10分でわかるビットコイン

ビットコインについて知りたかったことのすべて

提供 Relai

ビットコインとは?

ビットコインは、数ある暗号通貨の中でも最も成功を収め、世界中の関心を集めています。多くの人がその成功から利益を得たいと考える一方で、関心のない人や、懐疑的な人もいます。ビットコインは貨幣、投資、そしてテクノロジーをめぐる数々の議論を巻き起こしてきました。ビットコインを単なる投機手段と見なし、バブルだと非難する人もいれば、イノベーション、貨幣革命、あるいは現行の貨幣制度からの救済を口にする人もいます。

また、中国を含む多くの国がビットコインを脅威とみなし、戦う姿勢を見せる一方で、エルサルバドルのように、経済成長を期待してビットコインを公的な決済手段として導入した政府もあります。
しかし、そもそもビットコインとは一体何なのでしょうか?お金?デジタルゴールド?コンピュー　タサイエンティストや投機家の間の一時的な流行?それとも全く別の何かでしょうか?これらの疑問の真相に迫るとともに、ビットコインの背後にある思想や機能についての理解を深めるために、このデジタル貨幣を詳しく見ていきましょう。まずは、ビットコインの歴史をその起源からたどります。

ビットコインの歴史

ビットコインの原点は90年代前半にさかのぼります。1992年、カリフォルニアのコンピュータサイエンティストたちのグループが、暗号技術や数学、政治、哲学などについて同じ考えを持つ人々と意見交換するためのメーリングリストを立ち上げました。彼らはサイバーパンク（SF文学に登場する社会に懐疑的な人物）とサイファー（暗号化すること）をもじって、自分たちを「サイファーパンク」と呼びました。

サイファーパンク

サイファーパンクは、やがて寄り合い所帯へと成長しました。彼らはそれぞれ異なる背景を持ちながらも、インターネットが近い将来、人間の自由をめぐる最も大きな争いの場になるという確信で結ばれていました。

インターネットの統制、監視、検閲の脅威から身を守り、自由で開かれたインターネットを維持するためにサイファーパンクが用いた強力な武器、それが暗号技術でした。

1993年の マニフェスト, で、彼らはこう述べています。「サイファーパンクは［プログラミング］コードを書く。我々はプライバシーを擁護するためには誰かがソフトウェアを書かなければならないと確信しており、……我々はそれを書くつもりだ。」

しかし、暗号技術だけで自由なインターネットは実現しません。サイファーパンクはインターネットが独自のお金、つまり貨幣を持たなければ、本当の意味で自由にはなり得ないことを確信していました。こうして、彼らは国家、中央銀行、企業に依存しない貨幣、インターネットそのものと同じくらい公正で非中央集権的な暗号通貨の開発に乗り出しました。

貨幣実験

しかし、中央組織に依存しないデジタル貨幣を創り出すにあたって、サイファーパンクは技術的な課題を突きつけられます。1990年の時点で、暗号学者David Chaumは中央集権的ながらも暗号技術によって匿名性を確保した最初の暗号通貨eCashを開発していました。ところが、eCashは長期的に他のオンライン決済システムに対抗することはできませんでした。このプロジェクトの運営会社は8年後に倒産し、eCashは消滅しました。

その後もさまざまな試みが行われ、なかでも注目を浴びたのはE-Goldでした。E-Goldは金を裏付けとする暗号通貨で、誰でも利用することができました。ドットコム時代の1996年に設立され、ピーク時には年間20億ドル相当の取引を処理し、同業者の関心を呼びました。

しかし、E-goldには中央管理体が存在するため、攻撃を受けやすいという問題がありました。程なくして法的な問題が発生すると、米国政府はE-Goldに対して法的措置をとりました。そして2008年、E-Goldは米国の裁判所からマネーロンダリングと愛国者法違反で有罪判決を言い渡されました。資産はすべて凍結され、E-Goldは事業停止に追い込まれました。

これらの失敗は、2つの事実を明らかにしました。まず、eCashとE-goldはどちらも担保に支えられていました。担保は国家によって差し押さえられる可能性があるため、弱点であることが証明されました。したがって、自由な暗号通貨は、登録企業、銀行口座、サーバー拠点といった中心的な攻撃ポイントを持たないようにする必要があります。もう1つ明らかとなったのは、政府も規制当局も、国家から独立したデジタル貨幣には興味がないということでした。

サイファーパンクには、帳簿をつけ、二重支払いを防ぐ中央管理体を持たないデジタル貨幣をどう設計するのかという根源的な課題が残されました。中央管理体に依存することなく二重支払いの問題を解決することができれば、インターネットにネイティブな、自由なデジタル貨幣が実現するかもしれません。

神秘的な創造

こうしたことから、サイファーパンクは、中央管理体も担保も持たない暗号通貨の設計を模索し始めました。最も重要な概念は、b-money（1998年）とBit-Gold（2005年）の2つでした。これらの理論的概念は、実装には至りませんでしたが、暗号化のための公開鍵と秘密鍵のペアが想定され、新規コイン発行にプルーフ・オブ・ワーク（作業証明）が採用される予定であったという点で、その設計はすでにビットコインとよく似ていました。ビットコインの発明者もまた、ホワイトペーパーの中でb-moneyとBitGoldの存在を認めています。

しかし、b-moneyとBitGoldは、コンセンサス（現時点で誰がどれだけの貨幣単位を所有しているかの合意）を投票システムに依存していたため、それを操作して所有権を歪める悪意ある攻撃に弱いという問題がありました。

新たなインターネットマネーの誕生を阻むこの最後の問題に対して、2008年10月31日の金曜日に解決策が提示されました。その日、サトシ・ナカモトと名乗る人物が分散型決済ネットワークの概念を説明した

ビットコインホワイトペーパー が、サイファーパンクにメールで送られたのです。そして2ヵ月後の2009年1月3日、ビットコインネットワークが始動しました。

ビットコインネットワークに対する最初の反応は鈍いものでした。何人かの熱心な人がネットワークをテストしてエラーを報告し始めたものの、当初は主にサトシ・ナカモト自身がネットワークを運用していました。ところが、この真新しいインターネットマネーについての情報は徐々にコンピュータやテック系のフォーラムに広がり、関心が高まっていきました。そして1年後には、ビットコインネットワークはかなりの利用者を抱えるまでになりました。しかし、ビットコイン自体にはまだ価値がありませんでした。

「サトシ・ナカモト」とは何者なのか?

ビットコインホワイトペーパーとビットコイン発明者によって書かれたメールは、いずれも「サトシ・ナカモト」という名前で署名されていました。この名前は仮名と考えられており、ビットコイン発明者の正体は今も謎に包まれています。ナカモトは、志を同じくする人々や後にビットコイン開発者コミュニティと連絡を取るために、少なくとも3つのメールアドレスを使用し、送信者の身元を隠すために徹底的に暗号化を施していました。

これまで、何人もの人が自分こそがサトシ・ナカモトであると主張してきました。しかし、それを証明できた人は今日に至るまで一人もいません。ほぼ間違いなくサトシのものであるとされるウォレットアドレスからビットコインを送るという究極の証拠をまだ誰も提示できていないのです。

しかも、インターネットを通じてサトシ・ナカモトと「個人的に」連絡を取った人はほんのわずかでした。サトシ・ナカモトは、2010年12月12日にビットコインコミュニティに宛てて最後のメッセージを書きました。しかし、これは決して別れを告げるメッセージではなく、それ以降、単にコミュニケーションを取らなくなっただけでした。

この時に彼が退いたのは、より広いコミュニティからのみでした。ナカモトはその後も少人数のコアプログラマーと密に連絡を取り、ビットコインネットワークのさらなる開発について伝えていました。しかし、2011年4月、彼はこのグループにも最後のメッセージを送りました。2008年の謎めいた出現から3年後、ナカモトは再び姿を消したのです。

