ブロックチェーンと分散台帳管理

杉井靖典 （カレンシーポート代表取締役／CEO）

CurrencyPort

カレンシーポート株式会社
代表取締役　杉井　靖典

代表取締役・CEO 杉井 靖典 - プロフィール

CurrencyPort

カレンシーポート株式会社 - CurrencyPort Limited

- ✓ 経済産業省　ブロックチェーン検討会　委員
  システム評価軸整備検討委員会　委員
- ✓ 日本銀行　決済システムフォーラム　プレゼンター
  FinTechフォーラム　プレゼンター
- ✓ 全国銀行協会　ブロックチェーン活用可能性検討会　委員
  ブロックチェーン研究会　メンバー
- ✓ ブロックチェーン推進協会（BCCC）副代表理事
- ✓ 日本ブロックチェーン協会　正会員
- ✓ FinTech協会　会員

著書
- ✓ いちばんやさしいブロックチェーンの教本
- ✓ 書籍「ブロックチェーンの衝撃」
- ✓ ムック「ブロックチェーン＆ビットコイン入門編」

© 2017CurrencyPort Limited

カレンシーポート株式会社 - 会社概要

カレンシーポート株式会社 - CurrencyPort Limited

【会社情報】

本　社　東京都千代田区大手町1-6-1　大手町ビル4階　FINOLAB内
設　立　2015年10月1日
資本金　9,672万円（資本準備金を含む）
メンバー 17名（契約社員・外部協力者等を含む）
〈2017年1月末現在〉

【事業目的】

1. 電子財布システムの開発
2. 資金決済・送金システムの開発
3. 外国為替両替システムの開発
4. 自動売買アルゴリズムの研究開発
5. 分散合意形成アルゴリズムの研究開発
6. 越境商取引システムの開発
7. 店舗向け販促・販売システムの開発

FINOLAB THE FINTECH CENTER of TOKYO FinTech拠点施設フィノラボ

© 2017CurrencyPort Limited

私たちが関与した実証実験・事例

ブロックチェーン技術の実証実験　～国内企業4社協働による取り組み～

みずほフィナンシャルグループ
シンジケートローン業務に関する要件提示

電通国際情報サービス
業務システム設計、業務シナリオ作成、プロトタイプ開発

カレンシーポート
ブロックチェーン技術、スマートコントラクト開発支援

日本マイクロソフト
Azure BaaS（ブロックチェーンクラウドサービス）の提供

© 2017CurrencyPort Limited

私たちが関与した実証実験・事例

CurrencyPort

低トランザクション市場を想定した、技術的な限界や可能性について評価

証券取引所

JPX JAPAN EXCHANGE GROUP

証券会社

野村證券 NOMURA　MUFG　SBI GROUP SBI証券

他（非公表）、数社

技術協力

NRI 未来創発 Dream up the future.

CurrencyPort

© 2017CurrencyPort Limited

私たちが関与した実証実験・事例

CurrencyPort

実用化を見据えたトークン配布社会実験（富士通・富士通総研さまとの協働）

千葉ロッテマリーンズ
スタジアムにてスタンプラリー

CEATEC2016
FINTECHスタンプラリー

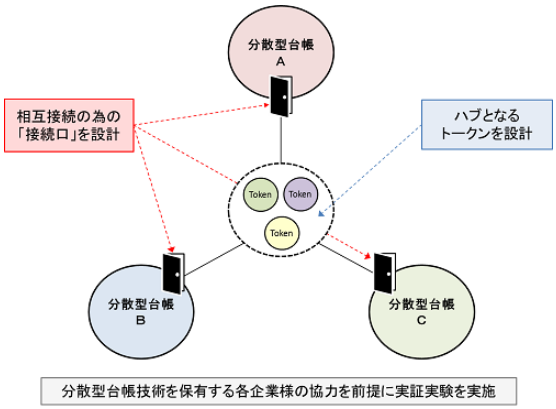
Vリーグオールスター
ファン投票スタンプラリー

© 2017CurrencyPort Limited

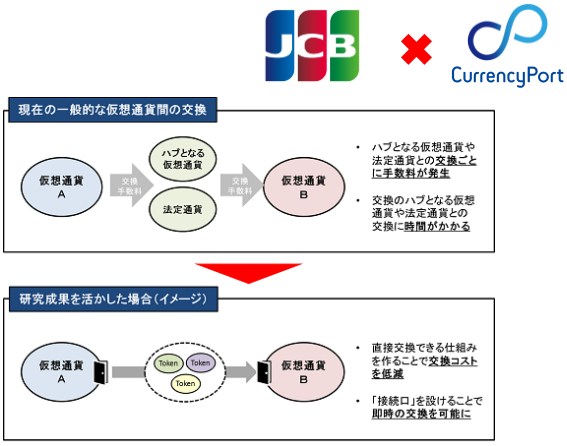
私たちが関与した実証実験・事例

CurrencyPort

JCBと当社共同よる、異種分散台帳間の相互運用性に関する研究開発を開始



分散型台帳技術を保有する各企業様の協力を前提に実証実験を実施



ブロックチェーンコア開発ベンダー10社程度による共同研究コンソーシアム化を想定

CurrencyPort © 2017CurrencyPort Limited 7

CurrencyPort

ブロックチェーンとは何かを知ろう

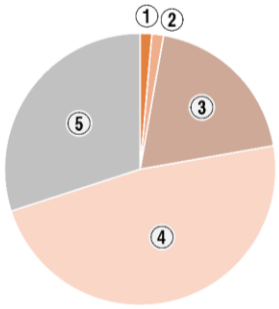
- ✓ ブロックチェーンの起こす社会変革の可能性
- ✓ ブロックチェーンをひとことで説明すると
- ✓ ひとこと説明がなぜそう言えるのかを技術面から深堀り
- ✓ ブロックチェーンになにを記録するか、なにが記録できるか
- ✓ ブロックチェーン上でお金を表現する仕組み

