■著作権について

本レポートと表記は、著作権法で保護されている著作物です。本レポートの著作権は発行者にあります。本レポートの使用に関しましては、下記の点にご注意ください。

■使用許諾契約書

本契約は、本レポートを入手した個人・法人（以下、甲と称す）と発行者（以下、乙と称す）との間で合意した契約です。本レポートを甲が受け取り開封することにより、甲はこの契約に同意したことになります。

第 1 条本契約の目的：

乙が著作権を有する本レポートに含まれる情報を、本契約に基づき甲が非独占的に使用する権利を承諾するものです。

第 2 条禁止事項：

本レポートに含まれる情報は、著作権法によって保護されています。甲は本レポートから得た情報を、乙の書面による事前許可を得ずして出版・講演活動および電子メディアによる配信等により一般公開することを禁じます。特に当ファイルを 第三者に渡すことは厳しく禁じます。甲は、自らの事業、所属する会社および関連組織においてのみ本レポートに含まれる情報を使用できるものとします。

第 3 条損害賠償：

甲が本契約の第 2 条に違反し、乙に損害が生じた場合、甲は乙に対し、違約金が発生する場合がございますのでご注意ください。

第 4 条契約の解除：

甲が本契約に違反したと乙が判断した場合には、乙は使用許諾契約書を解除することができるものとします。

第 5 条責任の範囲：

本レポートの情報の使用の一切の責任は甲にあり、この情報を使って損害が生じたとしても一切の責任を負いません。

Copyright © 杉浦和久 All Rights Reserved.

■目次

Copyright © 杉浦和久 All Rights Reserved.

1-1 そもそもビットコインとは何なのか？

はじめまして、杉浦和久と申します。
数あるレポートの中から、本レポートを受講して、頂き誠にありがとうございます。
この講座を受講しているということは、あなたは少なからず
「**ビットコインとは何なのか？**」

Copyright © 杉浦和久 All Rights Reserved.

と疑問に持っているのではないでしょうか？
結論から言いますと、ビットコインとは、「**お金としての価値を持っている電子データ**」です。
そして、ビットコインは、
「**ブロックチェーンに新しいブロックをつなぐためのノンスを探すマイニング**」
によって誕生します。
この説明で納得できた人は、この講座を受けなくても結構です。
本レポートは、むしろと、今の説明で
「何を言っているのかさっぱりわからない」っという人向けに作成されています。そして、本レポートを受講終えるころには、あなたは今の説明が理解できるようになっています。

1-2 分からないものに投資してはいけない

この講座を受講している人の中には、
・ビットコイン投資に興味がある人
・ビットコイン投資を始めようとしている人
・ビットコイン投資を始めたばかりの人

など色々な人がいると思います。
そんなあなたに伝えたいのは、よくわからないものに投資してはいけない
ということです。

あなたは、以下の質問に答えることができますか？
・ビットコインとは、そもそも何なのか？
・新しいビットコインは、どのように誕生しているのか？
・誰かがビットコインを改ざんすることができるのか？

少し偉そうに質問をしてしまい申し訳ありません。
しかし、安心してください。
これらの質問に答えられる人は、ビットコイン投資をしている中でも一握りだと思いますですが、せっかく自分の大切なお金を投資するわけですから、きちんと理解しているものに投資する方が良いに決まっています。

Copyright © 杉浦和久 All Rights Reserved.

1-3 この講座でビットコインの超基本をマスター

本講座のゴールは、**【ビットコインってそもそも何？】**
という状態のあなたに
・ビットコインの正体
・ビットコインの基本語句
・ビットコインができるまでの流れ
・ビットコインの安全性

など、ビットコインの超基本を理解していただくことです。
それでは、一緒にビットコインについて学んでいきましょう。

2-1 楽天ポイントはお金なのか？

古代初めてお金として使われたものは貝殻でした。
その後、金貨と銀貨が登場し、そこからお金は紙切れになり、今のお札という形をとるようになりました。
今は、現金を持っていなくてもクレジットカードやスマホがあれば決済ができ、キャッシュレス化が浸透しています。その結果、お金が形を持たなくなってきています。そしてついに、**楽天ポイント**なるものがお金として使われ始めることになりました。
楽天ポイントは、楽天が発行している単なる電子データにすぎないです。
楽天ポイントは、日本などの国が発行したものではなく、楽天という一つの企

Copyright © 杉浦和久 All Rights Reserved.

