報道各位

2019 年 9 月 20 日
株式会社インプレスR&D
https://nextpublishing.jp/

ブロックチェーン最新用語をこの1冊に！

『基本用語から最新規格までをわかりやすく～ブロックチェーン用語集』発行

技術の泉シリーズ、9月の新刊

インプレスグループで電子出版事業を手がける株式会社インプレス R&D は、『基本用語から最新規格までをわかりやすく～ブロックチェーン用語集』(著者:峯 荒夢)を発行いたします。

最新の知見を発信する『技術の泉シリーズ』は、「技術書典」をはじめとした各種即売会や、勉強会・LT 会などで頒布された技術同人誌を底本とした商業書籍を刊行し、技術同人誌の普及と発展に貢献することを目指します。

『基本用語から最新規格までをわかりやすく～ブロックチェーン用語集』
https://nextpublishing.jp/isbn/9784844378099

著者:峯 荒夢
小売希望価格:電子書籍版 2400 円(税別)／印刷書籍版 2600 円(税別)
電子書籍版フォーマット:EPUB3／Kindle Format8
印刷書籍版仕様:B5 判／カラー／本文 168 ページ
ISBN:978-4- 8443-7809-9
発行:インプレス R&D

＜＜発行主旨・内容紹介＞＞

本書は株式会社ガイアックスのブロックチェーンの情報サイト「Blockachain Biz」編集部によるブロックチェーンの用語集です。

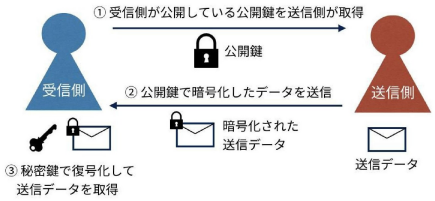
基本用語から技術トレンドまでを詳細に解説しています。仮想通貨やスマートコントラクトなど様々な場面で活用が進むブロックチェーンの用語を丁寧に解説しています。

(本書は、次世代出版メソッド「NextPublishing」を使用し、出版されています。)

基本的な用語から専門用語まで、図解を用いながら解説

信傍受による、鍵の流出も防ぐことができます。

公開鍵暗号方式のイメージ



署名

また、公開鍵暗号の応用に「署名」という仕組みがあります。これは公開鍵を用いた本人確認のシステムです。

公開鍵はその名の通り「公開」されているものなので、「私の公開鍵は○○です」と言っている人を無条件に信用することはできません。

そこで秘密鍵と公開鍵を入れ替えて使うことができる、という公開鍵暗号の性質を利用して本人確認を行います。流れは以下の通りです。

1．秘密鍵を持っている人が、ある文字列を秘密鍵で暗号化する
2．公開鍵を受け取った人は、暗号化された文字列を復号化して元の文字列と比較する
3．一致した場合、この公開鍵で正しく解読できる文章を作れるのは秘密鍵を持っている本人だけなので、本人確認ができる

秘密鍵・公開鍵の活用事例

1．ブロックチェーン

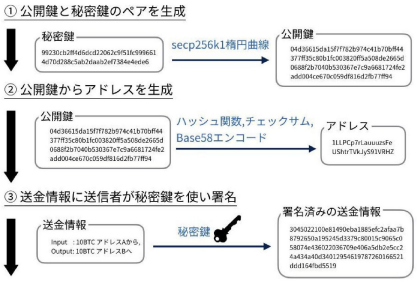
ブロックチェーンにおける活用事例を、ビットコインを例に紹介しましょう。公開鍵暗号の主な

使用方法は「データの暗号化」と「署名」の二つがあると説明しましたが、ビットコインにおいては主に「署名」の方を使っています。

ビットコインの取引では、公開鍵から生成されるビットコインアドレスから支払いをする時に、そのアドレスの秘密鍵を持っているビットコイン所有者が秘密鍵を用いて署名します。他の人は、その署名と公開鍵を使ってその署名が秘密鍵を持った人が行ったこと、署名された後に本文が改ざんされていないことを確認することが出来ます。具体的な送金の流れは以下のようになります。