「ビットコイン・ピザの日」

では、そもそもビットコインはどのようにして価値を持つようになったのでしょうか。当初、ビットコインはマイニング（採掘）してネットワークの参加者間で送受金することはできましたが、まだ価値はありませんでした。また、ビットコインの送受金ができる人はおろか、ビットコインを知っている人もまだほんのわずかでした。

しかし、2010年5月22日に転換点が訪れます。インターネット上のフォーラム bitcointalk.org に、一風変わったリクエストが書き込まれました。フロリダに住む28歳の男性Laszlo Hanyeczが、ピザを2枚届けてくれた人に1万ビットコインを支払うというのです。カリフォルニアのある学生がこの申し出に応じ、41ドル相当のLサイズピザ2枚がHanyeczの自宅に届くよう手配しました。その見返りとして、Hanyeczは彼に1万ビットコインを送りました。

その日以来、毎年5月22日は「ビットコイン・ピザの日」としてビットコイナーたちに祝われるようになりました。この記念すべき日は、次の3つのことを物語っています：

- ビットコインには価値がある。

- ビットコインは交換や支払いの手段として適している。

- ビットコインはデフレ通貨である 。

ビットコインの新規発行数は着実に減少しており、価値の上昇につながる可能性がある。

この2枚のピザは、世界で最も高価なピザとして歴史に刻まれました。2021年12月時点のビットコイン価格でその金額を計算すると、なんと4億6千万ドルが支払われたことになります。しかし、その1万ビットコインを受け取った人も、その後すぐにドライブ旅行の費用に充てるために売却してしまったとインタビューで述べています。現在のビットコイン価格では、おそらく人類史上最も高価なドライブ旅行です。

「ビットコイン・ピザの日」は、「ホールド（保持する）」に由来する「ホドリング」をビットコイナーたちがなぜ熱心に実践するのかをよく表しています。「ホドリング」とは、（できる限り）絶対に売らないつもりで、ビットコインを長期にわたって保有することを意味します。数年後には2倍、3倍、あるいは10倍の価値になる可能性を秘めたビットコインを、今使いたいと思う人がいるでしょうか?

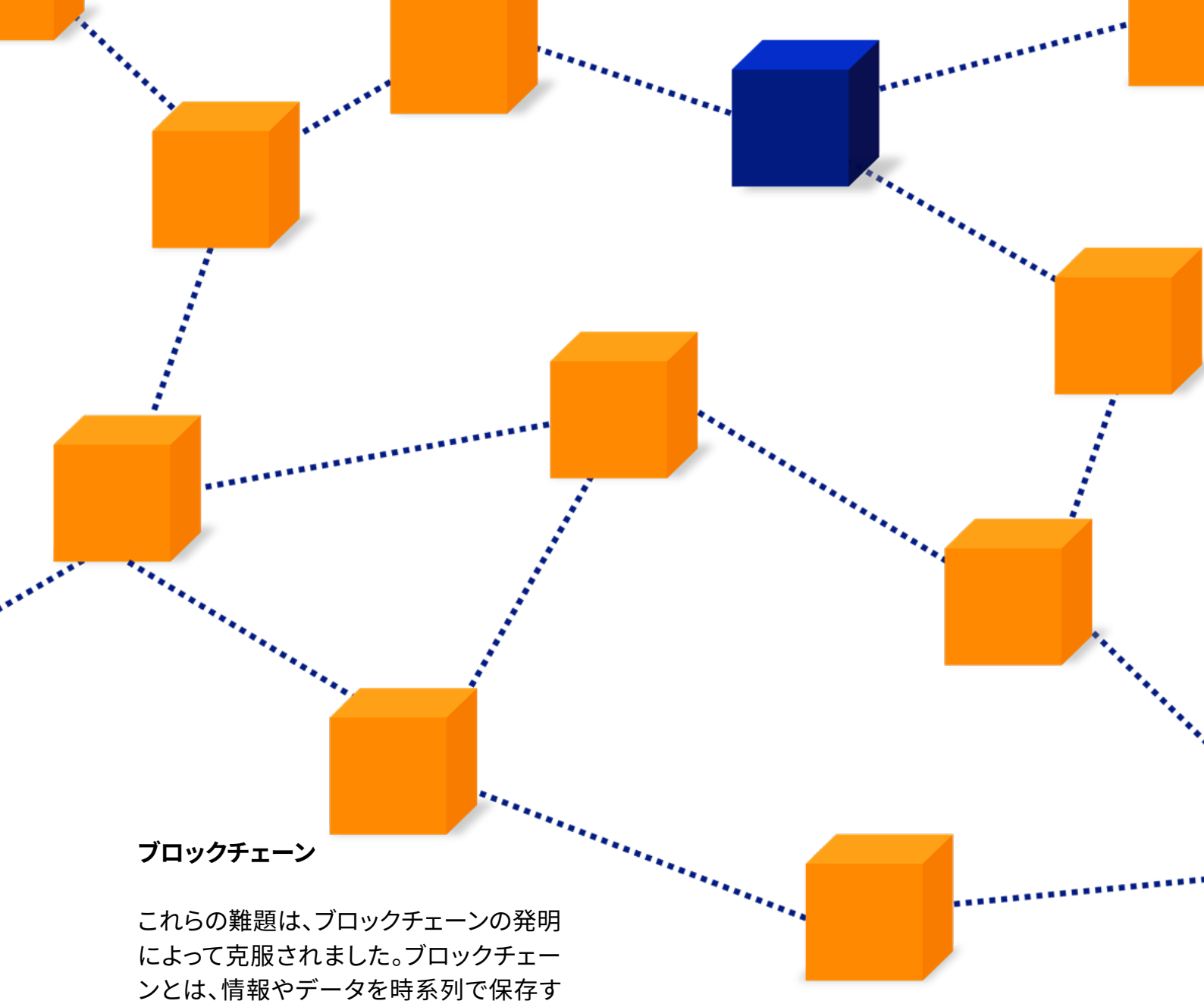
ビットコインの仕組みは?

ここまでビットコインの歴史について学んできましたが、次はビットコインの仕組みに踏み込んでいきましょう。ビットコインネットワークがどのように機能し、どのような問題を解決し、その実用的な利点が何であるかを理解することがその目的です。

ビットコインは、分散型ネットワークであることを意図して設計されています。ネットワーク参加者が単独でネットワークを支配することがないよう、意思決定権限と管理権限は参加者全員に分散されています。個人や政府、企業が単独でネットワークに変更を加えることはできず、ネットワーク参加者の合意によって初めて可能となります。

ビットコインは、すべてのネットワーク参加者が常に最新の所有権台帳の同一コピーを持っているという仕組みのもとで成り立っています。したがって、誰がどのビットコインを現在所有しているのかを全員が常に把握しています。誰かが実際より多くのビットコインを所有していると主張したとしても、ネットワーク参加者はこの主張を自分の台帳のコピーと照合し、それが誤りであることを証明することができます。

