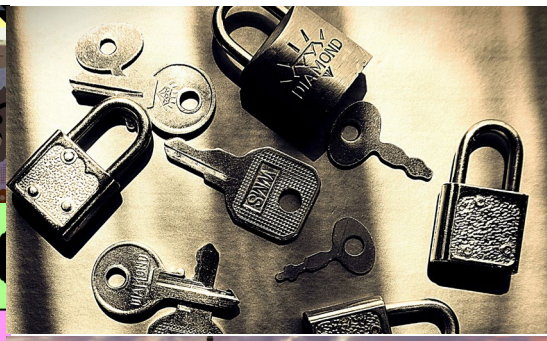
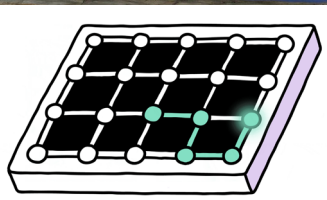
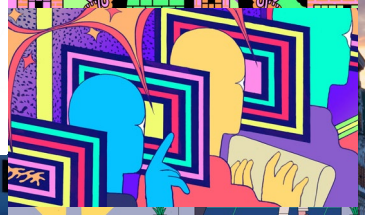
MIT Technology Review
Published by KADOKAWA / ASCII

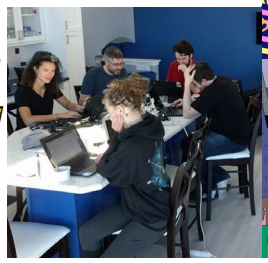
Blockchain

分散型元帳テクノロジーは社会をどう変えるのか






CONTENTS

001 バブル前夜のビットコインは
どのようなものだったのか？

008 国家並みの消費電力、
「大食漢」のビットコインに未来はあるのか？

011 資金調達の新潮流
「ICO」への期待と不安

016 大手銀行も触手、
暗号通貨を完全匿名化する「ゼロ知識証明」

019 金融業界はブロックチェーンに
何を求めているのか？

024 「採掘」でひと儲け、
ハッカーより怖い内職に気をつけろ

027 なぜイーサリアムは
世界を熱狂させるのか？

029 ブロックチェーンが変えた
フィンランドの難民支援

033 保健医療ネットワーク大改革
ブロックチェーンが注目される理由

040 中央集権型から分散型へ、
ブロックチェーンが実現する送電網の抜本的変革

044 ブロックチェーンは
パスワードの呪縛を解くのか

2008年に発表されたビットコインは、いまや暗号通貨の代名詞として連日のようにニュースを賑わせています。同時に関心を集めているのが、国家や銀行といった中央機構の関与がなくても、取引の安全性を確実に担保できる技術である「ブロックチェーン」です。
その特性に注目した世界中の研究者によって、ブロックチェーンは金融業界を超えて、医療データシステムから送電網まで、さまざまな用途での活用が検討されています。
このeムックは、MITテクノロジーレビューに2017年9月～12月にかけて掲載された、ビットコインやブロックチェーン関連の記事をまとめたものです。


BITCOIN · DIGITAL · DECENTRALIZED · PEER TO PEER
MONETARY METALS

バブル前夜のビットコインはどのようなものだったのか？

by Tom Simonite

Photo by allstars / Shutterstock

サトシ・ナカモトと名乗る人物がビットコインの論文を 2008 年に発表して 10 年近く経った。
ビットコインは現在、おそらく開発者たちが想定していた以上のブームになっている。
ビットコインが一般に知られるようになった 2011 年の MIT テクノロジーレビューの記事で、
基礎的な仕組みと当時の見解を振り返ってみよう。

※この記事は MIT テクノロジーレビュー米国版 Web サイトで 2011 年 5 月 25 日に公開されたものです。いくつかの個所で現状についての注釈を日本版編集部が追加しています。