Lesson 01

ブロックチェーンが起こす社会変革の可能性

CurrencyPort

▶ブロックチェーン関連の市場規模予測(国内) 図表01-1



市場規模 67兆円

①	1兆円	価値の流通・ポイント化・プラットフォームのインフラ化	地域通貨 / 電子クーポン / ポイントサービス
②	1兆円	権利証明行為の非中央集権化の実現	土地登記 / 電子カルテ / 出生・婚姻・転居などの登録
③	13兆円	遊休資産ゼロ、高効率シェアリングの実現	デジタルコンテンツ / チケットサービス / C2Cオークション
④	32兆円	オープン・高効率・高信頼なサプライチェーンの実現	小売 / 貴金属管理 / 美術品等真贋認証
⑤	20兆円	プロセス・取引の全自動化・効率化の実現	遺言 / IoT / 電力サービス

出典：経済産業省「ブロックチェーン技術を利用したサービスに関する国内外動向調査」
http://www.meti.go.jp/press/2016/04/20160428003/20160428003.pdf

Lesson 01

ブロックチェーンをひとことで説明すると

CurrencyPort

▶ブロックチェーンを簡単にいうと 図表01-2

「正しい記録しかできない」変更できない、消せない、改ざんできない、壊れても自動修復される、落ちない、「みんなに合意された情報だけが有効と認識される」ネットワーク共有型のデータベース」

▶ **合意形成されたデータのみが記録**される（☞ 分散型合意形成）

Lesson 01

ブロックチェーンを ひとことで説明すると

CurrencyPort

ブロックチェーンとは何かを知ろう

▶ ブロックチェーンを簡単にいうと 図表01-2

「正しい記録しかできない、変更できない、消せない、改ざんできない、壊れても自動修復される、落ちない、みんなに合意された情報だけが有効と認識される、ネットワーク共有型のデータベース」

- **合意形成されたデータのみが記録**される（☞ 分散型合意形成）
- **変更不可能性を有するデータ構造**を持つ（☞ ハッシュチェーン）

Lesson 01

ブロックチェーンを ひとことで説明すると

CurrencyPort

ブロックチェーンとは何かを知ろう

▶ ブロックチェーンを簡単にいうと 図表01-2

「正しい記録しかできない、変更できない、消せない、改ざんできない、壊れても自動修復される、落ちない、みんなに合意された情報だけが有効と認識される、ネットワーク共有型のデータベース」

- **合意形成されたデータのみが記録**される（☞ 分散型合意形成）
- **変更不可能性を有するデータ構造**を持つ（☞ ハッシュチェーン）
- **ネットワーク参加者全員が同じデータを共有**している
  （☞ P2P分散型ネットワーク共有ストレージ）

13

Lesson 01

ブロックチェーンを ひとことで説明すると

CurrencyPort

ブロックチェーンとは何かを知ろう

13

▶ブロックチェーンを簡単にいうと 図表01-2

「正しい記録しかできない、変更できない、消せない、改ざんできない、壊れても自動修復される、落ちない、みんなに合意された情報だけが有効と認識される、ネットワーク共有型のデータベース」

- **合意形成されたデータのみが記録**される（☞ 分散型合意形成）
- **変更不可能性を有するデータ構造**を持つ（☞ ハッシュ連鎖構造）
- **ネットワーク参加者全員が同じデータを共有**している（☞ P2P分散型ネットワーク共有ストレージ）

上記のような機能的特徴を有するデータベース

Lesson 01

ブロックチェーンを ひとことで説明すると

CurrencyPort

ブロックチェーンとは何かを知ろう

- **合意形成されたデータのみが記録**される（☞ 分散型合意形成）
- **変更不可能性を有するデータ構造**を持つ（☞ ハッシュ連鎖構造）
- **ネットワーク参加者全員が同じデータを共有**している（☞ P2P分散型ネットワーク共有ストレージ）

上記のような機能的特徴を有するデータベース

よくある質問に「ブロックチェーンとデータベースの違いはなんですか？」というものがありますが、「ブロックチェーンはデータベースを機能強化する仕組み」なのです。おそらく将来は「ブロックチェーン」とは呼ばれなくなり「データベース」という言葉に集約されていくものと筆者は考えています。

13

Lesson 01

ブロックチェーンを ひとことで説明すると

CurrencyPort

ブロックチェーンとは何かを知ろう

- **合意形成されたデータのみが記録**される（☞ **分散型合意形成**）
- **変更不可能性を有するデータ構造**を持つ（☞ ハッシュ連鎖構造）
- **ネットワーク参加者全員が同じデータを共有**している（☞ P2P分散型ネットワーク共有ストレージ）

上記のような機能的特徴を有するデータベース

よくある質問に「ブロックチェーンとデータベースの違いはなんですか？」というものがありますが、「ブロックチェーンはデータベースを機能強化する仕組み」なのです。おそらく将来は「ブロックチェーン」とは呼ばれなくなり「データベース」という言葉に集約されていくものと筆者は考えています。