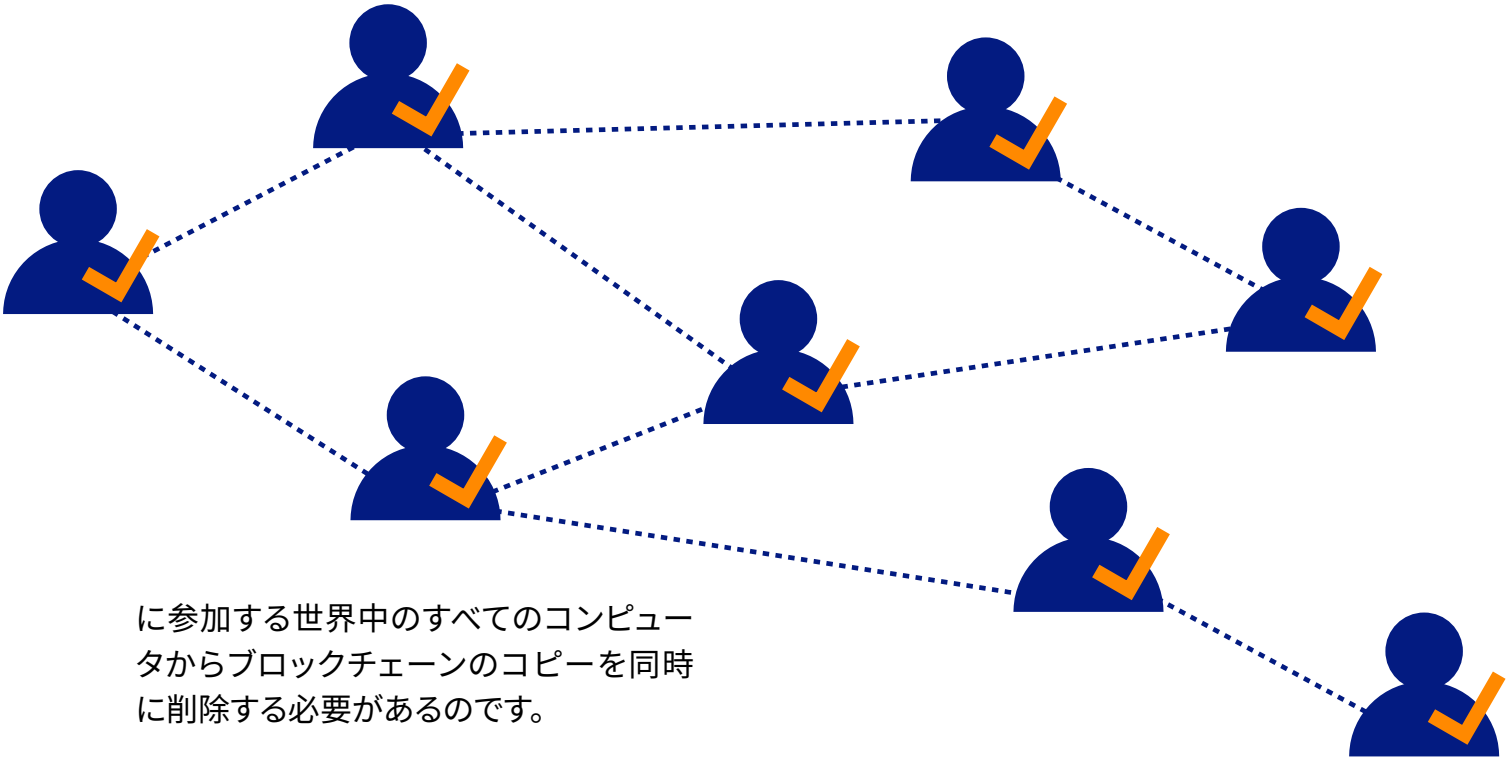
ビットコインが誕生する前、分散型ネットワークは2つの大きな課題に直面していました。1つ目は、所有権の変更に関する最新のアップデート、つまり、どのビットコインが誰に送られたかという情報を、参加者全員が確実に受け取るにはどうしたらよいかというもの。そしてもう1つは、参加者が受け取る情報が正確であることを、彼らがどうしたら確実に検証できるのかというものでした。



ブロックチェーン

これらの難題は、ブロックチェーンの発明によって克服されました。ブロックチェーンとは、情報やデータを時系列で保存するものです。ビットコインの場合、ビットコインが誕生してからのすべてのトランザクションが時系列で何万というブロックに格納され、それらが連なってビットコインブロックチェーンを形成しています。誰がどのビットコインを所有しているかをネットワーク参加者が知りたければ、ビットコインブロックチェーン上のトランザクション履歴を追跡し、現在誰が何ビットコイン所有しているかを正確に判断することができます。そのため、誰かがビットコインを送ろうとする場合、そのビットコインが本当にその人のものであるかどうかを誰もが確認できます。

ここまでの仕組みは銀行も同じようなプロセスを用いていますから、目新しいものではありません。顧客が1スイスフランを使いたい場合、銀行はトランザクション履歴を調べ、そのお金がまだ顧客のものなのか、すでに使われた（他の人に送金された）ものなのかを確認します。しかし、ブロックチェーンのユニークな特徴は、この情報が中央集権的な銀行のサーバーではなく、ネットワーク参加者（いわゆるフルノード）全員のコンピュータに保存されるため、世界中に何万ものコピーとして存在する点にあります。ビットコインを単純に削除することが不可能な理由もここにあります。削除するためには、ネットワーク



に参加する世界中のすべてのコンピュータからブロックチェーンのコピーを同時に削除する必要があるのです。

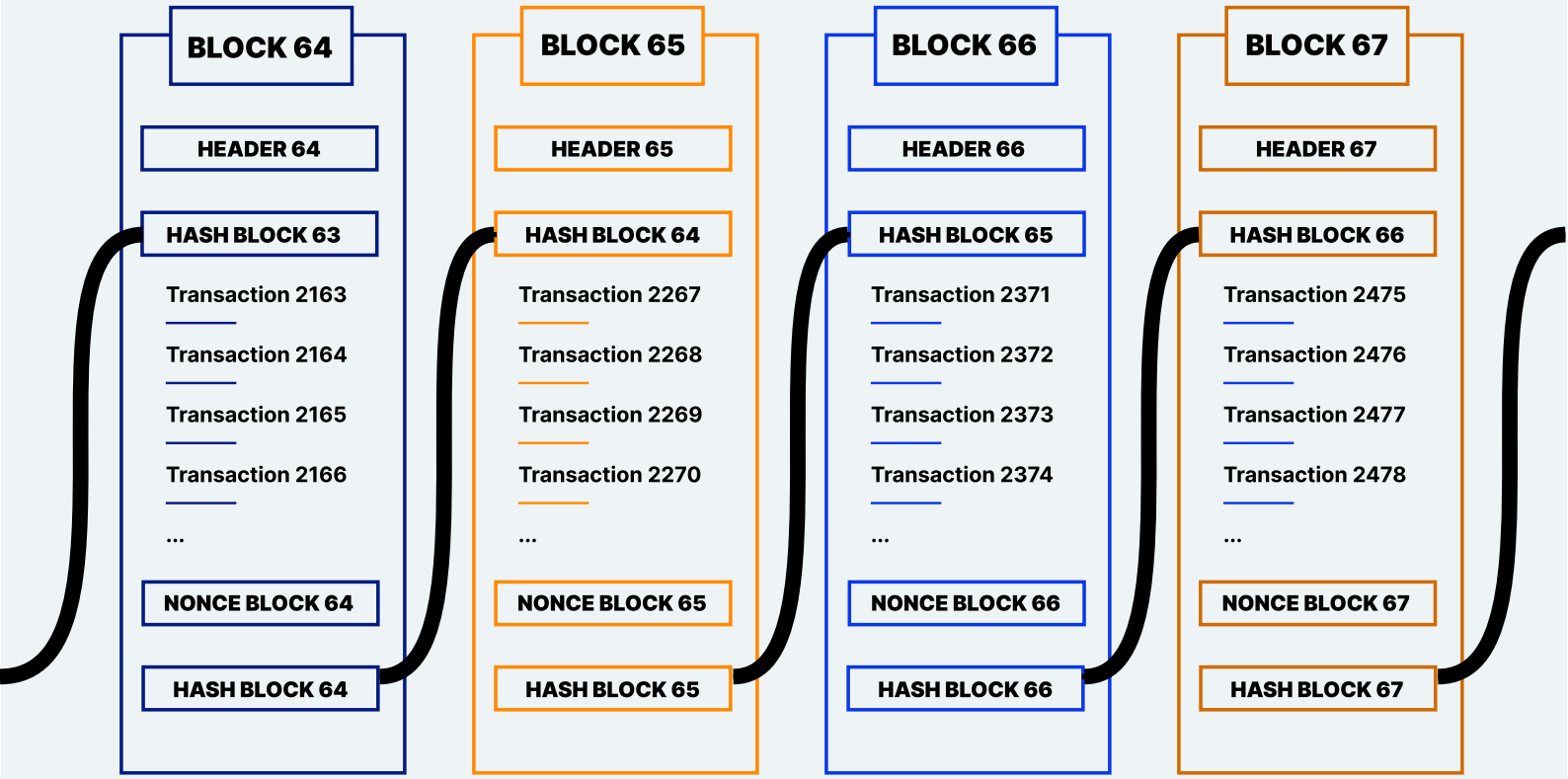
しかし、ここでブロックチェーンが直面する問題は、ネットワーク参加者が自分の持っているブロックチェーンのコピーが正確なものであり、誤ったトランザクションや不正なトランザクションが記録されていないことを絶対的な確信を持って判断できなければならないということです。新しいトランザクションを含む新規ブロックは約10分毎にブロックチェーンに追加されるため、ブロックチェーンは常に成長しており、ネットワークに参加する世界中のすべてのコンピュータで絶えず更新される必要があります。

