頭がおかしいので，文献 4)，5）などの論文をじっくりあたってほしい．

Bitcoin が出した答えの妙はどこにあるのか

信頼できる第三者が不要で，二重支払いを解決するシステムを作る別の発想をしたのが Bitcoin である．それは，支払いのデータをローカルでやりとりしつつあとで誰かが集計して帳簿を更新するのではなく，共通帳簿全体を系に参加する全員が共有し一定時間ごとに多数のプレーヤで力を合わせて帳簿データを更新していくという発想の転換だ．

取引の前後関係は，10 分単位で支払い要求を束にして，ハッシュ値を連鎖させて証明している．これは，1990 年に提案されたリンクトークン式タイムスタンプ☆1 と同じ技術で目新しくない．むしろ，問題は，それを分散環境でどう実現するかだ．当然，多数のプレーヤの中には悪い人がいるので，悪い人がいたとしても正しく帳簿が更新されないといけない．ここで Bitcoin が出した答えは，過半数のハッシュ関数の計算能力を持つプレーヤが正直な参加者であれば正常に動作するプロトコルを用いて，正直なプレーヤを増やすことで悪いプレーヤを少数派にするという発想だ．そのために，Bitcoin のプロトコルは，いつでも誰でも参加していいし，ネットワークから抜けてもいい，という許可不要な構造になっている．Bitcoin に，マイニングと呼ばれる処理があり，Proof-of-work のゲームを正しく解いた人に 10 分に 1 回，一定額の報酬としての Bitcoin が与えられるのは，ネットワークの参加者を増やしてセキュリティを向上させるためだ．そして，複数の人で共通の帳簿を更新するためには，「分散合意」と呼ばれるプロトコルを実行する必要がある．これは分散コンピューティングの根幹をなす研究テーマであり非常に数多くなされている．しかし，実用的な時間で解決しようとすると，ネットワークに参加するノード数や，ネットワークの同期に関する前提条件が厳しいことも分かっている．そこで，不特定多数のプレーヤが自由に出入りできる Bitcoin においては，新たな合意プロトコルが作られた．これは潔い割り切りをしていて，あとで合意が覆る可能性があってもいいので，確率的に合意をとる仕組みになっている．さらに，暗号処理に対する攻撃をすれば，Bitcoin でも二重支払いは可能となるが，プレーヤに悪い気を起こさせないためにも，自分が持って

☆1 タイムスタンプサービスの方式の 1 つ．利用者が作成する原データのハッシュ値を時系列にそって関連付けるリンク情報を生成する．各タイムスタンプトークンは 1 つ前に発行されたタイムスタンプトークンに必ず依存するように生成される．

いる計算機リソースを暗号の攻撃に費やすのではなく，Proof-of-work のゲームに勝って報酬を得たほうが合理的になることを目指して設計されている．

上記を 5 分で分かった気にさせることを要求するのは控えめに言って頭がおかしい．さらに，Bitcoin がビザンチン将軍問題☆2 を解いたという触れ込みで記事を書く人がたくさんいるが，提案された合意アルゴリズムはビザンチン将軍問題を解いていない．これを理解するのに 5 分で足りないことは明らかだろう．この辺については，文献 1) を熟読いただきたい．

上記で分かるように，解きたい問題や達成したい性質と，使われているテクニックの関係が必ずしも一対一対応していなくて，複雑に絡み合っている．この関係は，正確には現時点でも未解明であって，Bitcoin の登場から 10 年経った今でも，後追いで研究が続けられている．さらに言えば，解きたい課題を完全に解いているわけでもない．このことは，5 分どころか 5 年でも分かるわけがない．

でも本当は，やりたいことを 100% は実現できていない!

信頼できる第三者を不要にするという理想は，実は達成していない．暗黙のうちではあるが，ソフトウェアを実装するエンジニアを信頼している．また電子署名を使っている以上，秘密にすべき署名鍵を厳重に各々が管理することが前提になっているが，それを一般のユーザに求めるのは酷であり，耐タンパ性を持ったハードウェアウォレットの安全性を仮定しても，その設計者や製造者に信頼点を移しただけである．つまり，エンジニアにかかる責任が大きくなっただけとも言える．鍵管理は無理だからこそ，暗号資産の交換所に鍵を預けているケースもあるが，そうすると交換所が信頼できる第三者になってしまう．この辺の裏事情も含めて 5 分で分かるように説明せよというのは，控えめに言って頭がおかしい．

本稿を最後まで見て興味が湧いた読者の皆様は，この論文をむしろ温故知新のきっかけとして，過去の関連論文を時間をかけて読み直して，そしてこの論文を噛むほどに何度も味が出るスルメのように味わってほしい．

☆2 いくつかのコンポーネントが故障している，あるいは，コンポーネントが故障したかどうかの情報が不完全である，という状態で，全体で正しい合意形成ができるかどうか，という分散コンピューティングの問題の 1 つ．

参考文献

1) 松尾真一郎，楠　正憲，崎村夏彦，佐古和恵，佐藤雅史，林　達也，古川　諒，宮澤慎一：ブロックチェーン技術の未解決問題，日経 BP 社．
2) 中山靖司，森畠秀実，阿部正幸，藤崎英一郎：電子マネーの一実現方式について―安全性，利便性に配慮した新しい電子マネー実現方式の提案―，金融研究，第 16 巻第 2 号，日本銀行，金融研究所，1997 年 6 月号．
3) 藤崎英一郎，岡本龍明：エスクロー電子現金，電子情報通信学会論文誌 IT95-51, ISEC95-46, SST95-112, pp.7-12 (1996).
4) Shoup, V. : Practical Threshold Signature, EUROCRYPT 2000, LNCS 1807, pp.207-220 (2000).
5) Ben-Or, M., Goldwasser, S. and Wigderson, A. : *Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation*, STOC '88 Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, pp.1-10.

(2019 年 9 月 3 日受付)

松尾真一郎　Shinichiro.Matsuo@georgetown.edu

ジョージタウン大学・研究教授，CyberSMART 研究センター・ディレクター，NTT Research Inc. Head of Blockchain Research. BSafe.network 共同設立者．