13

Lesson 30

合意形成の基本は多数決

CurrencyPort

ブロックチェーンとは何かを知ろう

▶ リーダーを要する合意形成 図表30-2

例）Ⓐ or Ⓑ 2者択一の場合

11

Lesson 30

リーダーを要する合意形成

CurrencyPort

ブロックチェーンとは何かを知ろう

例）Ⓐ or Ⓑ 2者択一の場合

多数決型の合意形成をとる場合、必ず参加者の母数がわかっている必要があります。

プライベート環境なら必ずネットワークの参加者の母数がわかりますので、多数決型の合意も可能ですが、

パブリック環境で、ネットワークの参加者の母数が不定の環境では、どのように合意形成をしたらよいのでしょうか？

11-2

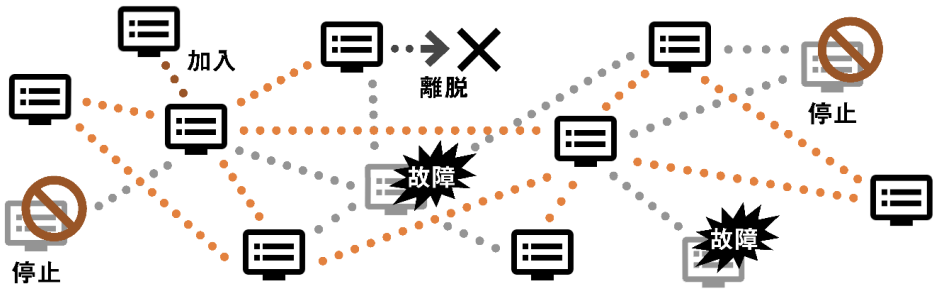
Lesson 30

リーダーが不要の合意形成

CurrencyPort

ブロックチェーンとは何かを知ろう

▶パブリックチェーンでは多数決を採用できない 図表30-1



加入・離脱・故障・休止がいつどこで起こるかわからないため、多数決に必要なノード総数が把握できない

母集団の人数が決まらない分散システムにおける合意形成は、単純に多数決で決めることができません。

11-1

Lesson 30

リーダーが不要の合意形成

CurrencyPort

ブロックチェーンとは何かを知ろう

11

▶ リーダー不要の合意形成 図表30-3

ブロックチェーンの発明以前

☑正しい可能性がある複数の選択肢は、どちらが正しいかを判断せずに分岐させる

☑どの分岐を選択するかは、**利用者に委ねる**

Ⓐ の選択

選んだけど正しい選択なのか半信半疑

Ⓑの選択

迷う、選べない

合意システムとして成立しない

例）Ⓐ or Ⓑ 2者択一の場合

ブロックチェーンの合意原理

☑正しい可能性がある複数の選択肢は、どちらが正しいかを判断せずに分岐させる

☑どの分岐を選択するかは、**利用者に委ねる**

経済的インセンティブ

単純なルール

Ⓐ の選択

正の選択をした者が、経済的利益の行使権を得る

Ⓑの選択

誤の選択をした者は、経済的利益の行使権を得られない（無駄）

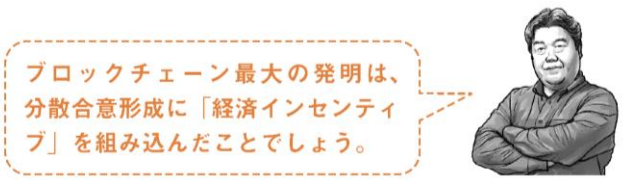
Lesson 30

リーダーが不要の合意形成

CurrencyPort

ブロックチェーンとは何かを知ろう

11



経済インセンティブ

☞ **コイン（仮想通貨）**

単純なルール

☞ **マイニング（合意形成）**

例）Ⓐ or Ⓑ 2者択一の場合

ブロックチェーンの合意原理

☑正しい可能性がある複数の選択肢は、どちらが正しいかを判断せずに分岐させる

☑どの分岐を選択するかは、**利用者に委ねる**

経済的インセンティブ

単純なルール

Ⓐ の選択

正の選択をした者が、経済的利益の行使権を得る

Ⓑの選択

誤の選択をした者は、経済的利益の行使権を得られない（無駄）

Lesson 01

ブロックチェーンを ひとことで説明すると

CurrencyPort

ブロックチェーンとは何かを知ろう

- **合意形成されたデータのみが記録**される（☞ **分散型合意形成**）
- **変更不可能性を有するデータ構造**を持つ（☞ ハッシュ連鎖構造）
- **ネットワーク参加者全員が同じデータを共有**している（☞ P2P分散型ネットワーク共有ストレージ）

上記のような機能的特徴を有するデータベース

よくある質問に「ブロックチェーンとデータベースの違いはなんですか？」というものがありますが、「ブロックチェーンはデータベースを機能強化する仕組み」なのです。おそらく将来は「ブロックチェーン」とは呼ばれなくなり「データベース」という言葉に集約されていくものと筆者は考えています。

13

Lesson 01

ブロックチェーンを ひとことで説明すると

CurrencyPort

ブロックチェーンとは何かを知ろう

- 合意形成されたデータのみが記録される（☞ 分散型合意形成）
- 変更不可能性を有するデータ構造を持つ（☞ ハッシュ連鎖構造）
- ネットワーク参加者全員が同じデータを共有している（☞ P2P分散型ネットワーク共有ストレージ）

上記のような機能的特徴を有するデータベース

よくある質問に「ブロックチェーンとデータベースの違いはなんですか？」というものがありますが、「ブロックチェーンはデータベースを機能強化する仕組み」なのです。おそらく将来は「ブロックチェーン」とは呼ばれなくなり「データベース」という言葉に集約されていくものと筆者は考えています。

13

Lesson 19

デジタル文書の改ざんを検出する一方向ハッシュ関数

CurrencyPort

ブロックチェーンとは何かを知ろう

▶通常の関数の場合 図表19-1

例）任意の文字列を複数与えたときに、それを単純に連結して返す関数「concat」の場合、どんな値が出力されるかは、当然想像ができる

concat("Block","Chain") →	"BlockChain"
concat("Clock","Chain") →	"ClockChain"
concat("Flock","Chain") →	"FlockChain"

▶hash関数の場合 図表19-2

例）任意の文字列を複数与えたときに、そのハッシュ値を返す関数「hash」場合、1文字ずつしか変更していないのに、まったく異なる数値が出力される

1ビットでも違うデータなら全く異なる値を出力します

hash("BlockChain") →	"3a6fed5fc11392b3ee9f81caf017b48640d7458766a8eb0382899a605b41f2b9"
hash("ClockChain") →	"90f1792f8a13bae8ed69628e48f2ad80948a5d0d99a683078cd17aef0cc41d63"
hash("FlockChain") →	"1fe91df24237be3e0650b2a22e1dc270a1b9149a7538b998ad4b913bff21948c"

77

テキストだけではなくファイル等、すべてのデジタルデータに適用可能

Lesson 20

一方向ハッシュ関数の耐衝突性

CurrencyPort

ブロックチェーンとは何かを知ろう

▶ハッシュ値の衝突とは 図表20-2

もとの値の長さに関わらず一定の桁数が返ってくるため、衝突する可能性がある

サハラ砂漠の砂粒の数
4.4 × 10 ^ 23

海の水分子の数
4.5 × 10 ^ 46

79

SHA2-256ハッシュ衝突確率＝5.7896 × 10 ^ 76 分の

※誕生日攻撃折込み済み

Lesson 44

ブロックチェーンの耐改ざん性を担保する仕組み

CurrencyPort

▶トランザクションの構造の概略図 図表44-1

- ▶バージョン情報
- ▶入力(Input)部
  - 入力の数
  - UTXOの含まれるトランザクションID(ハッシュ値)
  - UTXOのインデックス(何番目の出力を使うか？)
  - 送信者の電子署名と公開鍵
- ▶出力(Output)部
  - 出力の数
  - 送金する金額
  - 送金先のウォレットアドレス
  - お釣りの金額
  - お釣りの返却先のウォレットアドレス