新たに追加されたブロックは誰もが検証可能でなければいけません。この検証は、ビットコインネットワークのプログラミングコードに定義されている変更不可能な規則に基づいて行われます。これらの規則は、どのトランザクションが許可されるかされないかを厳密に定義しています。したがって、ブロックチェーンのコピーをダウンロードしたすべてのユーザーは、トランザクションが規定規則に違反していないかを検証することができます。違反している場合、すなわち不正確または不正である場合、そのトランザクションはネットワーク参加者（フルノード）によって拒否され、ブロックチェーンには含まれません。

プルーフ・オブ・ワーク（PoW）マイニング

さらに、ビットコインネットワークには新規ブロックの追加を制限する仕組みがあります。新しいトランザクションやブロックを誰でも追加できてしまえば、ブロックチェーンが世界中で同じ状態に素早く更新されず、ネットワークは大混乱に陥ります。

これを防ぐために、ビットコインはプルーフ・オブ・ワークと呼ばれる仕組みを採用しています。ブロックチェーンに新規ブロックを追加する権利を得るには、プルーフ・オブ・ワーク（作業証明）を提供しなければなりません。このプロセスは、例えるなら干し草の山の中から1本の針を探すようなもので、最初に針を見つけた人がブロックチェーンに新しいブロックを追加する権利を勝ち取ります。さらに、発見者には新規発行されたビットコイン、そしてブロックの送金手数料が報酬として与えられます。ブロックチェーンにブロックが追加されると、同じプロセスが再び始まり



前のブロックのハッシュ関数の結果であるヘッダー、現在のブロックのトランザクション履歴、ナンス（ランダムな値）が数学関数に入力される。ナンスは、ハッシュ関数の結果の先頭に一定数以上のゼロが並ぶまで変更される。このプロセスがマイニングと呼ばれる。

ます。

実際には、マイナー（採掘者）はハッシュ関数（SHA-256ハッシュアルゴリズム）を実行し、特別な数値を探します。前のブロックのハッシュ値、現在のブロックのトランザクション履歴、ナンス値をハッシュ化します。ナンス値は、ハッシュ関数が先頭に一定数以上のゼロが並ぶハッシュ値を吐き出すまで変更されます。例えば、2021年9月11日に作成されたブロック#700000の有効なハッシュ値は「0000000000590fc0f3e-ba193a278534220b2b37e　9849e1a-770ca959」でした。

この数値の探求はマイニングと呼ばれ、主に2つの役割を果たします。まず、ブロックを数学的・暗号学的に連結することで、誰でも簡単に正しい順番を確認することが可能になります。同時に、プルーフ・オブ・ワークの仕組みにより、この順番を変更することはほぼ不可能となります。2つ目に、この仕組みのもとでは、新規ブロックは約10分毎にしかブロックチェーンに追加されません。これにより、世界中のネットワーク参加者がブロックチェーンを同一の最新の状態に更新するのに十分な時間が与えられます。

以上のように、マイナーはビットコインネットワークを維持する役割を担っています。彼らの存在がなくては、新しいトランザクションは処理されず、ブロックチェーンにも追加されません。フルノードは、台帳のコピーを保持し、トランザクションが合意規則に反していないかを検証し、不正なトランザクションが台帳に記録されるのを阻止しています。

2,100万ビットコイン

マイナーはビットコインブロックチェーンに新しいブロックを追加する作業に対する報酬として新規ビットコインを受け取りますが、ビットコインの発行上限は2,100万ビットコインと決まっています。2,100万ビットコインを超えることは決してありません。しかし、2,100万枚のコインが最初から流通しているわけではなく、厳格なスケジュールとビットコインコードに従って発行されています。

ビットコインが始動した当初は、約10分毎に50ビットコインがマイナーに放出されていました。それから4年後、10分間隔で放出されるビットコインの数は半分になりました。このプロセスは「半減期」と呼ばれ、マイナーのブロック報酬が約4年毎に半減することを意味します。現時点で約1,900万ビットコインが流通しており、最後のビットコインが発行されるのは2140年になると見込まれています。それ以降、マイナーは送金手数料のみを報酬として受け取ることになります。

ビットコインを極めて希少性の高い財たらしめる根本的な特性の1つが、供給量に課されているこの厳密な制限です。ビットコインが長期にわたる価値貯蔵手段として機能するためには、この絶対的なデジタル希少性が重要な前提条件となります。そのため、ビットコインはデジタルゴールドやゴールド2.0と呼ばれることもあります。

結果：デジタル資産

ビットコインネットワークのすべての特徴を総合的に検討すると、この発明の重要性は明白です。ビットコインは、歴史上初めて厳密に限られた数しか存在することのないデジタル財です。ビットコインをコピーまたは複製して供給を2倍にすることはできません。

この偉業から、ビットコインはよくデジタル資産と称されます。地球上のすべての土地が唯一無二であるように、各ビットコインも固有のものであり、デジタル空間に一度しか生み出されません。

さらに、ビットコインは本当の意味で所有することができます。64文字からなる英数字の組み合わせである秘密鍵を所持している人だけが、紐づけられたビットコインを動かすことができます。この秘密鍵がなければ、ビットコインを盗んだり、没収したり、差し止めたりすることはできません。その人が大富豪であろうと政治難民であろうと、所有者は自分の金融資源を完全に管理することができます。つまり、コンピュータの発明以来初めてデジタル資産を真に所有することが可能になったのです。

なぜ、ビットコイン?

とはいえ、なぜビットコインはこれほど騒がれているのでしょうか。デジタル資産を真に所有できるということは確かに革新的かもしれませんが、そもそもビットコインを所有したいと思う理由はどこにあるのでしょうか?

いいとこ取り

これまで何世紀にもわたって、貴金属や後には硬貨や紙幣などの現金が支払手段として用いられてきました。こういった手段には、「現金は印刷された自由である」という言葉にもあるように、第三者を介さずに保管、使用できるという利点がありました。しかし一方で、インターネット上のデジタル空間での使用は難しいという欠点があります。そのため、オンラインショッピングが普及し始めると、デビットカードやクレジットカードが一般消費者の間に定着しました。

しかし、現金のかわりに銀行口座内の電子マネーを使うことが一般的となった今、人々はより大きなカウンターパーティーリスクに直面しています。例えば、金融機関が破綻を宣言すれば、顧客の預金は失われるかもしれません。現金引き出しが厳しく制限され、資本規制が敷かれ、預貯金に対する強制収用が行われた2013年のキプロスのような状態に陥れば、人々はもはや自分のお金をコントロールすることはできません。また、最近多くの西側諸国でみられるように、銀行の顧客がキューバやイランに住む親族への送金を許されないとしたら、彼らはすべての取引を第三者による承認に依存していることになります。

銀行口座に保管されるお金が紙ベースからデジタルなものに置き換わったことで、私たちは自分のお金をコントロールする力を失いました。しかしこれまでは、このようなマイナス面はデジタル化された社会に参加するためには仕方のないことでした。

ビットコインは、このジレンマに対する解決策をもたらしました。デジタル通貨としてのビットコインは、デジタル空間での決済に最適です。同時に、ビットコインの所有者はコインを秘密鍵の形で自分が最

