モノづくり通信

iLINK

Vol.60　2019 年 10 月発行

1．ごあいさつ

猛暑もようやく終わり過ごしやすくなってきたこの頃、いかがお過ごしでしょうか。（株）アイリンクの照井清一です。夏休に子供とプールへ行ったら、腹の肉をさんざん摘まれ笑われました。悔しかったのでダイエットを決意しましたが、秋の味覚、度重なる宴会と、ダイエットには厳しい道のりを様々な誘惑と戦っています。

2. 仮想通貨の生まれた背景　～ブロックチェーン技術とビットコイン～

ビットコインを代表とする仮想通貨、価格が乱降下し大損する人が出るなど、多くの人々はわけがわからないものと感じています。仮想通貨が生まれた背景は 2 つあり、1 つは思想です。欧米では国家権力への不信から私的財産への制限を嫌い、個人の自由を重んじるリバタリアンと呼ばれる人達がいました。その一部が「中央銀行の呪縛から解き放たれた通貨」として仮想通貨に取り組みました。もう 1 つは、新興国では脆弱な経済基盤や政府の失策により自国通貨の価値が極めて不安定なため通貨が暴落し富裕層が資産を失うことがあり、交換が容易で自国通貨より安定した貨幣のニーズがありました。

2-1　ビットコインとは何か

ビットコインとは、紙幣や硬貨などの実態のない電子的な貨幣です。一般的な貨幣のように中央銀行が発行せず、ビットコイン財団が管理･運営するオープンソースプログラムにより運用されています。そのため円やドルなどの通貨との交換レートは保証されていません。このような電子的な貨幣を仮想通貨(暗号通貨)と呼びます。

1990 年代、リバタリアン的思想のソフトウェア技術者達が政府の介入の及ばない電子マネーに取り組んでいました。2008 年 8 月サトシ・ナカモトは、彼らのコミュニティに 9 ページの論文を投稿しました。論文には完全にオープンな環境でも偽造できない電子マネーの仕組みが書かれていました。これは発生した取引をネットワークに参画するすべてのコンピューターに記録する方法で、取引記録を承認するには難しい暗号を解く必要があります。最初に暗号を解くと報酬として一定の電子マネーが与えられます。サトシはこれをビットコインと名付けました。

2-2　ビットコインの技術とは

他人にお金を送金するには金融機関の決済システムを利用します。決済システムにより自分の口座から相手の口座に金額が移動し送金が完了します。

ビットコインはブロックチェーン技術を用いて、世界中どこでもインターネットがつながっていれば短時間に極めて低い手数料で送金ができます。このビットコインのコア技術を以下に述べます。

①　P2P ネットワーク

ビットコインは、ビットコイン全体を管理するサーバーのない P2P ネットワーク（Peer to Peer）です。これはネットワークにつながっているコンピューター同士が情報を交換する方式で、すべての取引は誰でも見ることができます。ビットコインのプログラムをインストールすると、2009 年から続いたすべての取引データ(元帳)が何十ギガバイトと送られてきます。

②プルーフ・オブ・ワークとマイニング

10 分間ごとのビットコインの取引記録をまとめたものがブロックです。新しいブロックの承認は誰でもできますが、そのためには誰よりも早く問題を解かなければなりません。その問題とは、前のブロックのハッシュ値がシステムの要求する値となるような値(ナンス値)を求めることです。これは 1 つずつ値を入れて探すしかなく、コンピューターのパワーを大量に投入した総当たり戦で行います。その結果、勝者になれば 12.5 ビットコイン(2019 年 9 月 18 日の相場で 1,333 万円)と、10 分間分の送金手数料を獲得します。