トランザクションファイルの
ハッシュ値

＝トランザクションID

例）ビットコインの取引データ
＝トランザクションの中身

Lesson 44

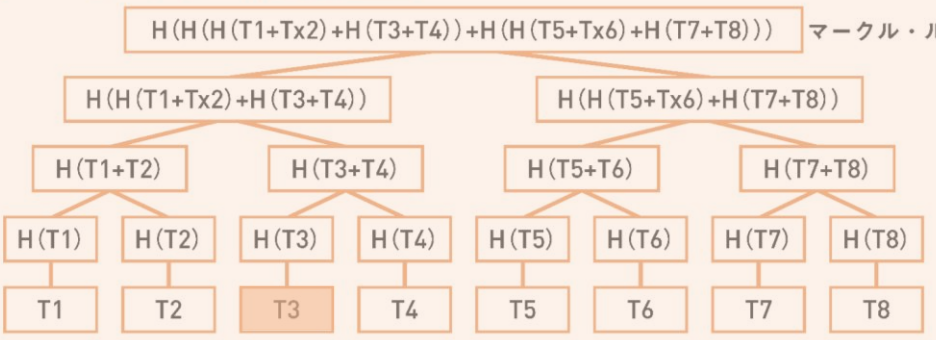
ブロックチェーンの耐改ざん性を担保する仕組み

CurrencyPort

ブロックチェーンとは何かを知ろう
15

▶マークルツリー構造 図表44-2

Tn …トランザクション
H …SHA2-256 ハッシュ



下から2つごとのトランザクション（T1とT2、T3とT4など）それぞれをハッシュ関数に掛けていくと、一番上の根元の値は、このブロックに含まれるすべてのトランザクションに依存性を持つ

実際のブロックチェーンのブロックには、数百以上のトランザクションが含まれる

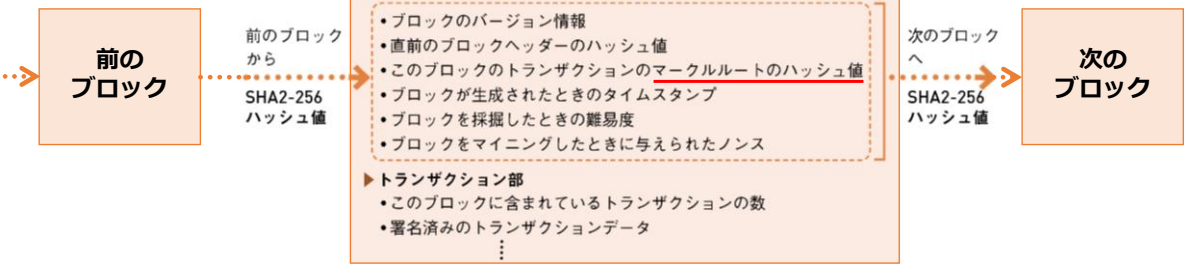
Lesson 44

ブロックチェーンの耐改ざん性を担保する仕組み

CurrencyPort

ブロックチェーンとは何かを知ろう

▶ブロック構造の概略図 図表44-3



ブロックチェーンの改ざん不可能性は、すべてのトランザクションならびにブロックに依存性を持たせたハッシュの連鎖構造を作ることで実現されています。

16

Lesson 01

ブロックチェーンをひとことで説明すると

CurrencyPort

ブロックチェーンとは何かを知ろう

- **合意形成されたデータのみが記録**される（☞ **分散型合意形成**）
- **変更不可能性を有するデータ構造**を持つ（☞ **ハッシュ連鎖構造**）
- **ネットワーク参加者全員が同じデータを共有**している（☞ **P2P分散型ネットワーク共有ストレージ**）

上記のような機能的特徴を有するデータベース

よくある質問に「ブロックチェーンとデータベースの違いはなんですか？」というものがありますが、「ブロックチェーンはデータベースを機能強化する仕組み」なのです。おそらく将来は「ブロックチェーン」とは呼ばれなくなり「データベース」という言葉に集約されていくものと筆者は考えています。