現時点（2011 年 5 月 25 日）で、ビットコインで買えるものはほとんどない。新しい通貨であるビットコインがドル通貨と競合するのはかなり先の話になるだろう。この解説記事では、ビットコインとは何なのか、なぜ重要なのか、ビットコインが成功するためには何が必要なのかを紐解く。

ビットコインの開発者

2008 年、サトシ・ナカモト（偽名が通説とされている）というプログラマーが暗号に関するメーリングリストにビットコイン構想の概要に関する論文を発表した。その後、2009 年前半に、その人物がそのスキームを使ってビットコイン取引に使うソフトウェアを発表した。そのソフトウェアは 2011 年 5 月 25 日時点で、4 人のコア開発者が取りまとめをするボランティアのオープンソース・コミュニティによって運営されている。

「サトシは少し謎めいた人物ですね」と、コア開発者の一人でビットコイン経済を追跡・観察するビットコイン・ウォッチ（2017 年 12 月時点ではビットコインチャート（Bitcoincharts）が価格や相場の情報を掲載している）の創業者であるジェフ・ガルジックはいう（ジェフ・ガルジックは 2015 年にブロックチェーン関連企業のブロック（Bloq）を共同創業し、最高経営責任者（CEO）を務めている）。「他のコア開発者も私も、たまに

サトシとメールしていますが、返信があるかどうかはいつも賭けなのです。メンバー全員、サトシとはメールやフォーラムでやり取りをするだけの関係です」と、ガルジックはいう。

ビットコインの仕組み

ナカモトは、銀行やペイパル（PayPal）などの第三者機関がなくても、電子的に安全な金銭取引ができるようにしたいと考えていた。送り主に信用がない場合でも、受け取った通貨が本物であると確認できる暗号技術をビットコインの基礎としたのだ。

ビットコインの基礎知識

ビットコインのクライアント・ソフトをダウンロードして起動すると、クライアント・ソフト（以降、クライアント）はインターネットを介して全ビットコイン・ユーザーがつながる分散型ネットワークに接続する。そして、クライアントに固有の、数学的に関連付けられたペアの鍵を生成する。ユーザーは個々に割り当てられたこれらの鍵を使うことで、他のクライアントとビットコインの取引ができる。

ペアの鍵のひとつは「秘密鍵」と呼ばれ、他人には非公開で、ユーザーのコンピューターに秘匿される。もうひとつは「公開鍵」と呼ばれる。公開鍵を使って生成したビットコイン・アドレスを他のユーザーに伝えれば、ビットコインを受け取ることができる。重要なのは、最速のスーパーコンピューターを使っても、公開鍵から秘密鍵を算出するのは現実的には不可能だということだ。このため、他者になりすますことができないようになっている。公開鍵と秘密鍵は別のコンピューターに転送できるようにファイルに格納されており、たとえば、コンピューターをアップグレードしても使い続けられる。

ビットコイン・アドレスは、「15VjRaDX9zpbA8LVnbrCAFzrVzN7ixHNsC」といったような文字列だ。たとえば、アルパカの靴下を販売している店舗がビットコインを受け付けている場合、

店舗のビットコイン・アドレスを教えてもらえばビットコインで支払いができるというわけだ。

ビットコインの送金

あるユーザーが取引を実行するときには、そのユーザーのクライアントが、送金先の公開鍵とユーザー自身の秘密鍵を、ビットコインの送金額と結びつけるための数学的な処理をする。この処理の結果がビットコイン・ネットワーク全体に送信され、取引に関わっていない別のクライアントによって取引が検証される。

検証作業をするクライアントは取引に関する2つの照合を実施する。1つは、公開鍵を使ってペアの鍵の本当の所有者が送金したことを確認することだ。これは公開鍵と秘密鍵の間の数学的な関係性から調べられる。2つめは、すべてのビットコイン・ユーザーのコンピューターに蓄積された公開取引履歴を参照して、その人がビットコインを使ったことを確認することだ。