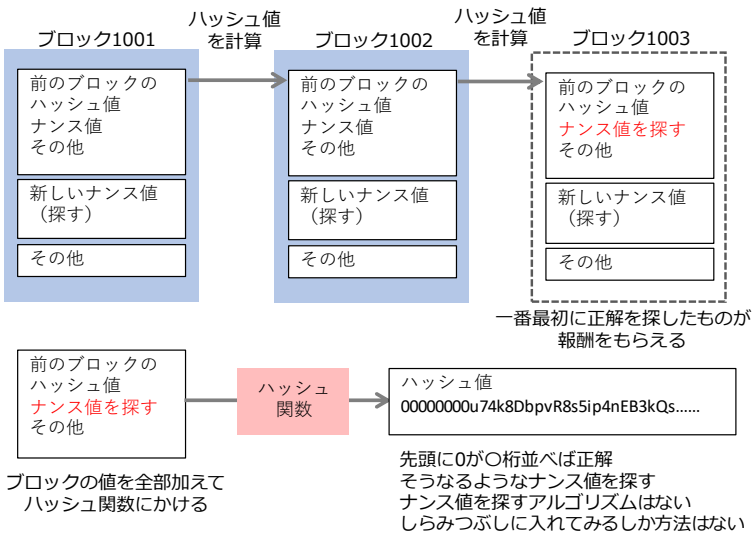

図 1　プルーフ・オブ・ワークの仕組み

これがプルーフ・オブ・ワークで、このナンス値を決めることをマイニングと呼びます。マイニングには膨大な計算パワーが必要なため、現在は特定のグループが組織的に行っています。もし、悪意ある者が取引記録(ブロックのデータ)を改ざんしようとすれば、再びプルーフ・オブ・ワークの答えを出さなくてはなりません。それには膨大な労力が必要で、それよりマイニングに参加した方が効率よく報酬が得られます。そのため誰も改ざんしなくなります。ビットコインの総発行量は 2,100 万 BTC と決まっています。

＜ハッシュ関数＞

ハッシュ関数とは、どのような入力値を入れても、一定の長さの文字列に変換する関数で、出力された文字列から入力値が分からないという特徴があり、ソフトウェアでの暗号化によく使われます。

2-3　ビットコインのブロックチェーン技術の特徴

以下、ビットコインの特徴をまとめました。

【長所】
- ● 完全にオープンでかつ改ざん不可能な高いセキュリティ
- ● すべての取引が記録され、誰でも見ることができる
- ● P2P 方式で管理主体が不要なため事故やトラブルに強い
- ● 供給量が制限され価値が低下しないため、通貨としての機能を持つ

【短所】
- ■ システムを維持するためのマイニングに大変な努力が必要
- ■ 承認作業に時間がかかる
- ■ すべての取引を毎回記録するため、ネットワーク間に大量の通信が発生
- ■ 管理主体がないため、アップデートが容易でない

2-4　プライベートチェーンの特徴

ビットコインはセキュリティの高いシステムですが、このような短所があるため、現在は「管理主体(銀行や団体)によるクローズなシステム（プライベートチェーン)」が主流になっています。

① 取引の承認は管理主体によって指定された一部のノードに限られている
② 取引の承認を少数のノードで行うため、迅速な取引承認が可能。しかもプルーフ・オブ・ワークが不要
③ 管理主体があるため、アップデートが容易

3. 国際送金の問題と金融サービス

海外、特に新興国は銀行の支店が少なく、銀行間の送金に数日かかることは珍しくありません。しかも銀行口座を持てない人も多く、彼らは十分な金融サービスを受けられません。そんな彼らも海外へ出稼ぎに行くと、海外から家族へ国際送金する必要が生まれます。

現在の海外送金は次の問題があります。
① 手数料が高い、② 時間がかかる、
③ 手数料が不透明、④ 送金状況が不透明

3-1　新興国の金融サービス

多額の現金を送るニーズがあったケニアでは、個人向け送金システム「エムペサ」が広く普及し、国民の半数以上が利用しています。

エムペサは至る所にあるエムペサの取扱店で送金したい相手の携帯番号を知らせ送金するお金を払います。その後相手に金額と暗証番号をショートメッセージで送ります。相手は近くのエムペサ取扱店で、金額、取扱番号、暗証番号を入力すれば現金を受け取ることができます。