13

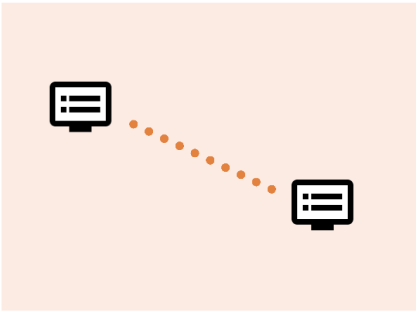
Lesson 25

P2P方式の分散ネットワークとは

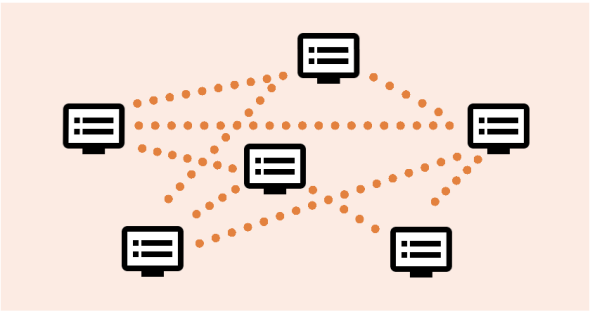
CurrencyPort

▶ P2P接続とP2Pネットワーク 図表25-1

P2P方式（1対1の接続）



P2P方式の接続がたくさん集まったネットワーク



1対1接続のノードが多く集まった状態をP2Pネットワークという

98

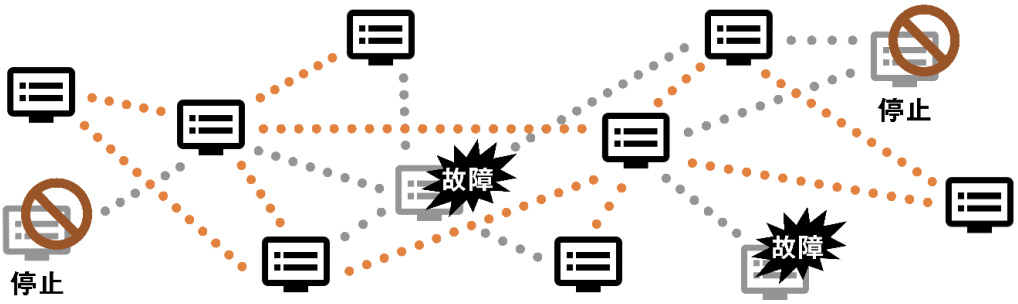
中心がないネットワーク

Lesson 26

P2Pの安全性と信頼性

CurrencyPort

▶ 安全なネットワーク 図表26-1



10

多少の故障ノードや停止ノードがあっても動き続けるネットワーク

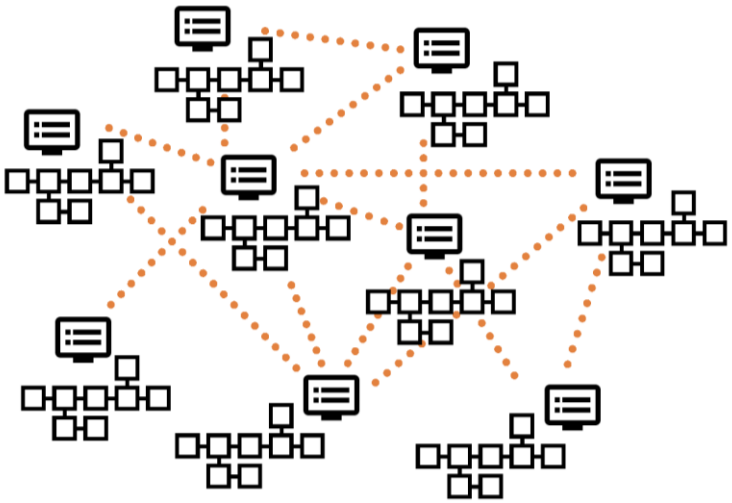
ゼロダウンタイム

Lesson 25

ブロックチェーンは、P2P分散ネットワーク上の分散システム

CurrencyPort

▶P2P分散ネットワーク上の各ノードにブロックチェーンは保持される 図表25-2



それぞれのノードが同じブロックチェーンを持つ

ブロックチェーンに保持されるデータは、全ノードが保有しているため、冗長性が高いのが特徴ですが、これは利点でもある反面、長い目で見ると欠点にもなりかねません。

Lesson 01

ブロックチェーンをひとことで説明すると

CurrencyPort

- **合意形成されたデータのみが記録**される（☞ **分散型合意形成**）
- **変更不可能性を有するデータ構造**を持つ（☞ **ハッシュ連鎖構造**）
- **ネットワーク参加者全員が同じデータを共有**している（☞ **P2P分散型ネットワーク共有ストレージ**）

上記のような機能的特徴を有するデータベース

よくある質問に「ブロックチェーンとデータベースの違いはなんですか？」というものがありますが、「ブロックチェーンはデータベースを機能強化する仕組み」なのです。おそらく将来は「ブロックチェーン」とは呼ばれなくなり「データベース」という言葉に集約されていくものと筆者は考えています。

Lesson 02

ブロックチェーンの着目すべき機能的特徴

CurrencyPort

「ブロックチェーンとデータベースはなにが違うのですか？」という質問に対して、ここで改めて回答しておきましょう。基本的にブロックチェーンは、情報の記録媒体という意味では、データベースの一種であることには間違いありません。ただし、従来のデータベースと決定的に異なることは、以下のような機能を「『すべて』備えている」点です。

▶ ブロックチェーンの機能的特徴 図表02-5

- データは複数の参加者に確認されルールに従った書式のものだけが記録されること
- 参加者全員によって合意されたデータだけが有効となる約束で運用されていること
- 耐改ざん性のあるデータ構造（ハッシュチェーン構造）を持っていること
- 改ざんしようとすると即時検出され、そのデータが破損していると認識されること
- 破損データは正常なデータを持つほかの参加者から取り寄せて自動復旧できること
- 一度書き込まれたデータは変更も削除も誰にもいっさいできないこと
- システム全体を止めることは誰にも不可能なこと

Lesson 03

デジタルでお金をどうやって表現するのか

CurrencyPort

▶ お金としての実用上の機能 図表03-3

従来のリレーショナルデータベースを用いてお金の移動を表現する方法

残高データ（送信前の状態）

利用者	残高
Aさん	12,500
Bさん	9,800
Cさん	6,700
Dさん	23,600

−2,000
+2,000

残高データ（送信後の状態）

利用者	残高
Aさん	10,500
Bさん	9,800
Cさん	8,700
Dさん	23,600

履歴データ

日時	対象	操作	金額
10：32	Bさん	出金	1,600
10：32	Dさん	入金	1,600
10：38	Aさん	出金	2,000
10：38	Cさん	入金	2,000

AさんがCさんに2,000円送金すると、利用者ごとの残高データのうち、AさんとCさんのデータの状態は送金前と送金後で変化する。そして履歴として誰がいついくら入出金したかが残る