業が発行したものです。
そんなお金とかけ離れた存在ともいえる楽天ポイントが、1 ポイント=1 円の価値を持っています。単なる電子データが、お金として扱われ始めています。
そして、ビットコインも単なる電子データです。

2-2 ビットコインの正体は電子データ

ビットコインの正体は、**単なる電子データ**です。
どんな電子データかと言うと

A から B に 1 ビットコイン送るよ、という電子データです。
これが ビットコインの正体なのです

ビットコインと言ってはいますが、実際にコイン という実物があるわけではありません当然現金のように持ち歩くこともできません。
ですがビットコインにはお金としての価値があります。
なんだか不思議な存在ですね。

2-3 ビットコインは、イメージ的には楽天ポイントと同じ

楽天ポイントもビットコインと同じで実体のないただの電子データです。
当然現金のように持ち歩くことはできません。
にもかかわらず、楽天ポイント自体に 1 ポイント=1 円の価値があり、買い物にも使えます現在は、1 ビットコインは、約 600 万円なので、1 ビットコインで約 600 万円分の買い物ができます。

ビットコインで買い物？
そんなことをしている人を見たことがない、という人がほとんどだと思いますですが、案外ビットコイン決済ができるお店はあるんです。もちろん日本にもあります例えば全国のビックカメラでは、ビットコインで買い物をすることができます楽天ポイントと同じでスマホで、ﾋﾟｯと決済ができてしまいます

Copyright © 杉浦和久 All Rights Reserved.

2-4 ビットコインには現金にない特徴がある

ビットコインは電子データで、その電子データ自体にお金としての価値があります。楽天ポイントは、楽天への信頼があるため 1 ポイント=1 円という価値を持っています。

対してビットコインには、今までの現金には無かった特徴があります。その特徴が多くの人に認められているからこそ、1 ビットコイン=600 万円という価値を持っています。

ビットコインの持つ特徴は以下の 6 点です

＜ビットコインの特徴＞

① 所有者がわかる
② 改ざんが不可能
③ プライバシーが守られている
④ 中央政府が管理していない
⑤ 価値が上がっていく
⑥ 海外に安く送金できる

このようになります。
それでは、これら特徴について解説していきます

2-5 ビットコインは、所有者がわかる

ビットコインには、所有者が分かるという特徴があります。
もしあなたが 1 万円落としてしまい、誰かがその 1 万円拾ったとします。
お金を拾った人は、コンビニに行き、あなたの 1 万円を使ってしまいました。
その後、あなたがコンビニに行き、今の 1 万円は、私のものだから返してと言っても返してもらえませんよね。ビットコインなら所有者が分かるのでこのような悲劇は起きません。先ほど、ビットコインは、楽天ポイントみたいなものだと言いました。

例えば、楽天ポイントだと楽天から A さんに 2000 ポイント送るよ、という明確なデータが残ります。なので楽天ポイントは、誰の楽天ポイントがすぐわか

Copyright © 杉浦和久 All Rights Reserved.

るわけです。
それと同じで、ビットコインにも A から B に 1 ビットコイン送るよ、だからこの 1 ビットコインは B さんのだよーというデータが残っています。
そのため私のビットコインが勝手に使われた、なんてことはないです。

ちなみに“https://www.blockchain.com/”というサイトを使えば、誰でもビットコインのデータを確認することができます。
ビットコインアドレスと取引の記録は残っているので、ビットコインの所有者はすぐに分かります。

2-6 改ざんが不可能

ビットコインには、改ざんできないという特徴があります。
なぜならビットコインには、ブロックチェーンという仕組みが導入されているからですその上、ハッシュ関数という、とてつもない暗号技術が採用されています。