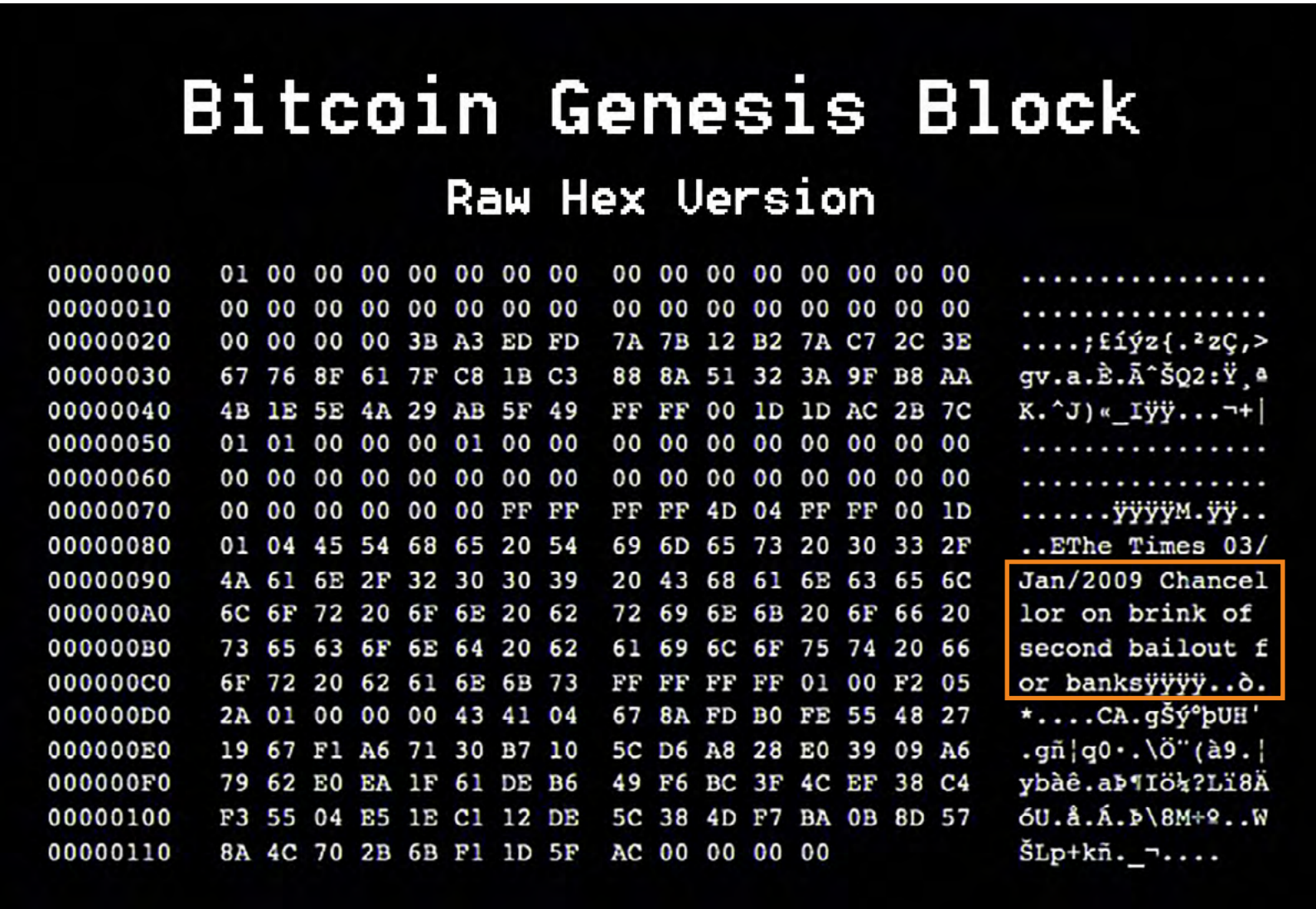
も安全と思う場所に保管できますから、第三者（銀行）に依存することなくビットコインをデジタル資産として貯蔵することも可能です。

最高のタイミング

ビットコインは、2008年9月に発生した世界金融危機の渦中で生まれました。ビットコインブロックチェーンの最初のブロック（ジェネシスブロックとも呼ばれる）に、サトシ・ナカモトは強力なメッセージを残しています。それは、イギリスのタイムズ紙に掲載された「銀行救済に二度目の公的資金注入へ（Chancellor on brink of second bailout for banks）」という見出しでした。

これは、サイファーパンクの国家批判的思想をサトシが表明したものでした。2008年の金融危機の際、中央銀行は銀行を救済するために紙幣を大量に増刷しました。その代償を払ったのは、ジャブジャブにばら撒かれたお金によって貯蓄の価値が目減りした人々でした。このことから、サイファーパンクは国家や中央銀行への不信を再確認し、国家から独立した貨幣が一刻も早く必要であるという確信を強めたのです。

新型コロナウイルスのパンデミック禍においても、同様のことがより大きな規模で繰り返されました。2020年だけでも米国のマネーサプライは50%拡大し、スイスを含む他の国々でも紙幣の増刷は止まる気配がありません。その直接的な結果としてもたらされたのが、記録的な低金利（スイスではマイナス金利）と強力な資産インフレです。



貨幣価値の切り下げに対するヘッジ

ビットコインはこれ以上ないタイミングで登場しました。お金の問題がこれほど身近に迫り、人々に大きな疑問を抱かせたことはかつてありませんでした。供給上限が2,100万と決まっているビットコインは、際限なく拡大する中央銀行のバランスシートとは対照的です。ビットコインの限られた供給は、過去数十年間にあらゆる通貨に見られた財産価値の希釈からの保護という恩恵をもたらします。

ビットコインはその特殊な仕組みによって、購買力を長期にわたって確実に維持できるように設計されています。希少性の高いビットコインは、毎年1〜2%の純流入がある金よりもさらに効果的にその役割を果たすでしょう。さらに、ビットコインは保管や移動にかかるコストも金に比べて大幅に低く、より長期にわたる価値保存が可能です。

財産の保護

ビットコインが解決に貢献するもう一つの問題は、財産の保護です。金や現金は盗難を防ぐための保管に多額の費用がかかりますが、ビットコインは事実上ゼロコストで保管・移動が可能です。12個または24個の単語からなる暗号コードを使えば、たとえ大金でも簡単に持ち運ぶことができます。ひとたび記憶し、物理的に破壊してしまえば、暗号コードが盗まれることはありません。暗号コードと紐づいたビットコインの安全は確保され、所有者が望めばお墓まで持っていくこともできます。

ビットコインを購入する

ビットコインを入手するには、マイナーとしてビットコインを稼ぐか、他者からビットコインを購入するかの2つの方法があります。家庭用デバイスでのマイニングがほとんど不可能になった今、初心者にはビットコインを購入するという道しか残されていません。

暗号通貨取引所・ブローカー

ビットコインを購入する最も簡単な方法は、暗号通貨取引所またはブローカーを利用することです。使い方は株式取引プラットフォームと似ています。個人口座を開設した後、スイスフラン、ユーロ、または米ドルを銀行振込またはクレジットカードで送金します（利用可能な通貨や送金方法は国により異なる場合があります）。取引所の個人口座に資金が到着すると、数クリックするだけで、24時間いつでもその時の市場価格でビットコインを購入することができます。ヨーロッパでは、ビットコイン専用投資アプリ Relaiを使い、登録や認証、初回入金なしでビットコインを購入することが可能です。

P2P取引所

暗号通貨取引所を介さない方法として、個人間で取引するためのプラットフォームを通じて他の市場参加者からビットコインを直接購入することもできます。個人情報を明らかにする必要がないため、より高い匿名性が確保されます。

ビットコインATM

ビットコインはATMで購入することもできます。スイス, ドイツ, オーストリア をはじめ、世界中のさまざまな国に設置されています。ビットコインATMでは、現金を用いて匿名で、あるいはクレジットカードでビットコインを引き出すことができます。口座や既存の暗号通貨ウォレットは不要です。