1．公開鍵と秘密鍵のペアを生成する（ビットコインでは秘密鍵から公開鍵への変換はsecp256k1という楕円曲線を利用します。）
2．公開鍵からハッシュを2回とり、チェックサムを加えてBase58フォーマットしたアドレス（口座番号）を生成する
3．送信するビットコイン、アドレス等の情報を含んだ送金情報（取引データ）に、アドレス所有者である送信者が秘密鍵を使い署名する
4．P2Pネットワークに送金情報である取引データをブロードキャスト する
5．取引内に含まれる公開鍵と署名済みの送金情報を照合して取引が正しいことを検証する

ビットコイン取引のイメージ



ブロックチェーンの種類についても紹介

の話をするときは、「パブリック」なのか「プライベート（コンソーシアム）」なのかを切り分けて考える必要があります。

パブリックチェーンの特徴

パブリックチェーンの特徴としては、以下の点が挙げられます。

・中央管理者がいない
・合意形成に参加するノード数に制限がない
・合意形成に関する証明は厳格におこなわれなければならない
・秘密鍵・公開鍵さえ作ってしまえば誰でもすぐに使用できる
・ブロックチェーンの中身は誰でも検証できる

画像：中央銀行から見たブロックチェーン技術の可能性とリスク | 日本銀行（https://www.boj.or.jp/announcements/release_2016/rel161128a.pdf）

	プライベート型	コンソーシアム型	パブリック型
管理者	単独の機関	複数のパートナー	存在せず
ノード参加者	管理者による許可制	管理者による許可制	制限なし
合意形成	厳格ではないことが可能	厳格ではないことが可能	厳格であることが必要（PoW、PoS等）
取引速度	高速	高速	低速
	現在、金融業界が実証実験のターゲットとしているブロックチェーン		Bitcoin、Ethereum等の仮想通貨の基盤に利用されている

パブリックチェーンにおいて取引の承認を担うのは不特定多数のノードやマイナーです。例えばパブリックチェーンに分類されるビットコインにおいて生成されたブロックを承認するのは、ビットコインブロックチェーンに参加している不特定多数のノードやマイナーです。秘密鍵（及びそれに一対一で対応する公開鍵）を作成してしまえば、誰でもノードやマイナー、利用者になることができるのが大きな特徴です。

さらにプルーフ・オブ・ワークやプルーフ・オブ・ステークといった、不特定多数のノードによっておこなわれる取引の合意形成は非常に厳格であり、管理者がいなくとも改ざんがないような仕組みになっています。

また「パブリック」とあるだけに、ブロックチェーンに書かれている内容は誰でも参照することができます。すなわち使用しているデータベースを誰もが見ることができるということです。これは後述しますが、メリットでもありデメリットにもなりえます

パブリックチェーンのメリット

ここまでの定義や特徴を踏まえて、パブリックチェーンのメリットについて説明していきましょ

う。一番のメリットはやはり中央集権的な管理者がいなくても成り立つという点です。ブロックチェーンの生みの親であるビットコインを発明したナカモトサトシは、ビットコインを「管理者がいなくてP2Pネットワークで機能する合意システム」を意図として開発しています。従って、パブリックチェーンに該当するブロックチェーンはすべて、管理者を排除した形で完成されたものであると言えます。

またパブリックチェーンの合意形成に関して、プルーフ・オブ・ワークやプルーフ・オブ・ステークはブロックが生成されるたびにすべてのノードによって取引記録の検証と正当性の担保がおこなわれているので、改ざん不可能性や検閲耐性が強いといった点もメリットとして挙げることができます。さらにこのような合意形成は、ブロックチェーンの中身を誰もが参照できるという公共性からも、その正確性が担保されます。

パブリックチェーンのデメリット

それでは、パブリックチェーンにデメリットはあるのでしょうか。一つは合意形成に時間がかかってしまう点です。管理者なしで多数のノード合意形成により厳格に承認をおこなう場合は、その代償として多くの時間や計算パワーを消費してしまいます。

また、パブリックチェーンは管理者なく運営されているため、仕様の変更に関して多くの時間を要してしまいます。仕様の変更にはコミュニティ全体で議論をして最終的にはブロックチェーン上で多数の合意が取れて初めて仕様変更がおこなえます。これは独裁的にプロトコルが変更されてしまう危険を防ぐためにはメリットですが、素早い仕様の変更を必要とするシステムにおいてはデメリットとなってしまいます。