ブロックチェーンやハッシュ関数については後日説明いたします。実際に 2011 年から現在まで、ビットコインの改ざんは一度も行われていません。
それに比べ現金は、日本円でさえ大量の偽札が作られています。

警察庁のデータによると、2018 年には 1500 枚以上の 1 万円の偽札が発見されました。発見なので実際にはもっと多くの二セ札が出回っていることは容易に想像できます。そう考えるとビットコインの安全性はかなり驚異的と言えます

2-7 プライバシーが守られている

ビットコインには、プライバシーが守られているという特徴があります。
というのもビットコインで決済する場合は
・ビットコインを誰に送るか
・ビットコインアドレス
の二つの情報開示すれば決済が完了します。

Copyright © 杉浦和久 All Rights Reserved.

それに比べクレジットカード決済では
・住所
・氏名
・電話番号
・クレジットカード番号
・買ったもの

など多くの個人情報を企業に開示することになります。
Google などの企業はこうして集めた個人情報から、個人に適した広告を表示しています。クレジットカード決済が普通になって今だからこそ、プライバシーについて考えるべき、ときが来ていると言えます。

2-8 中央政府が管理していない

2000 年、ジンバブエのムガベ大統領は、白人から農地を強制的に取り上げ、黒人に分配しました。この政策に反発した欧米諸国は、ジンバブエに経済制裁を与え、ジンバブエの財政は大打撃を受けました。
ムガベ大統領は、財政再建のため自国の通貨を乱発しました。その結果、ジンバブエの通貨は、著しく価値を失ってしまいました。
対米ドル換算ですと、1 ドル=三京 5000 兆ジンバブエ　というとてつもないハイパーインフレがジンバブエを襲ってしまいました。
中央政府には、貨幣発行権があり、好き勝手に紙幣を印刷することができます。
中央政府に権力を集めすぎた結果、起きてしまった悲劇です。

ビットコインは、中央政府が管理してないという特徴があります。
では誰が管理しているのかと言うと、みんなで協力して管理しています。
具体的には、
・ビットコインの使用者
・ビットコインを作るマイナー
・ビットコインの不正を取り締まるフルノード
・ビットコインのシステムを作る開発者

Copyright © 杉浦和久 All Rights Reserved.

というような人たちが、ビットコインを管理しています
マイナーとフルノードについては、後で再登場するので頭の片隅に入れておいてください。

日本に住んでいると、日本銀行が作るお札は信じられない、日本が発行していないお金が欲しい、なんて思う人はほぼほぼいません。
ですが先ほどの話でも紹介したとおり、ジンバブエなどの発展途上国では自国のお金は信じられない！国が発行していないお金が欲しい、という人は山ほどいます。そんな人たちの願いを叶える通貨が、ビットコインです。
繰り返しになりますが、ビットコインは、みんなが協力して管理しています
中央政府が管理していないお金という、他に類を見ない特徴がビットコインにはあります。

2-9 価値が上がっていく

ビットコインには、価値が上がっていくという特徴があります
というのも、ビットコインには、2100 万枚しか作れないというルールがあります。欲しい人が増えても、2100 万枚限定なので、価値が上がっていくことが予想されています。

それに比べ国が発行する紙幣は、無限に発行することができます。
実際に日本でも毎年約 13 兆円もの日本円が発行されています。
なので現金は価値が下がっていくのが自然なんです。

Copyright © 杉浦和久 All Rights Reserved.