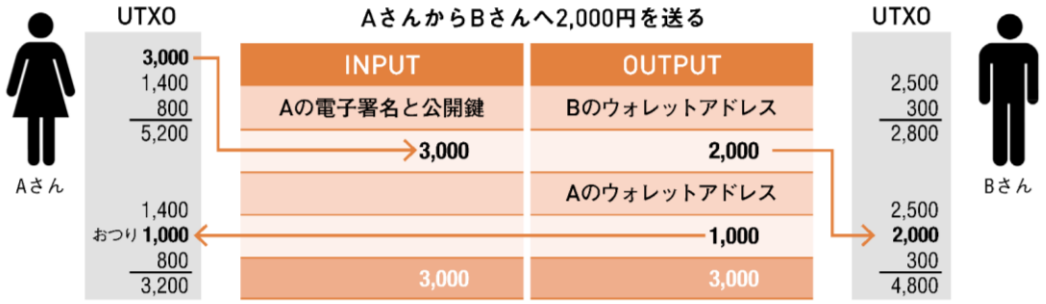
Lesson 40

ブロックチェーンとは何かを知ろう

帳簿の連続性を保証する仕組み
未使用残高「UTXO」Unspent Transaction Output

CurrencyPort

▶ UTXOの概念図 図表40-1



14

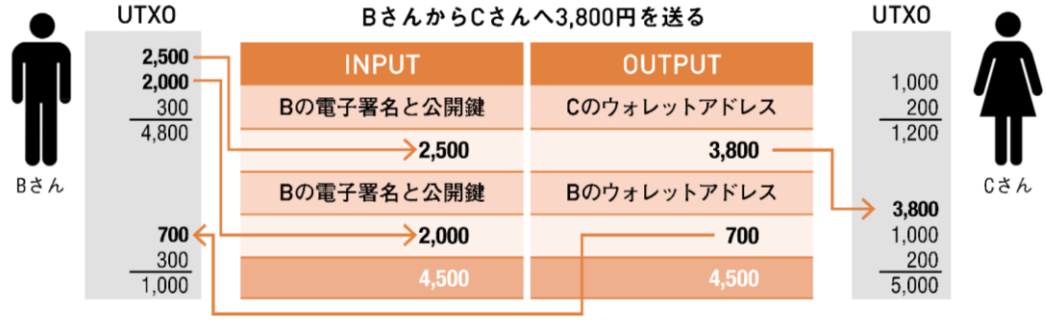
ブロックチェーンが「台帳技術」といわれるゆえん

Lesson 40

ブロックチェーンとは何かを知ろう

帳簿の連続性を保証する仕組み
未使用残高「UTXO」Unspent Transaction Output

CurrencyPort



送金するときは、送金額を満たすUTXOから送金する。足りない場合は、複数のUTXOをInputに配置する。
InputとOutputの合計は常に同じ額となる

14

ブロックチェーンが「台帳技術」といわれるゆえん

Lesson 44

トランザクションの構造の概略

CurrencyPort

ブロックチェーンとは何かを知ろう

15

▶トランザクションの構造の概略図 図表44-1

- ▶バージョン情報
- ▶入力(Input)部
  - 入力の数
  - UTXOの含まれるトランザクションID(ハッシュ値)
  - UTXOのインデックス(何番目の出力を使うか？)
  - 送信者の電子署名と公開鍵
- ▶出力(Output)部
  - 出力の数
  - 送金する金額
  - 送金先のウォレットアドレス
  - お釣りの金額
  - お釣りの返却先のウォレットアドレス

→ ブロックチェーンに記録

未使用残高の中から送金に充分な金額を入力

予算≧入力≧出力

次に使える人を限定
(送金先のウォレットアドレスに対応する秘密鍵を持っている人)