パブリックであり誰もがデータベースを参照できることもデメリットにもなりえます。基本的にほとんどのブロックチェーンでは秘密鍵・公開鍵、ハッシュ関数などを使うことで各IDが誰のものかわからないようになっていますが、なんらかの方法で鍵の所有者が誰かがわかってしまうと、そのIDによる記録は完全に追跡されてしまうため、プライバシーの観点から問題視されている一面もあります。

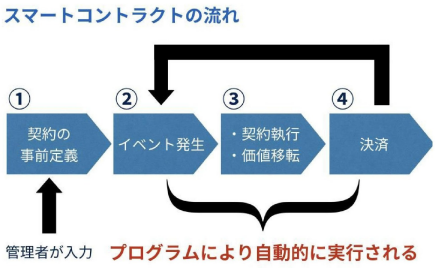
ビットコイン

ここまで何度か言及されていますが、パブリックチェーンを利用したもので一番有名なものがビットコインです。ビットコインのブロックチェーンは、不特定多数のコンピューターが自由に参加できる状況のなかでも、中央の管理者なしにネットワークの合意形成を得ることができるプロトコルを持った通貨「ビットコイン」のために作り上げられたブロックチェーンです。正確にはビットコインが発明され、その仕組みとしてブロックチェーンが使われ、そのブロックチェーンが後にパブリックチェーンと分類されるようになったと言えます。すなわち、ブロックチェーンは元来パブリックチェーンだけしかありませんでした。

ビットコインブロックチェーンにおいて、非中央集権的な運営をおこなっていくというパブリックチェーンの目的が達成されているのは、プルーフ・オブ・ワークや経済的インセンティブ（マイニングによる成功報酬）をうまく組み合わせたからであると言われています。プルーフ・オブ・ワーク

ブロックチェーン利用形態の一つであるスマートコントラクトについてもわかりやすく紹介

スを実現でき、社会に大きな変化をもたらす可能性があると言われています。



ブロックチェーン上でのプログラムとしてスマートコントラクトを実行すると契約が改ざんされないことが保証される上に、人を介すことなく確実に執行できます。ただしプログラムという性質上、曖昧な内容や解釈を要する免責条項などは定義が難しいため、従来の契約をそっくりそのまま代替できるわけではありません。

また、仮にスマートコントラクトにバグや脆弱性があった場合、不正な処理が行われブロックチェーンに誤った情報が書き込まれるリスクも存在します。従って、スマートコントラクトを使用する際は、プラットフォームやサービスの特性に応じて自由度と安全性のバランスを考慮する必要があると言えます。

自動販売機

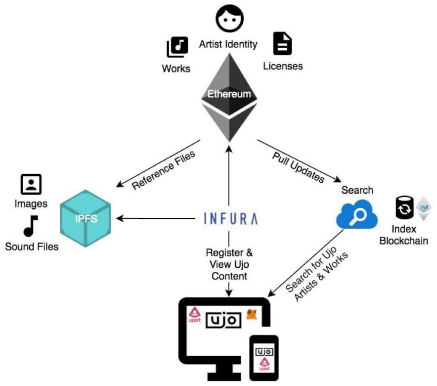
スマートコントラクトの考え自体はビットコインよりも古く、1990年代にNick Szaboという法学者・暗号学者によって最初に提唱されました。Szaboはスマートコントラクトをはじめに導入した例として、自動販売機を挙げています。「利用者が必要な金額を投入する」、「特定の飲料のボタンを押す」の二つの契約条件が満たされた場合にのみ、自動的に「特定の飲料を利用者に提供する」という契約が実行されることになります。このように、コントラクト（契約）とは書面上で作成された契約のみをさすのではなく、取引行動全般をさします。

Ethereumのスマートコントラクト

Ethereumは、ブロックチェーン技術をベースに、特別な中央管理者のいないP2Pシステム上で様々なアプリケーションサービスを実現するための基盤を提供するものです。ビットコインはブロックチェーンの技術を用いて悪意のある参加者が参加する可能性のあるP2Pネットワーク上でお金の取引を正しく動作させる環境でした。一方でEthereumは、取引だけでなくアプリケーション（処理）をこのようなP2Pのネットワーク上で正しくに動作させることを可能にする環境を提供しています。これを実現するための機能として、大きな役割を果たすのがEthereum特有の自由度の高い記述ができるスマートコントラクトです。現在では、様々な業界でその検証がされるようになりました。