歴史上最も価値が安定している通貨である米ドルさえも、100 年で 90%価値が下がっています。無限に作ることができないというのは、ビットコインの大きな特徴の一つだと言えます。

2-10 海外に安く送金できる

ビットコインには、海外に安く送金できるという特徴があります。
そもそもなぜ、海外への送金にお金がかかるかと言うと、多くの銀行が間に入るからです。多くの銀行に手数料払う分、現金を海外に送るための費用は高額になります。

それに比べて、ビットコインは、個人が個人にビットコインを贈るだけです。
個人間のやり取りで、銀行の手数料が発生しない分、海外の人にも安く送金できるというわけです。

2-11 第２章のまとめ

ビットコインとは、何だったか覚えていますか？
答えは、ビットコインは、ただの電子データです。
しかし、その電子データ自体に、お金としての価値があります。

ビットコインには、６つの特徴があります。

１．所有者がわかる
２．改ざんが不可能
３．プライバシーが守られている
４．中央政府が管理していない
５．価値が上がっていく
６．海外に安く送金できる

このような特徴になります。

・１．ビットコインには、今までの現金にはなかった、多くの特徴があるのでお金としての価値を持っています。

Copyright © 杉浦和久 All Rights Reserved.

・２．ビットコインには、ブロックチェーンやハッシュ関数といった暗号技術が使われ、改ざんがほぼ不可能です。

・３．ビットコイン決済では、個人情報を開示する必要がありません。

・４．ビットコインは、使用者・マイナー・フルノード・開発者など多くの人によって管理されています。

・５．ビットコインの発行は、2100 万枚までというルールがあるので、価値が上がっていく仕組みになっています

・６．ビットコインは、銀行などの協力が必要ないので、安く海外に送金することができます

ビットコインの正体は、 A から B に 1 ビットコイン送るよ、的な電子データだということを学びました。ですがなぜ A から B に 1 ビットコイン送る、という電子データがビットコインになり得るのでしょうか？

次の第３章で、この内容について解説致します。

3-1 ビットコインの基本語句とは？

これから学ぶ基本語句は、こちらの７つです

１．トランザクション
２．ブロック
３．ブロックチェーン
４．マイニング
５．ノンス
６．マイニング報酬
７．ハッシュ関数

Copyright © 杉浦和久 All Rights Reserved.

これら７つになります。
詳細説明については、次の講義から説明しています。

3-2 トランザクション

トランザクションとは、ビットコインにおける一つの取引です。
ビットコインは、人から人へ送られます。
その一つの取引が、トランザクションと呼ばれています。
単純に取引を英語訳するとトランザクションになります。

例えば A から B に 1 ビットコイン送るよ、というのが 1 つのトランザクションです。
以前の講義でビットコインの正体は、 A から B に 1 ビットコイン送るよ、という電子データだとお伝えしました。

ビットコインとはつまり、このトランザクションの集まりなんです。

とはいえビットコインは、世界中で取引されているので、世界中でトランザクションが溢れています。そのため世界中に溢れるトランザクションを、まとめることが必要になってきています。

3-3 ブロック

ブロックとは、10 分間のトランザクションのまとまりです。
ビットコインは、世界中で取引されているので、世界中でトランザクションが溢れています。
というわけで、トランザクションを 10 分に 1 回まとめています。
そのようにまとめられたものが、ブロックと呼ばれています。
10 分に一個のブロックができるので、時間が経てば経つほど、世界中にブロックが溢れて行きます。

Copyright © 杉浦和久 All Rights Reserved.

3-4 ブロックチェーン

ブロックチェーンとは、ブロックがつながった一本のチェーンです。
ブロックは、10 分に一個できるとお伝えしました。
なので、1 時間で 6 個、1 日で 144 個できる計算になります。

ブロックチェーンにある最後尾のブロックに、新しいブロックをくっつけて行くのでブロックチェーンは枝分かれのない一本のチェーンになります。

10 分に 1 回、こうして長くなっていく一本のチェーンが、ブロックチェーンと呼ばれているわけです

これらをまとめると
1．まず、トランザクションを集める
2．そして、10 分間で集めたトランザクションを一つのブロックにする
3．最後に、できたブロックをブロックチェーンにくっつける

という感じになります。
なのでブロックチェーンには、すべてのトランザクションが集まりビットコインに起きたすべての取引が記録されています。
実際にブロックチェーンには、2009 年にビットコインが誕生してから、すべての取引内容が記録されています。

3-5 マイニング

マイニングとは、ブロックチェーンに新しいブロックをつなげるための鍵を探す作業です。ちなみにマイニングをする人をマイナーと言います。

ブロックチェーンの最後尾のブロックには、新しいブロックが勝手にくっつくわけではありません。ブロックチェーンとブロックをつなげるためには、ノンスと呼ばれる鍵が必要になります。その鍵を探す作業がマイニングなのです。

Copyright © 杉浦和久 All Rights Reserved.