検証をしたクライアントは、詳細をネットワーク上に送信し、他のクライアントが照合をする。このようにして取引は迅速に実施され、オンライン上のすべてのクライアントによって検証される。さらに、「マイナー（採掘者）」と呼ばれる一部のクライアントが、新しい取引を公開履歴に加えるために暗号パズルの解読競争をする。いずれかのクライアントが解読に成功すると、更新された取引履歴がビットコイン・ネットワーク全体に送信される。クライアントが更新された取引履歴を受け取ったら、支払いがうまくいったことがわかる仕組みだ。

セキュリティ

数学の性質上、取引を検証するのは簡単だが、偽の取引を生成して、保有していないビットコインを使うことは実質的に不可能だ。さらに、すべての取引履歴が公開されているので、資金洗浄（マネーロンダリング）を阻止できるとガルジックはいう。「取引台帳は世界中に公開されています。台帳を見れば、すべてのビットコインについて生

成以降のすべての取引を追跡できます」。

ビットコインの入手方法

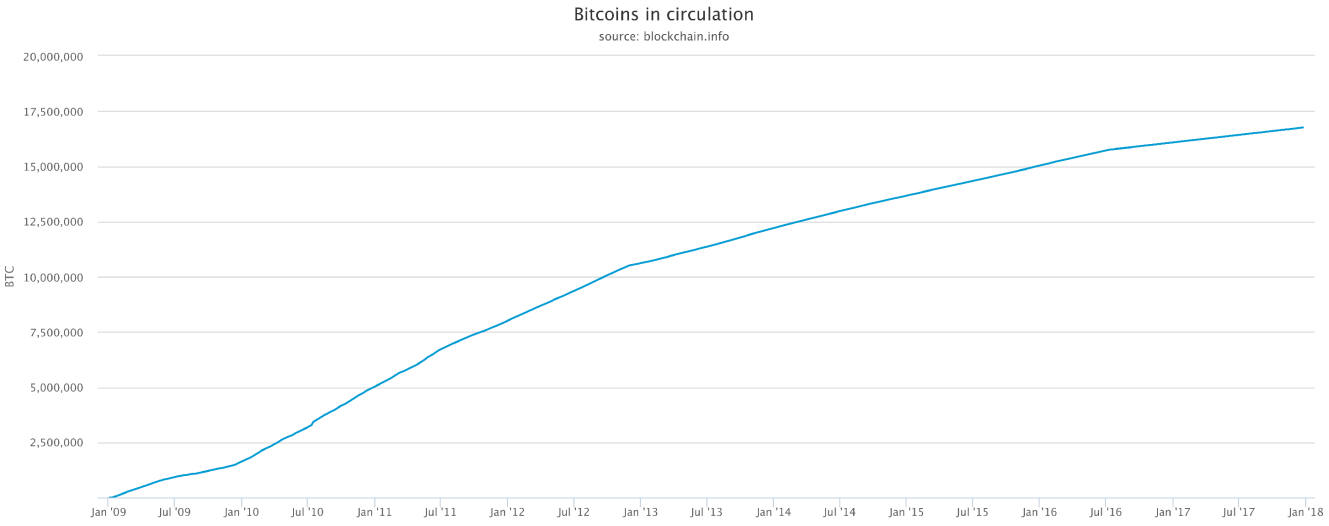
他の通貨とビットコインを交換するには、マウントゴックス（Mt.Gox：2014 年に破綻し現在破産手続き中）のような取引所を使う。一部の熱狂的なユーザーは、Web サイト作成などの仕事の対価としてビットコインを受け取り始めている。ビットコインの支払いを受け付ける請負業務を広告している求人掲示板もある。