そのひとつとして、ujo MUSICが挙げられます。このサービスは、著作権やアーティストへの対価の支払いをより理想の形に近づけるために創られた音楽配信サービスです。

画像：From The Technical Underground To The Future（https://blog.ujomusic.com/building-ujo-1-from-the-technical-underground-to-the-future-a39e825612ef）



これまで、アーティストが楽曲をリリースして、楽曲が買われて、アーティストに収入として入っ

＜＜目次＞＞

4.2 ビザンチン将軍問題
4.3 ファイナリティー
4.4 取引手数料
4.5 採掘難易度(Difficulty)
4.6 ASIC
4.7 半減期
4.8 スマートコントラクト
4.9 Solidity
4.10 UTXO
4.11 Block Height
4.12 Segwit
4.13 ソフトフォーク・ハードフォーク
4.14 User Activated Soft-Fork:UASF
4.15 署名・マルチシグ
4.16 シュノア署名
4.17 ライトニングネットワーク
4.18 ハードウェアウォレット
5. 規格に関する用語
5.1 BIP
5.2 ERC20
5.3 ERC223
5.4 ERC721
6. 機能に関する用語
6.1 エスクロー
6.2 クラウドセール
6.3 Initial Coin Offering(ICO)
6.4 BasS
6.5 ステーブルコイン
6.6 カラードコイン
6.7 プルーフ・オブ・バーン
6.8 Proof of Existence

＜＜著者紹介＞＞

峯 荒夢

シェアリングエコノミーに注力する株式会社ガイアックス開発部のブロックチェーン担当マネージャー。
シェアリングエコノミーを支える最も重要な技術としてブロックチェーンに取り組む。ブロックチェーンで応援を力に変えるサービスの「cheerfor(チアフォー)」や、Facebook 社を中心に開発が進んでいる Libra を使ったプロトタイプの開発を行っている。社外では、ブロックチェーンの国際標準を検討するISO/TC307 国内検討委員にも名を連ねている。

＜＜販売ストア＞＞

電子書籍:

Amazon Kindle ストア、楽天 kobo イーブックストア、Apple Books、紀伊國屋書店 Kinoppy、Google Play Store、honto 電子書籍ストア、Sony Reader Store、BookLive!、BOOK☆WALKER

印刷書籍:

Amazon.co.jp、三省堂書店オンデマンド、honto ネットストア、楽天ブックス

※　各ストアでの販売は準備が整いしだい開始されます。

※　全国の一般書店からもご注文いただけます。

【インプレス R&D】 https://nextpublishing.jp/

株式会社インプレスR&D（本社：東京都千代田区、代表取締役社長：井芹昌信）は、デジタルファーストの次世代型電子出版プラットフォーム「NextPublishing」を運営する企業です。また自らも、NextPublishing を使った「インターネット白書」の出版など IT 関連メディア事業を展開しています。

※NextPublishing は、インプレス R&D が開発した電子出版プラットフォーム（またはメソッド）の名称です。電子書籍と印刷書籍の同時制作、プリント・オンデマンド（POD）による品切れ解消などの伝統的出版の課題を解決しています。これにより、伝統的出版では経済的に困難な多品種少部数の出版を可能にし、優秀な個人や組織が持つ多様な知の流通を目指しています。

【インプレスグループ】 https://www.impressholdings.com/

株式会社インプレスホールディングス（本社：東京都千代田区、代表取締役：唐島夏生、証券コード：東証 1 部 9479）を持株会社とするメディアグループ。「IT」「音楽」「デザイン」「山岳・自然」「旅・鉄道」「学術・理工学」を主要テーマに専門性の高いメデイア&サービスおよびソリューション事業を展開しています。さらに、コンテンツビジネスのプラットフォーム開発・運営も手がけています。

【お問い合わせ先】

株式会社インプレス R&D NextPublishing センター
TEL 03-6837-4820
電子メール: np-info@impress.co.jp