3-6 ノンス

ノンスとは、ブロック同士をつなげるための鍵で、1 から約 43 億までのランダムな数字のことです。
なので、
100 もノンス
3000 もノンス
10 億もノンス
なんでもかんでもノンスです！

マイニングに必要な鍵と言いましたが、この鍵とはただの数字のことです。
イメージ的には、自転車の暗証番号式の鍵を思い浮かべてください。

例えば、暗証番号を忘れたら、1 から 9999 まで頑張って試しますよね。
マイニングは それらの 1 から 43 億バージョンで、正解の暗証番号がノンスと呼ばれています。

ここで再度、まとめると
１．トランザクションを集める
２．10 分間で集めたトランザクションを一つのブロックにする
３．できたブロックをブロックチェーンにくっつける
４．くっつけるためには 1 から 43 億の中から正解の数字（ノンス）が必要になる
５．マイナーはマイニングによって正解の数字を探す

という感じになります
なのでマイニングを超簡単に表すと数字探しゲームです。
１から 43 億までの数字の中で、正解を見つける数字探しゲームが、10 分に一回、新しいブロックが出来る度にスタートします。
そして、一番早く数字の正解を見つけた人がゲームの勝者です。
マイニングといっても、ただの数字探しゲームと考えると簡単に思いますね。

Copyright © 杉浦和久 All Rights Reserved.

3-7 マイニング報酬

マイニング報酬とは、マイニングに成功したマイナーに支払われる報酬です。
マイニングとは、簡単に言うと

1 から 43 億の数字の中から正解を探す数字探しゲーム

でしたよね？

実は 1 から 43 億までの数字は当てずっぽうで探していきます。
なので最悪 43 億回の試行錯誤は必要なわけです。

マイニングは、ものすごく大変です。
ちなみに必死に数字を探して、マイニング報酬を獲得する様子が鉱山労働者が採掘する様子に似ているのでマイニングと呼ばれています。

とにかくマイニングは、大変なのでマイナーからするとボランティアでマイニングはやってられないです。
そのためマイニングに成功したマイナーには、報酬としてビットコインが与えられています。そしてマイナーに与えられるビットコインこそが新しくできるビットコインなのです。

ここまでの流れをまとめると

1．トランザクションを集める
2．10 分間で集めたトランザクションを一つのブロックにする
3．できたブロックをブロックチェーンにくっつける
4．くっつけるためには 1 から 43 億の中から正解の数字が必要になる
5．マイナーはマイニングによって正解の数字（ノンス）を探す
6．正解の数字が見つかると新しいビットコインが誕生する
7．新しくできたビットコインはマイナーにプレゼントされる
という感じになります。
なのでマイナーは ビットコインを作る人と言われています。

Copyright © 杉浦和久 All Rights Reserved.

ちなみに 1 回のマイニング報酬は、ビットコイン価格によりますが、現在はおおよそ 3,000 万円以上になります。

3-8 ハッシュ関数

ハッシュ関数とは、何でも 64 桁の数字で返す関数のことです。
厳密には少し違いますが、とりあえず 64 桁で帰ってくる関数という認識で OK です。ビットコインは、改ざんがほぼ不可能だと説明しました。
何を隠そう、ビットコインの改ざんを防ぐ暗号の役割をしているのが、このハッシュ関数なのです。
ハッシュ関数は、ビットコインの暗号技術の根幹と言っても過言ではありません。ちなみにハッシュ関数から得られる値のことをハッシュ値と言います。
ハッシュ関数の凄さは大きく分けて二つあります