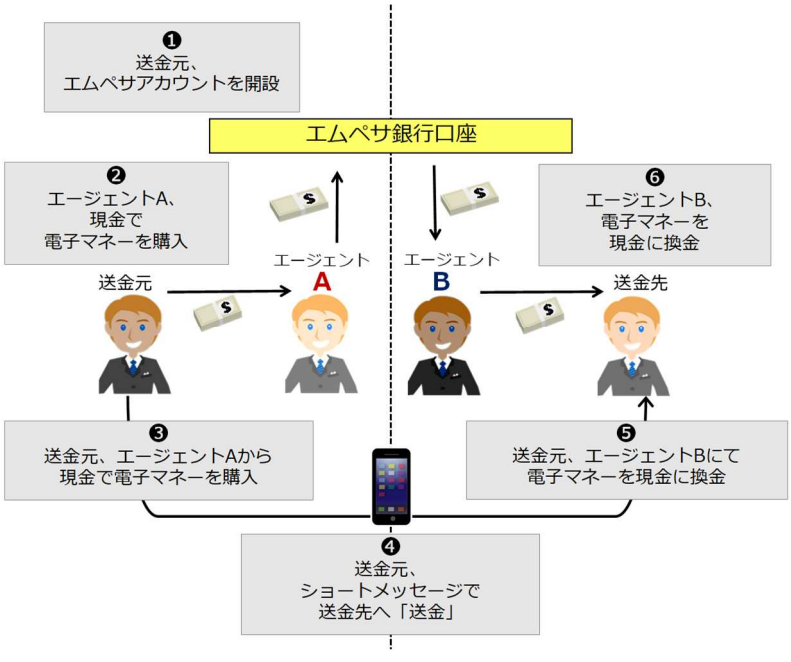

図 2　エムペサの仕組み

3-2　お金にマイナスの金利をつける「ゲゼルマネー」の復活

1920 年代、景気刺激策として、ドイツの経済学者シルビオ・ゲゼルは、紙幣にマイナスの金利をつける「ゲゼルマネー」を提唱しました。これは保有期間に応じたスタンプを購入し、紙幣にスタンプを押さなければ使えなくなるお金です。お金の価値が低下するため、受け取った人は早く使います。ゲゼルマネーは 1930 年代にオーストリアで地域内通貨として発行され地域経済を短期間に活性化しましたが、疑似通貨とみなされ政府から発行を禁止されました。

マイナス金利政策でも消費は上向かず、デフレ対策に行き詰っている先進国の中央銀行は、これを打破するためにゲゼルマネーの復活案が出ています。紙幣から電子マネーになれば、時間の経過とともに金額を減らすのは容易になり、スタンプを使わなくてもマイナス金利が実現します。

4. フィンテックで変わる金融サービス

IT 技術とファイナンスを融合したフィンテックが脚光を浴びています。フィンテックには様々なものがありますが、ここでは 2 つ紹介します。

4-1　少額送金

【トランスファーワイズ】

ターベット・ヒンリンクスとクリスト・カールマンという 2 人のエストニア人が創業した企業で、1 回の海外送金を 2 回の国内送金で実現することで海外送金の手数料を大幅に引き下げました。

図 3 のようにイギリスからドイツに送金したい人とドイツからイギリスに送金したい人をマッチングし、トランスファーワイズの口座を経由して送金します。その結果、2 回の国内送金で 1 回の海外送金ができます。為替レートや海外送金の手数料が不要となり、従来の 1/8 の費用で海外送金を実現しました。

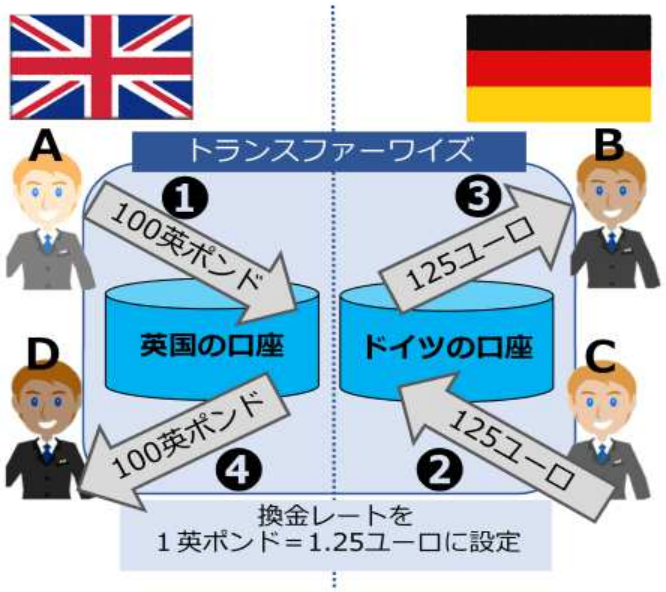

図 3　トランスファーワイズの仕組み

4-2　マイクロペイメント

仮想通貨や電子マネーの利点は送金コストが非常に安いことです。これにより、従来のクレジットカード決済では手数料が大きくて成り立たなかった少額の決済が可能になります。

例えば、デリバティブやオプションは、リスクをヘッジするための金融商品ですが、どちらかを予測する賭けの面もあります。このような賭けを少額で広く募集すれば、大勢の人の予測結果を売るビジネスができます。またマイクロペイメントは少額の寄付や支援が容易で、例えば太陽光発電で発電した少量の電気を個人が最も高く買ってくれるところに売ることもできます。デジタルグリッド(株)は自社でコントローラを開発し太陽光発電の電気を自由に電力網へ供給することを可能にしました。ローカルな地域間、あるいは建物同士で再生電力を売買でき、取引記録にはブロックチェーン技術を活用しています。