ビットコインを安全に保管する

ビットコインを入手したら、次はそれを安全に取り扱い、保管する必要があります。ビットコインや暗号通貨の原則は「Not your keys, not your coins（鍵を持たぬ者は、コインを持たず）」というものです。ビットコインを真に所有するには、それと紐づく秘密鍵を所有する必要があります。つまり、ビットコインを自分のデジタルウォレットに保管し、その秘密鍵を所有していない限り、そのビットコインを本当に管理しているのはあなたではありません。

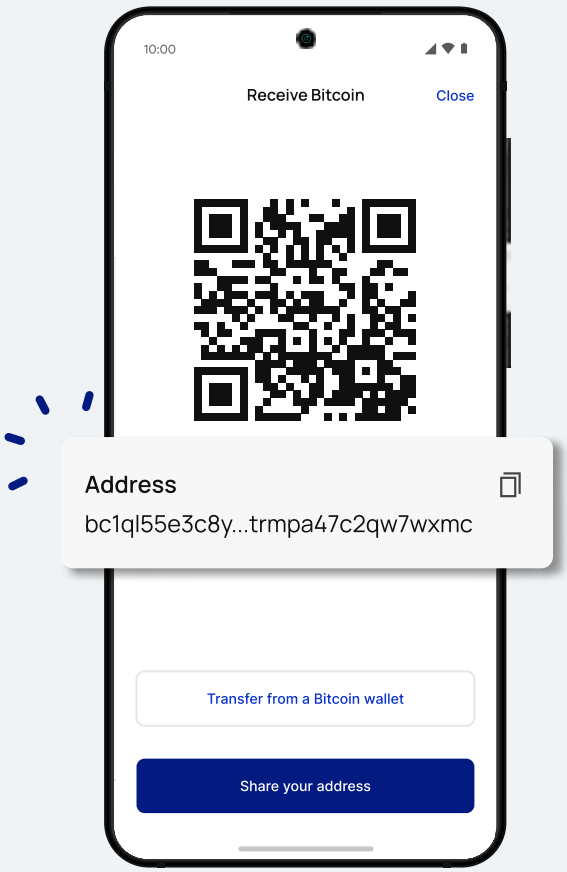
ビットコインが暗号通貨取引所に預けられている限り、それは取引所の管理下にあります。取引所がハッキングされたり、倒産したり、不正を働いたりすると、そのビットコインを永遠に失うことになりかねません。

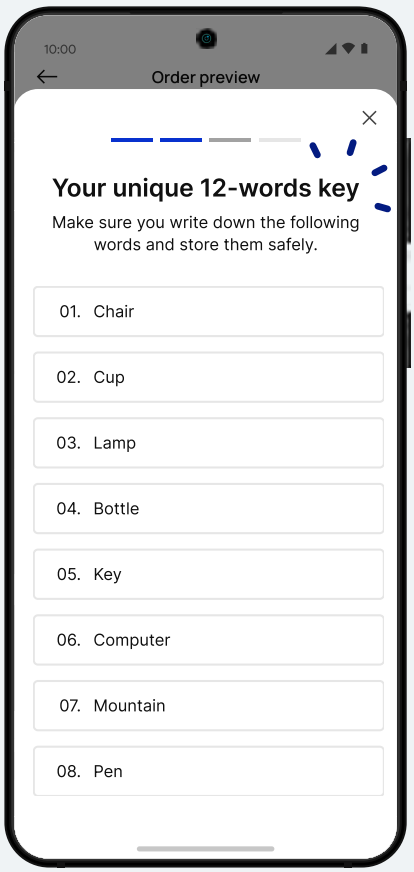
セルフカストディ

銀行口座とは異なり、ビットコインは個人ウォレットに保管することができます。あなたがあなた自身の銀行となるため、ビットコインを完全にコントロールできるという利点があります。しかし、これには責任も伴います。12個または24個の単語で構成される秘密鍵は、ビットコインの所有者自身が保管し、安全に保つ必要があります。取り扱いを誤ったり、怠ったりすると、ビットコインの紛失という取り返しのつかないことになる可能性もあります。

ウォレット：デジタルウォレット

デジタルウォレットとは、ビットコインの秘密鍵を安全に保管するためのツールです。ビットコイン自体は常にブロックチェーン上に保管され、ウォレットに移動することはできません。ウォレットに保管でき





るのは、ビットコインへのアクセスキーのみです。

そこで作られたのが、秘密鍵を安全かつ簡単に保管するためのウォレットです。数クリックでビットコインを送受金することもできます。したがって、ウォレットはビットコインを扱うための便利なツールであると言えます。

ソフトウェアウォレット

最も一般的なウォレットは、ソフトウェアウォレットです。ソフトウェアウォレットは、デスクトップアプリケーションもしくはスマートフォンアプリとしてセットアップできます。セットアップの際、ウォレットの秘密鍵が12個または24個の単語（シードフレーズ）の形で表示されます。これらの単語はそのウォレットにあるビットコインと同義であり、それを知っている人がコインをコントロールできます。したがって、単語は紙などにアナログで書き留め、誰にも知られないように保管する必要があります。万が一パソコンやスマートフォンを紛失したり、盗まれたりしても、これらの単語があればいつでもウォレットを復元することができます。

ソフトウェアウォレットは、短時間でセットアップできて使い勝手が良いという利点があります。しかし、ソフトウェアウォレットはデバイスにインストールされたコンピュータプログラムであり、インターネットに直接接続されているため、ハッカーの攻撃を受ける危険性に常に晒されています。

ハードウェアウォレット

セキュリティを重視したい人は、ハードウェアウォレットを使いましょう。ハードウェアウォレットは、ビットコインにアクセスするためのコードを保管するUSBメモリのような小さな端末で、必要なときだけコンピュータに接続します。これらの端末は、悪意のあるソフトウェアに感染したコンピュータでもコードにアクセスできないように設計されています。

ハードウェアウォレットをセットアップする際、12個または24個の単語（シードフレーズ）が生成されます。それらはアナログで書き留め、安全に保管する必要があります。万が一ハードウェアウォレットを紛失しても、それらの単語をもとに復元することができます。ハードウォレットの例としては、BitBoxやTrezorがあります。