１つ目が、**一文字変わるとハッシュ値が大幅に変わる**

そして２つ目が、**一方向性**
です。

まず、一文字変わるとハッシュ値が大幅に変わる　について解説します。
ハッシュ関数には、入力する文字が一文字でも変わると出てくるハッシュ値は大幅に変化するという性質があります。
こちらは、ハッシュ関数が体験できるサイトです。
こちらに「ハッシュジェネレータ」があります。

⇒https://www.convertstring.com/ja/Hash/SHA256

ここに例えば、”あああ”と”ああい”を別々に入力し、ハッシュ値を求めてみてください。
”あああ”と”ああい”のハッシュ値を見て頂ければ一目瞭然です。
全く異なるハッシュ値がでてきます。

Copyright © 杉浦和久 All Rights Reserved.

次に、一方向性　についてです。
ハッシュ関数には、一方向性という性質があります

具体例を出すと
さきほどのハッシュジェネレータに“あいうえお”を入れると､ハッシュ値は簡単に求められます。
しかし、このハッシュ値をもとに、「あいうえお」を求めることは、ほぼ不可能です。ハッシュジェネレータに文字・数字を入れまくるれば、もしかして、奇跡的に同じハッシュ値になるかもしれませんが、同じ文字・数字の答えを導くのはほぼ不可能です。
これがハッシュ関数の持つ、一方向性と言われる性質になります。
まあ一方通行みたいなイメージです。
さすがは Bitcoin の暗号技術の根幹を支える関数です。

3-9 第３章のまとめ

第３章では、覚えるべき＜ビットコインの基本語句＞７つをお伝えしました。
その７つの基本語句とは、

１．トランザクション
２．ブロック
３．ブロックチェーン
４．マイニング
５．ノンス
６．マイニング報酬
７．ハッシュ関数

これら７つです。
１．トランザクションは、ビットコインにおける一つの取引で、A から B に１ビットコイン送るよっという感じの内容です。

２．ブロックは、10 分間のトランザクションのまとまりです。

３．ブロックチェーンは、ブロックが繋がった一本のチェーンです。

Copyright © 杉浦和久 All Rights Reserved.

４．マイニングは、ブロックチェーンに新しいブロックをつなげるための鍵を探す作業で、最も早くマイニングに成功した人にマイニング報酬として新しく誕生したビットコインが与えられます。

５．ノンスは、ブロック同士をつなげるための鍵で 1 から約 43 億までのランダムな数字です。

６．マイニング報酬は、マイニングに成功したマイナーに支払われる報酬です。

７．ハッシュ関数は、どんな文字や数字も 64 桁の数字で返す関数で、一方向性があるので、ハッシュ値から元の数字・文字を求めることはほぼ不可能です。

4-１　ビットコインの安全性

結論から言うと、ビットコインは安全です。
しかし、ビットコインを改ざんすることは理論上可能です。
ですがビットコインの改ざんは、ほぼ不可能に近く実際にやろうとする人はなかなか現れないです。

ビットコインを改ざんするには、二つの方法を行う必要があります。

Copyright © 杉浦和久 All Rights Reserved.

まず、**１つ目の方法は、**
過去のブロックを改ざんする　必要があります。

そして、次に

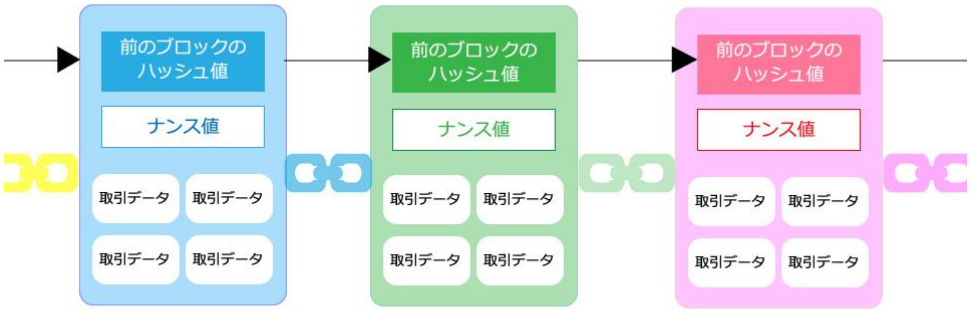
新しいブロックを改ざんする　必要があります。

１．過去のブロックを改ざんする場合は、全てのブロックを改ざんする必要があり、世界中のデータを一気に改ざんする必要があります。

そして、
２．新しいブロックを改ざんする場合は、世界中のマイナーが敵になります。
なぜならば、改ざんするとビットコインの価値がゼロになるからです。
これら詳細については、次の講義を説明致します。