4-2　最後に　～誰が金融のグーグルになるのか？～

様々な電子マネー(仮想通貨)ができると個人のお金を管理するシステムが必要になってきます。このシステムは、個人の資産、収入、支出など貴重な情報を手にします。グーグルはインターネットの入り口の検索エンジンを制覇したことで個人の思考、好みなどの重要な情報を手に入れました。そして検索エンジンに広告を売ることで莫大な富を手にしました。同様に、個人のお金の情報を支配すれば「お金のグーグル」が生まれ、もっと大きな富を手にするかもしれません。

5. 温故知新「世界を変えた地味な技術『標準化と互換性』」

「電球が切れたので新しいものと交換できる」当たり前のことが 250 年前は夢物語だと聞いたら、あなたはどう思うでしょうか。これは「標準化」と「互換性」の賜物です。

図 4　火打ち式銃の発火装置
（Wikipedia より）

18 世紀、当時の最先端機器は銃でした。製造は主にやすり掛けでした。部品同士に互換性はなく、戦場で部品が 1 つ壊れればもう使えません。銃が火縄（マッチロック式）から火打ち式（フリントロック式）に変わった 1760 年代、フランスのオノレ・ブランは、戦場で発火装置が壊れても交換できるように発火装置に“互換性”を持たせることを考えました。試行錯誤の末、ブランは互換性を実現しましたが、職人の強い反対に遭い、互換性を持った製造方法は普及しませんでした。

1785 年、(後のアメリカ大統領となる)トーマス・ジェファーソンはパリの銃工場を訪れ、ブランの製造方法を見学しました。イギリスとの独立戦争が迫るアメリカは、銃を大量に必要としていました。ジェファーソンは 1774 年、アメリカのスプリングフィールドに銃を製造する工廠を設立しました。

そこではブランのゲージを活用し、さらにフライス盤、ならい旋盤、水力式プレスなどの工作機械を開発して互換性を持った銃の量産が実現しました。この互換性のある「標準化された製品」を大量生産する「アメリカン・システム」は、ミシンや自転車などの工業製品の製造に用いられ、工業立国アメリカの礎となりました。

1851 年、第 1 回ロンドン万国博でコルトの銃が展示され、互換性を持ったピストルに世界中が驚愕しました。

第二次世界大戦中、標準化と互換性の重要性を認識していたアメリカは、戦闘機や爆撃機の種類、エンジンの種類を極力絞り、標準化された機体を大量生産して数で日本を圧倒しました。対して日本は、エンジンや機体の種類が非常に多く、そのため生産は進まず、前線では部品不足で飛べない機体が増えていきました。

6. 未来戦略ワークショップ「AI で仕事はなくなる？　人工知能と仕事について」

2014 年、オックスフォード大学のオズボーン氏は、今後 20 年間で 47%の仕事が 1950 年代に人工知能に取って替わると発表しました。本当に仕事はなくなってしまうのか？人工知能にできること、できないことは何か？人工知能と仕事について考えます。未来戦略ワークショップは前日までに連絡すればどなたでも参加できます。（連絡先は本頁下部にあります）

7. 冊子「中小企業・小規模企業のための個別製造原価の手引書」

「この受注はいくらでできるか」を把握するには自社のアワーレートを知る必要があります。ところが製造業はアワーレートに関する費用項目が多く、どの費用をどのように分配するのか、多くの企業が悩んでいます。弊社では中小企業がアワーレートを簡単に計算する方法をセミナー等で説明していて、この度「わかりやすいテキストが欲しい」という要望に応えて冊子を制作しました。会計の専門的な用語を使わず、とても分かりやすい内容です。（税別 2,000 円）　下記の弊社 HP からご購入いただけます。

8. 編集後記

年とともに基礎代謝は低下し、仕事中についお菓子をつまんでいれば太るのは避けられません。無理せず少しずつ摂取カロリーを落としていこうと思います。

感想がありましたらぜひお聞かせください。また本ニュースレターが不要な方はお手数ですが、下記通信欄に、お名前又は社名と「不要」とご記入の上、FAX して頂くか、メールにて不要とお知らせください。

株式会社アイリンク　代表取締役　照井清一
〒444-0835　愛知県岡崎市城南町２丁目１３－４
TEL 0564-55-5661 / 0564-77-6810　FAX 0564-77-8203
URL http://ilink-corp.co.jp　メルマガ http://ilink-orp.co.jp/malmag.html
E-mail terui@ilink-corp.co.jp　https://www.facebook.com/se.terui
【通信欄】