Made in Switzerland

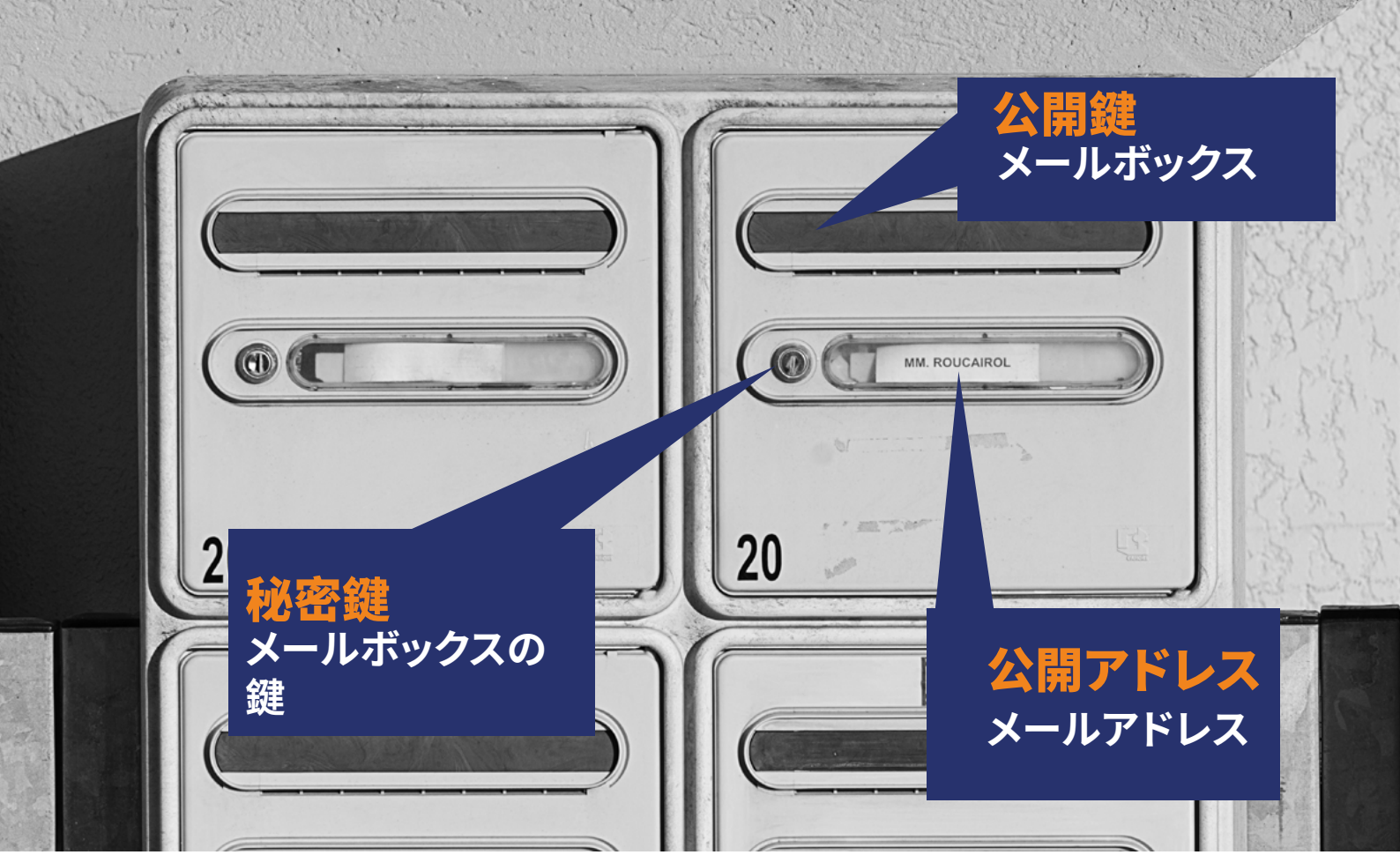
EUROPE'S EASIEST BITCOIN APP

Relai

Download on the App Store

GET IT ON Google Play

Buy bitcoin in 1 minute from as little as 10 EUR/CHF without verification.



ビットコインを送受金する

ビットコインの送受金はとても簡単です。各ビットコインウォレットには、いわゆる「公開鍵」から生成された公開アドレスがあります。これは、IBAN（国際銀行口座番号）と同様に受金アドレスとして機能します。このアドレスを知っている人は、対応するウォレットにビットコインを送ることができます。公開アドレスはQRコードで表示することもできます。

ビットコインを誰かに送りたい場合は、ウォレットの「送金」画面で受金者のビットコインアドレスを入力するか、対応するQRコードをスキャンします。発生した送金手数料は、送金者のウォレットから自動的に差し引かれます。送金手数料はネットワークの混雑状態によって変動し、こちら.で確認することができます。送金したビットコインが受金者に届くまでには、平均10分ほどかかります。ただし、送金者が支払う送金手数料によってはそれ以上かかることもあります。

ビットコインで支払う

ビットコインは誕生した当初から、将来的に日常の決済に使われるようになることが期待されていました。現在では、理論的にはこれが可能です。ビットコインを支払手段として受け入れる企業は増加の一途をたどり、一部の政府の税務局や非営利団体でもビットコインでの決済が可能になっています。しかし、ビットコインネットワークを介した送金には数スイスフランのコストがかかり、少なくとも10分かかるため、大きな金額でなければ意味がありません。ビットコインを安く速く送るためには、別のソリューションが必要です。

ライトニングネットワーク - より速く、より安く

そこで、ビットコインネットワークの上に新たなレイヤーが構築されました。このネ

ットワークはライトニングと呼ばれ、限りなく低コストかつ即時のビットコイン決済が実現しています。エルサルバドルなどの国ではすでに活発に利用され、成果を上げています。

このため、ビットコインによる日常的な決済の大半は、将来的にライトニングネットワークを介して行われるようになると考えられています。この分野の開発は急速に進んでいて、例えばTwitterは、ライトニングネットワークを利用した「投げ銭」機能を最近導入しました。また、Strikeのようなアプリは、ライトニングネットワークを通じてさまざまな通貨による国際送金をゼロコストで提供しています。したがって、将来的にはビットコインネットワーク上での決済は大きな金額に限られ、その他の決済はすべてライトニングネットワークを介するようになることが予想されます。

ライトニングネットワークでは主に少額の送金が行われるため、ビットコインの代わりにsatoshi（略してsat / sats）が計算単位として用いられます。1ビットコインは1億satoshiに相当します。ライトニングネットワークを利用するには、ライトニングウォレットを作る必要があります。

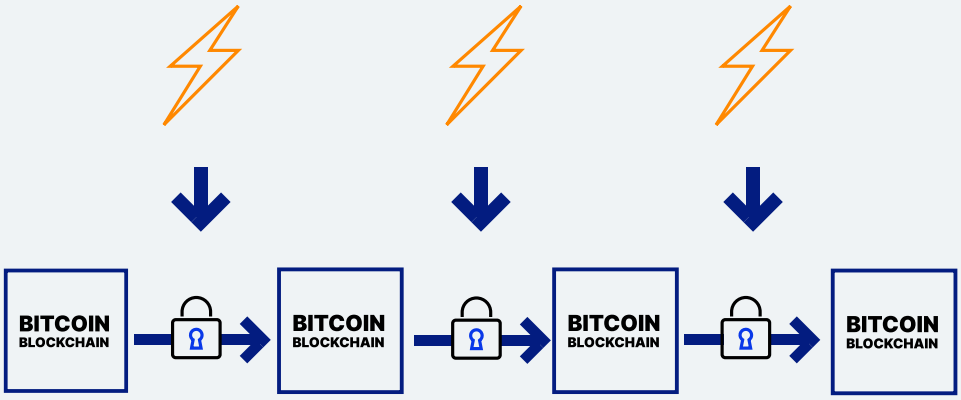
未来への展望

10年以上にわたる歴史の中で、ビットコインは高値と安値を何度も行き来しました。暴落のたびにビットコインは「死んだ」と宣言され、人々の忘却の彼方に追いやられました。それでもなお、ビットコインは着実に世の中に広まり続けています。

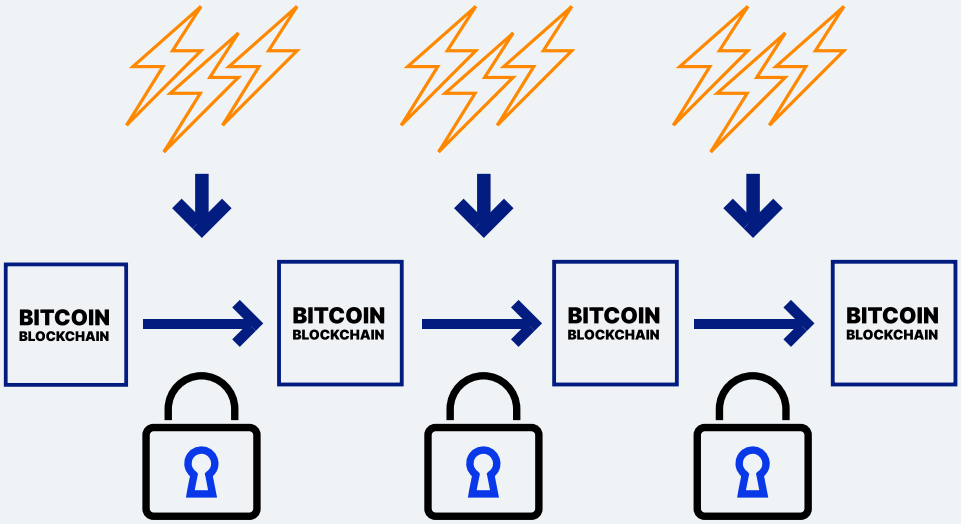
ビットコインとエネルギー

ビットコインの発展をめぐって提起されることの多い懸念のひとつが、ビットコインネットワークのエネルギー消費量です。ビットコインマイニングはすでに世界中で膨大な電力を消費しており、今後参入する人が増えるにつれて、この消費量はますます増加することが予想されます。