4-2 過去のブロックを改ざんする

■ブロックチェーンのデータ構造



各取引データは、順番にブロックに格納。各ブロックが、直前のブロックとハッシュ値でつながっているため、改ざんが極めて困難

ビットコインを改ざんする方法の一つ目は、
過去のブロックを改ざんする
ことです

ではビットコインを改ざんしようとする人をハッカーＡと名づけます。

Copyright © 杉浦和久 All Rights Reserved.

ハッカーＡは、過去のブロックの中にある Ａ から Ｂ に１ビットコイン送るを改ざんします。これは理論上可能ですが、実際にやる人は現れにくいです。
なぜならば、過去のブロックを改ざんする場合、全ての過去のブロックを改ざんする必要があるからです。
ひとつのブロックを改ざんするには、全てのブロックを改ざんする必要があります。なぜなら一つのブロックを改ざんすると全てのブロックに異常をきたしてしまうからです。

ハッシュ関数には、入力する文字・数字が少しでも変わるとハッシュ値が大幅に変わるという性質があります。ブロックを改ざんするとハッシュ関数から出てくるブロックハッシュ値が大幅に変わります。
つまり過去のブロックを改ざんすると、後に続く全てのブロックがおかしくなってしまいます。

そのため過去のブロックを改ざんしたハッカーＡは、新たに改ざんしたブロックに適したノンスを探し直す必要があります。というように全てのノンスを探し直す作業が必要なわけです
ノンスを探すのがどれだけ大変か、ここまで講義を受けたあなたには理解できると思います。これが過去のブロックを改ざんする人は現れない理由です。

4-3 世界中のデータを一気に改ざんする必要がある

ブロックが改ざんされにくい二つ目の理由は、
世界中のデータを一気に改ざんする必要がある
からです

では実際にどのデータを改ざんすれば良いのでしょうか？
答えは世界中に散らばった 1 万 5000 以上のパソコンのデータを一気に改ざんする必要があります。
世界中に散らばった１万 5000 以上のパソコンのことをフルノードと言います。
本来のフルノードはパソコンのことですが、ややこしいので、人として考えてみると、フルノードは ビットコイン界の警察的な役割を担っています。

Copyright © 杉浦和久 All Rights Reserved.

というのも、フルノードは過去のビットコイン取引が全て保管されています。
なので何かおかしいことがあった時には、
あれブロックが改ざんされてない？
と気づくことができます

そしてフルノードたちは、改ざんされたブロックを見抜き、正しいブロックとは認めません。まさにフルノードは ビットコイン界の警察的な役割を担っています。そしてフルノードは先ほど言った通り 15000 人以上いて、世界中に散らばっています。
ちなみにあなたのパソコンにもビットコインの全取引データをダウンロードすればフルノードになれます。
ハッカーＡは、世界中に散らばった１万 5000 以上のパソコンのデータを
一気にハッキングして、一気にノンスを求めて、一気に改ざんする必要があります。
どんなに優秀なハッカーでもこの作業はほぼ不可能です。
そのためブロックチェーンは改ざんできないと言われています。
やはりブロックチェーンとハッシュ関数を使った暗号技術はすごいですね。

4-4 第４章のまとめ

ビットコインを改ざんするには、まず、
１．過去のブロックを改ざんする
そして、
２．新しいブロックを改ざんする　必要があります。

１．過去のブロックを改ざんする　には、全てのブロックを改ざんする必要があり、世界中のデータを一気に改ざんする必要があります。

次に２．新しいブロックを改ざんする　には、
世界中の 15,000 以上あるフルノードを一気に一気に改ざんする必要があります。改ざんができたとしても、ビットコインの価値がゼロになるので、マイニングに勝てるなら普通に稼いだ方がいいことになるからです。

Copyright © 杉浦和久 All Rights Reserved.