例）ビットコインの取引データ
＝トランザクションの中身

Lesson 21

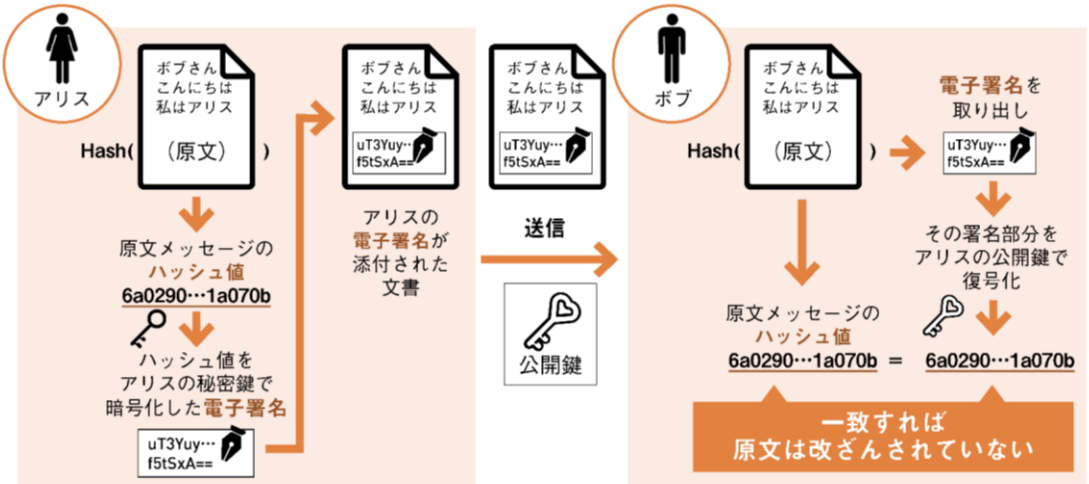
トランザクションの作成者を証明する方法「電子署名」

CurrencyPort

ビットコインの世界を学ぼう

80

▶電子署名検証の基本的な仕組み 図表21-1



アリスの電子署名をアリスの公開鍵で復号化し、原文のハッシュ値と照合する

Lesson 21

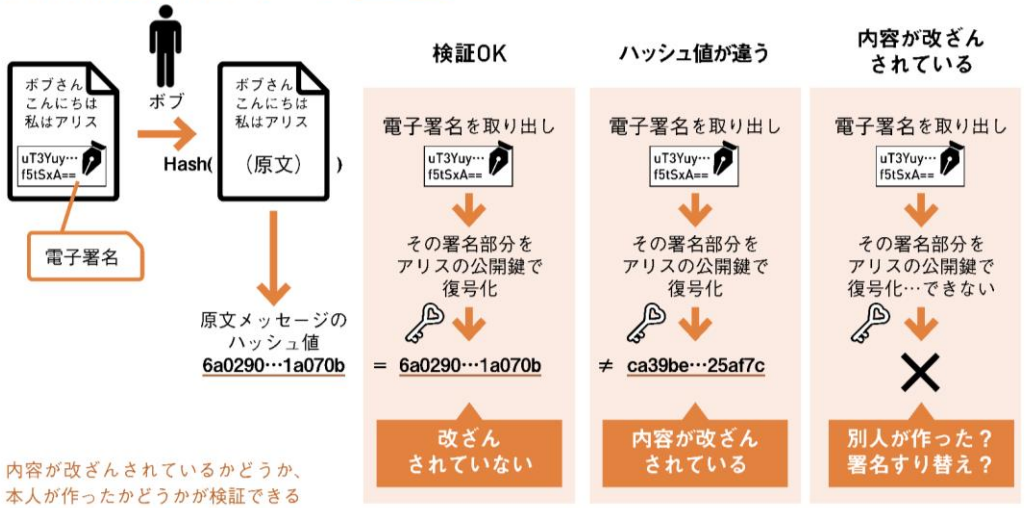
電子署名があればトランザクションの正当性が証明できる

CurrencyPort

ビットコインの世界を学ぼう

80

▶ 電子署名の検証パターン 図表21-2



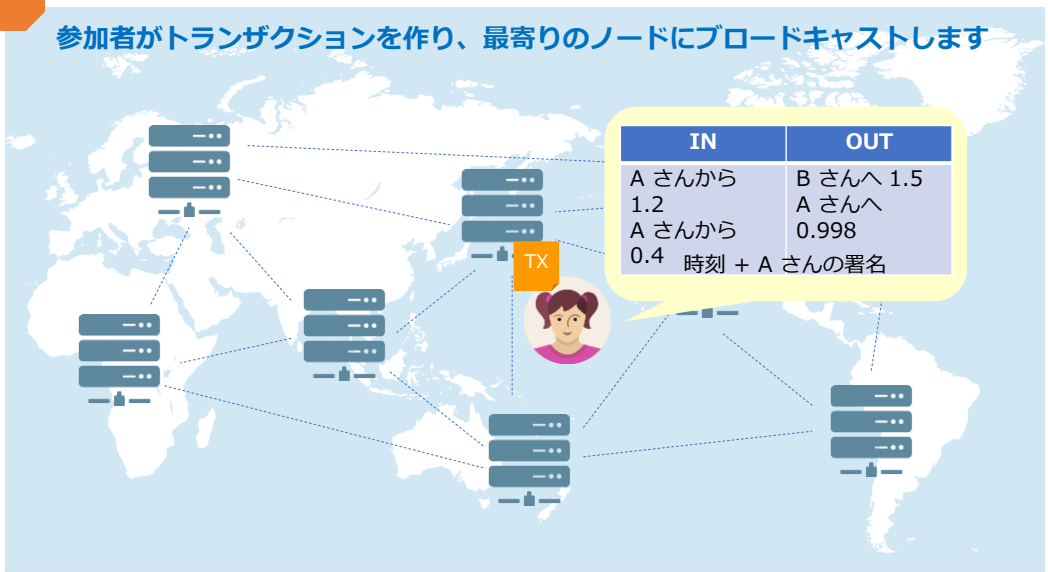
内容が改ざんされているかどうか、
本人が作ったかどうかが検証できる

Lesson

ブロックチェーン (Bitcoin) の仕組み

CurrencyPort

ブロックチェーンとは何かを知ろう



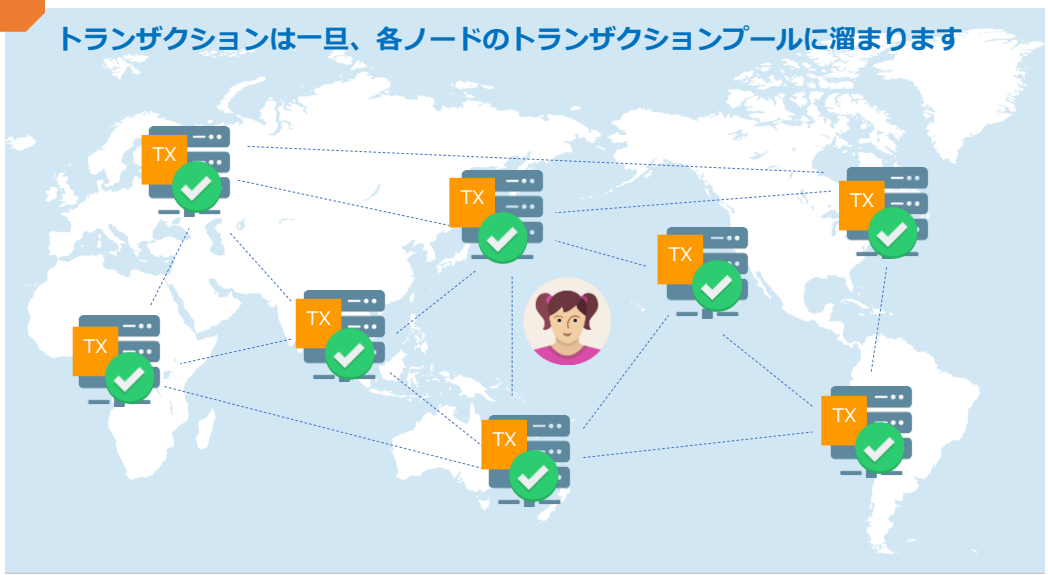
© 2015-2017 CurrencyPort Limited

Lesson

ブロックチェーンとは何かを知ろう

ブロックチェーン (Bitcoin) の仕組み

CurrencyPort



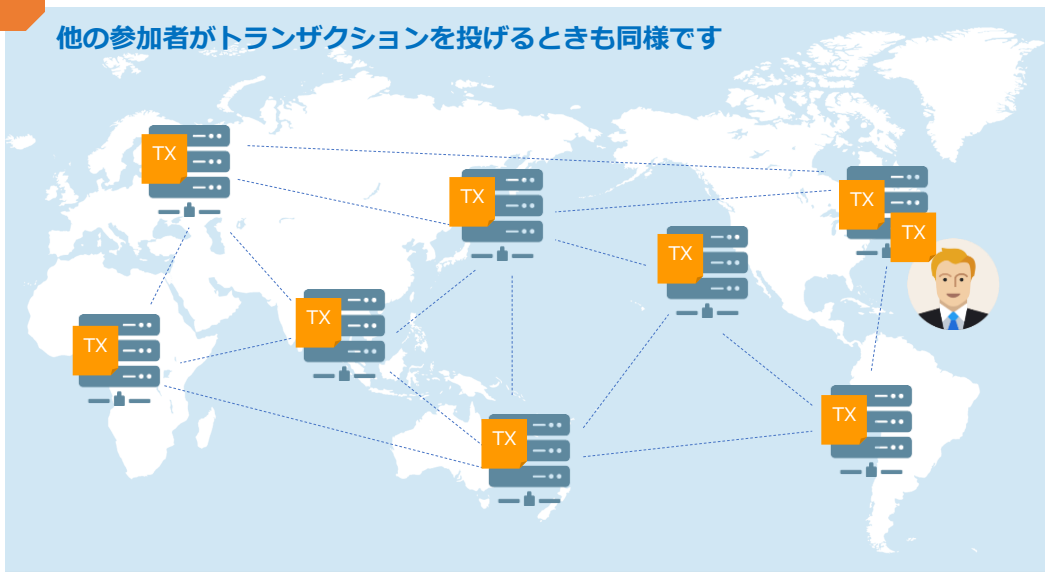
CurrencyPort
© 2015-2017 CurrencyPort Limited