ビットコインとエネルギーについて検討する際には、ビットコインネットワークに投じられる電力量がネットワークの安全性にとって極めて重要であるという点を理解しておく必要があります。ビットコイ



ビットコインブロックチェーンの生成に要する演算能力、つまりエネルギーが少なければ少ないほど、後で変更することが容易になる。



ビットコインブロックチェーンの生成に必要な演算能力、つまりエネルギーが多ければ多いほど、後で変更することが困難になる。

ンブロックチェーンに変更を加えるためには、最初にブロックチェーンを生成するために費やされたのと同じだけの演算能力、すなわち電力を再び消費する必要があります。これは、ネットワークに投じられる電力が多ければ多いほどその安全性が高まることを意味します。ビットコインネットワークには世界中で数百万台のコンピュータが演算能力を提供しており、個人や組織、あるいは国家であってもブロックチェーンにほんのわずかな変更を加えられるだけの演算能力を確保することはほぼ不可能です。したがって、ハッシュパワーとそれに伴うエネルギー消費は、ビットコインネットワークのセキュリティ対策の要であると言えます。

ビットコインのマイニングコンピュータには、世界中どこにでも設置できるという強みもあります。マイニングで利益を出すためには可能な限り安価な電力が必要ですから、マイナーの多くは余剰（であるがゆえに安い）電力が豊富に手に入る場所を選択します。長期的には、最も安い電力を生産できる再生可能エネルギーが豊富な地域が選ばれる可能性が高いとみられています。

ビットコインマイニング評議会によると、現時点でのビットコインマイニングにおける再生可能エネルギーの利用率は約56％で、この割合は増加傾向にあります。ビットコイン専門家の多くは、将来的にビットコインマイニングが100％再生可能エ

ネルギーで賄われるようになる可能性もあると予想しています。

しかしそれまでは、ビットコインのエネルギー消費は、安全性が高く偽造不可能な貨幣・価値貯蔵手段がこれだけのエネルギー消費に見合うのかという問いに行き着きます。

エルサルバドル - ビットコインを国の通貨に

先見の明のある人々は、ビットコインが国家によって法定通貨として認められる日が来ることを数年前の時点で予想していました。そして2021年夏、それは現実となりました。エルサルバドルが世界で初めてビットコインを法定通貨として導入したのです。以来、国内の店舗やレストランをはじめ、あらゆるサービスプロバイダが米ドルに加えてビットコインでの支払いを受け入れています。市民には政府公式のビットコインウォレットが提供され、ライトニングネットワークを介した決済がわずか数秒のうちに、しかも最小限のコストで可能になりました。

同様の法案はウクライナ、ブラジル、パナマなど他の国でも議論されています。他の国々がエルサルバドルに続けば、ビットコインの需要がさらに高まるばかりか、何よりビットコインの「貨幣」としての信頼性の裏付けにつながります。したがって、国家によるビットコイン法定通貨化の加速は、世界がビットコインに順応していく過程における重大なフェーズを意味します。

法律と規制

こうした動きから、国家や中央銀行、企業は暗号通貨に集中的に取り組む必要に迫られました。スイス　を含むさまざまな国が、暗号通貨に関する規制やガイドラインを発表しています。このような進展はクリプトプロジェクトと投資家の双方に法的確実性をもたらすことから、多くの市場参加者に歓迎されています。

また、これまで自由放任主義をとってきた米国でも規制は目前に迫っています。クリプトセクター全体に多大な影響を及ぼす米国の新しい規制法がどのような形を取るのか、世界中のクリプトコミュニティが注視しています。

その他の暗号通貨

ビットコインは決して唯一の暗号通貨ではありません。いまや、16,000種類以上の暗号通貨や暗号資産が存在します。これらのコインやトークンはそれぞれ異なる特徴や機能を持ち、すべてが「通貨」やお金としての利用を想定しているわけではありません。中には、その価値がクリプトプロジェクトの成功を反映するという意味で、より株式に近いものもあります。また、特定のサービスを利用するために必要なものもあります。いわゆるミームトークンと呼ばれるものは、ジョークとして作られた通貨です。

損失を避けるためには、投資を行う前にそれぞれの暗号通貨とその背後にあるプロジェクトを詳しく調べることが推奨されます。

中央銀行デジタル通貨（CBDC）

暗号通貨は、規制のない無法地帯のフェーズから、規制されたクリプト金融の世界へと移行しつつあります。このような発展には中央銀行も無関心ではいられず、中央銀行が独自の暗号通貨を発行すべきだという考えも出てきています。中央銀行デジタル通貨（CBDC）を提唱する人々は、それが国家通貨の安定性と、ブロックチェーンベースの通貨の利点を兼ね備えていると主張します。いわばデジタルキャッシュを作り出すということです

しかし、CBDC　はその設計に応じて根本的に異なる形態をとることになります。さまざまな国が異なるCBDCの試験運用を実施し、数カ国ではすでに正式導入されています。しかし、米国、EU、中国など経済力のある通貨圏がCBDCを発行するのか否か、またどのような形で発行するのかは今後の明確化が待たれています。

貨幣競争

ここ数十年で国家通貨に慣れきってしまった私たちの社会では、他の種類のお金について想像することはなかなかできません。しかし、そう遠くない過去には、さまざまなお金が並行して流通することが日常生活の一部でした。銀行ごとに発行される紙幣、異なる金属でできた硬貨など、さまざまな貨幣価値が存在し、支払手段として利用されていました。

ビットコインの登場によって、国家通貨に代わる手段として非国家通貨を利用することが再び可能になりました。ビットコインに対する攻撃を困難にするその非中央集権的な性質も相まって、これまで大半の政府はビットコインを容認してきました。市民にとっては、国家通貨に代わる、金や銀ではないデジタルな手段を手に入れたことを意味します。この新たな貨幣競争がもたらす効果は、今後注目されるところです。

ビットコイン、次はどうする?

ここで得た知識をどう生かせばいいの?という方にご提案があります。ビットコインの世界に入るには、時間もお金も何もかかりません。その一方で、私たちの世界と未来を変えようとしているテクノロジーを直接知ることができます。

ですから、暗号通貨取引所でアカウントを作成するか、スマートフォンにウォレットをダウンロードし、50スイスフランでビットコインを購入してみましょう。あるいは、同僚からビットコインをウォレットに送ってもらいましょう。とにかく一度はビットコインを手にしてみてください。

ビットコインが躍進し、インターネットのように広く普及する頃には、あなたはビットコインを理論的に知っているだけでなく、すでに体験していることになります。このテクノロジーを実際に目の当たりにし、感じることで、大多数の人々の先を行くことができます。そしてこのことが、後に大きな違いを生むことになるかもしれません。

ABOUT

著者

Daniel Jungenは、暗号資産に精通した経済学者、金融ジャーナリストである。Danielは、クリプトに関するあらゆることを専門とするリサーチブティック、InsightDeFiの共同設立者である。InsightDeFiのパートナーとともに、ビットコイン、DeFi、クリプトについて隔週でニュースレター (German) ドイツ語）を配信している。

RELAI

Relaiは、ビットコインを購入するための安全で手間のかからないスペースを見つけるのに苦労したことをきっかけに、Julian LinigerとAdem Bilicanによってスイスで設立されました。ビットコインの貯蓄や投資をより身近なものにするRelaiアプリは、ビットコインのみを取り扱い、デザインはシンプルで直感的。ヨーロッパに住む誰もが、ほんの数分でビットコインを売買できます。登録、認証、入金は不要です。外部の監査を受け、3500万スイスフラン以上のビットコインがプラットフォームを通じて投資されているRelaiは、貯蓄と投資のための新たな手段を提供しています。

詳しくは Relai.app をご覧ください。

この電子書籍を英語から日本語に翻訳してくれた@Haruko_Maruyamaに感謝します。