要点をまとめると、
ビットコインの改ざんは、理論的に可能だが、やろうとする人が現れにくい仕組みになっている。
過去の１ブロックを改ざんするとノンスを全て探し直さないといけない。
フルノードは世界に15000人以上いて過去のビットコイン取引が全て保管されている。ビットコインに改ざんが起こるとビットコインの価値がゼロになる。
このような理由から、ビットコインは安全です。

5-1 最後に

本講座を最後まで受講して頂き、誠にありがとうございます。
如何でしたか？
冒頭で、
・ビットコインとは、お金としての価値を持っている電子データです。
・ビットコインは、ブロックチェーンに新しいブロックをつなぐためのノンスを探すマイニング作業によって誕生します。

という二つの文章をお伝えし、全て講義を受けた後に、あなたがこの二つの文章を理解できるようになることをお伝えしました。
あなたが無事にこの２つの文章を理解できたと信じていますが、残念ながらそれを確かめる手段がありません。

もし、この２つの文章を理解することができていたら、レビューでお伝えして頂けると嬉しいです。

それでは、今回は以上となります。
ありがとうございました。
——

■発行者情報
発行者：杉浦和久
連絡先：crypto@dotcomexpertsecrets.com

Copyright © 杉浦和久 All Rights Reserved.

ブログ：https://dotcomexpertsecrets.com/

■おススメ教材

商品名:4 年に 1 度しか訪れない仮想通貨投資の一大イベントが来年 2024 年 4 月に訪れるのをあなたは知っていますか？

⇒ **コチラから**

1． 今さら聞けない、仮想通貨（暗号資産）ビットコインの基礎の基礎

⇒ **コチラから**

2．仮想通貨（暗号資産）ビットコインの超基本を学ぶ

⇒ **コチラから**

3．仮想通貨（暗号資産）ビットコインの全ての基礎がわかる

⇒ **コチラから**

4．草コインからビットコインに次ぐ将来有望な銘柄の探し方

⇒ **コチラから**

5．日本人の 99%が全くわかっていない仮想通貨の超ポテンシャル

⇒ **コチラから**

6．仮想通貨投資を元手に資産形成をし老後を自由気ままに過ごす戦略

⇒ **コチラから**

7．失敗しない国内仮想通貨取引所を選ぶために注目すべき 4 条件

⇒ **コチラから**

8．失敗しない海外仮想通貨取引所を選ぶために注目すべき条件

⇒ **コチラから**

Copyright © 杉浦和久 All Rights Reserved.

9. メタマスク（MetaMask）完全操作マニュアル
⇒ **コチラから**

10. NFT(ブロックチェーン)ゲームを無課金で遊べるおすすめ９選
⇒ **コチラから**

11. 2024 年４月の４度目のビットコイン半減期を大予測
⇒ **コチラから**

12. 年利 8%以上で運用ができる仮想通貨ステーキング【超入門】
⇒ **コチラから**

13. 意外と知られていない超高いコスパの仮想通貨積立とは？
⇒ **コチラから**

14. １億倍を達成した第２のビットコインを探し出すアルトコイン戦略
⇒ **コチラから**

15. 草コインを当中させ億り人になるアルトコイン完全攻略マニュアル
⇒ **コチラから**

16. 2024 年５月からビットコイン仮想通貨のバブル相場が始まる！
⇒ **コチラから**

17. 仮想通貨積立ｘステーキングを同時実現させるハイブリッド投資
⇒ **コチラから**

18. 通勤時のすき間時間にポイ活して毎月１万円のこ小遣いを貯める
⇒ **コチラから**

19. リスクゼロで３万円の軍資金を準備する【自己アフィリエイト】
⇒ **コチラから**

Copyright © 杉浦和久 All Rights Reserved.