だが、まずはビットコインが生成されなければならない。ビットコインは「採掘（マイニング）」によって生成される。つまり、公開取引履歴の更新を完了したクライアントに、見返りとして新しいビットコインが支給されるのだ。すべてのクライアントが、共有された取引履歴の次の「ブロック」を完成するために、暗号パズルの解読競争に取り組む。その競争に勝つと、50 BTC（BTC はビットコインの通貨単位）がもらえる仕組みだ（採掘報酬は 21 万ブロック生成するごとに半減し、2016 年 7 月 9 日以降のマイニング報酬は 12.5BTC になっている。次に半減するのは 2021 年と言われている）。ビットコインは通貨としてまだ初期段階にあるので、この方法で分配している。ゆくゆくは新規のビットコインはこの方法で発行しなくなり、代わりに、承認された取引から少額の採掘手数料が支払われるようになるだろう。

採掘をするには、コンピューターに非常に大きな負荷がかかる。このため、今後数年以内に、高性能グラフィックスカードなしではビットコインを採掘することは難しくなると思われる。

ビットコインを使えるところ

今すぐに使えるところは多くない。一部の熱心なビットコインのユーザーは自分自身のビジネス、たとえばお茶や書籍、Web デザインとビットコインを引き換えられるようにしている。だが、主要小売店でビットコインを受け付けているところはまだない。



ビットコインの流通量は 2011 年時点の 600 万 BTC から、3 倍近くにまで増加している（出所＝ blockchain.info）。

連邦準備制度理事会（Federal Reserve Board: FRB）がドルを管理しているように、ビットコイン経済を管理している組織はあるのか？

ビットコイン経済に管理者はいない。ナカモトが構築したプロトコルによって、ビットコイン経済は運営されている。

ナカモトのルールでは、ビットコインの流通量の増加率を徐々に減少させていき、流通させる最大限を 2100 万 BTC と規定している。2011 年 5 月 25 日時点では、流通量は 600 万 BTC を超えたところだ。2030 年には 2000 万 BTC を超えると予想される（2017 年 12 月 10 日時点の流通量は 1673 万 BTC）。

だが、ナカモトの方法には抜け道がある。ビットコイン・ネットワークの計算能力の半分以上が 1 つのグループに支配された場合、ルールを変更できるのだ。このことは例えば、犯罪集団が取引履歴を自分たちに有利なように改ざんして他のユーザーをだますを防ぐのに役立つだろう。

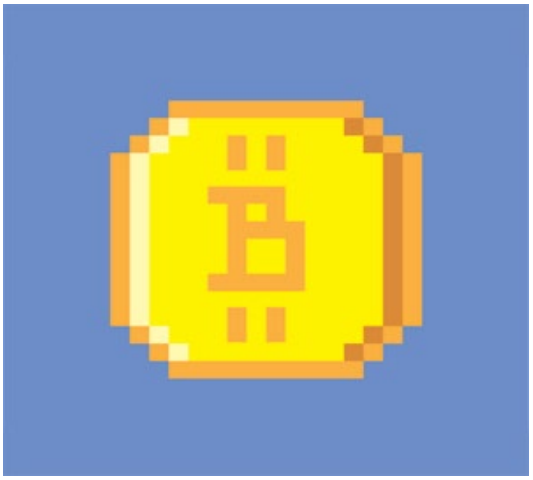
だれかがこんな支配力を手にすることはまずありそうにない。「ネットワークの力を結集すれば、今のところ世界最速のスーパーコンピューターに匹敵します。サトシのルールはおそらく盤石でしょう」とガルジックはいう。

通貨供給量が制限されるのは危険ではないか?

それは明らかに違う。「ドルやユーロなど他の通貨は、通貨量が増えすぎないように入念な制御をしているわけではない」と、ジョージ・メイソン大学で経済学の教鞭をとっているラッセル・ロ

バーツ教授はいう。ビットコインの流通量の増加率が減少して価値が上昇すれば、結果的にゆっくりした安定的なデフレになる可能性が高い。

「現在の経済において、通貨量制限が起こると非常に有害だと思います。予期されていないからです」と、ロバーツ教授はいう。だが、デフレが予期されているビットコイン経済には当てはまらないと考えている。「ビットコインの世界では、すべての人が将来的な通貨量制限を予期しています。そして、自分たちが過去に支払った額で、当時や今以上の価値を購入できることを知っているのです」。



ビットコインはドルなど他の通貨の脅威となるか?

ありそうにない。「特定の技術サービスへの支払い方法として、ニッチな市場を持つかもしれません」とロバーツ教授はいう。しかし、限られた成功だとしても、ビットコインは既存通貨の運命を変えるかもしれないと付け加える。「通貨同士でさえも、競争があることは良いことです。ビットコインの登場が FRB の施策に影響を与えるかもしれません」。

世界中の中央銀行が、世界規模の景気低迷に対処するため、自国の通貨供給量を大幅に増やしてしまった。ビットコインは、小規模ではあるが、中央銀行などの介入を許さない経済もまたうまくいくことを示す成功事例になるかもしれないとロバーツ教授はいう。

ビットコインには「採掘」に大量のエネルギーを消費するという問題がある。
エネルギーを節約できる採掘の手法も提案されているが、
解決しなくてはならない欠陥がまだたくさんある。

ビットコインに長期的な未来があるのかという議論には、決まって次のような話が登場する。「確かにビットコインは、信任された中央機関がなくても価値を交換することを可能にしてくれます。それはすばらしいことですが、そのためにどれだけのエネルギーが必要なのか知っていますか？」

実際、ビットコインはエネルギーを食う。ビットコインが年間に消費する電力量は、ナイジェリア全体の年間の電力消費量に匹敵する。イーサリアムも、他のほとんどの暗号通貨と同じように大量の電力を消費する。最悪だと思うかもしれないが、解決策が手に入るかもしれないと信じるのには理由がある。

■「採掘」とは何か?

解決策に話を進める前に、採掘者（マイナー）の話をしておこう。世間の注目を集めているブロックチェーンだが、それだけではデータセット

の共有にすぎない。ビットコインやイーサリアムのような暗号通貨は、ネットワーク内のすべてのコンピューターが「ブロックチェーンの情報は正しい」と同意し続けることで、命を吹き込まれるのだ。そのために使われているのが、合意形成メカニズムと呼ばれるアルゴリズムだ。「採掘（マイニング）」という言葉の方が、馴染みがあるかもしれない。

暗号通貨の採掘者の仕事は、新しいコインを発行するだけではない。採掘のプロセスの中で、人々が不正にコインを利用していないかブロックチェーンをチェックし、そしてブロックと呼ばれる新しい取引のリストをチェーンに付け加える。電力を大量に消費するのは、2 番目のステップの、攻撃に対してブロックチェーンのセキュリティを確保する過程である。

採掘者は最終的には、もっとも直近の取引を、その情報が正しいことを保証するデジタル署名へと変換しなければならない。すべての採掘者はどんな入力でも受け取って、一見ランダムな文字列を吐き出す暗号化ツールを使ってデジタル署名へ変換できる。しかし、ビットコインの開発者であるサトシ・ナカモトは、この作業をとりわけ困難なものにした。

ナカモトはいわば、暗号化のためのコンペを立ち上げたのだ。このコンペの目的は、先行するブロックの署名、新しい取引のリスト、ランダムに決められた数という 3 つの入力から、特定の署名を最初に探し当てることだ。採掘者たちは 3 つめの数が何であるのか知らないので、誰かが正しい署名を当てるまで、デジタル署名を繰り返し生成し続けなければならない。この際に、大量のエネルギーを消費する。大量にエネルギーを消費することが、ビットコインのネットワークの参加者たちに、採掘の処理が信頼できることを知らせるのだ。

■ 計算量から保有資産量へ

「プルーフ・オブ・ワーク」と呼ばれるこの方法は、合意形成の手順として最も定着しているが、