Lesson

ブロックチェーンとは何かを知ろう

ブロックチェーン (Bitcoin) の仕組み

CurrencyPort



CurrencyPort
© 2015-2017 CurrencyPort Limited

Lesson

ブロックチェーンとは何かを知ろう

ブロックチェーン (Bitcoin) の仕組み

CurrencyPort

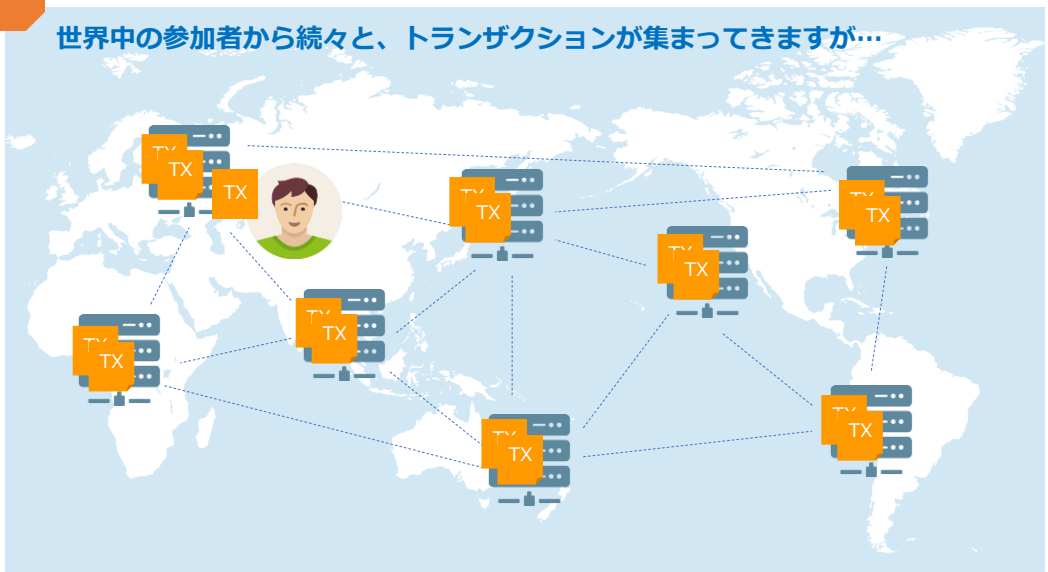
© 2015-2017 CurrencyPort Limited

Lesson

ブロックチェーンとは何かを知ろう

ブロックチェーン (Bitcoin) の仕組み

CurrencyPort



© 2015-2017 CurrencyPort Limited

Lesson

ブロックチェーンとは何かを知ろう

ブロックチェーン (Bitcoin) の仕組み

CurrencyPort

© 2015-2017 CurrencyPort Limited

Lesson

ブロックチェーンとは何かを知ろう

ブロックチェーンのしくみ

CurrencyPort

© 2015-2017 CurrencyPort Limited

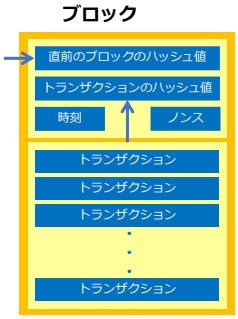
Lesson

ブロックチェーンとは何かを知ろう

ブロックチェーン (Bitcoin) の仕組み

CurrencyPort

不特定多数のネットワーク参加者間で行う合意形成（トランザクション承認）



ハッシュ値

- ✓ １バイトでも情報が異なると、まったく違う値を返す性質を持つ
- ✓ 得られた値から元のデータを復元できない（**一方向関数**）

例）

This is a pen.
5a3737e180810ef8afea4b1125190febcb86980a2b3e8a99140e42b1ccf18efd

This is a pan.
b821aef5d6ef2d6f43064a026cdd891502a0affc8d07382d1e6ac93ee39500a0

ノンス

- ✓ 使い捨ての適当な数値

ノンスの発見競争
マイニング

例）

This is a pen. 49
00be0d7327f1cc784769b40f39419554ca8d7812f6dfb6302a5581f97e0117a8

ハッシュ値を取ったとき
先頭に0が並ぶ数値は？

© 2015-2017 CurrencyPort Limited

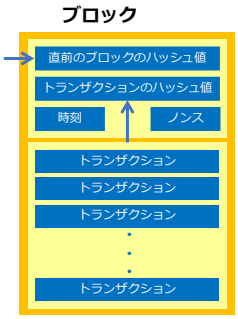
Lesson

ブロックチェーンとは何かを知ろう

ブロックチェーン (Bitcoin) の仕組み

CurrencyPort

不特定多数のネットワーク参加者間で行う合意形成（トランザクション承認）



ノンス

- ✓ 使い捨ての適当な数値

ノンスの発見競争
マイニング

例）
This is a pen. 49
00be0d7327f1cc784769b40f39419554ca8d7812f6dfb6302a5581f97e0117a8

0が2つ並ぶくらいなら、人の手でも探せますが…
0がたくさん並ぶと、コンピュータでもかなり大変。

例えば、2017年9月現在、ビットコインでは
0が18～19個程度並ぶハッシュを探さないといけない。

エネルギー効率が
とても悪い…

Proof of Work（PoW）

© 2015-2017 CurrencyPort Limited

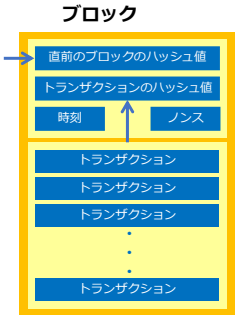
Lesson

ブロックチェーンとは何かを知ろう

ブロックチェーン (Bitcoin) の仕組み

CurrencyPort

分散合意形成（BFT:ビザンチンフォールトトレランス）アルゴリズム



Proof of Work（PoW）

- ✓ ビットコイン
- ✓ Ethereum（まもなくPoSに移行予定）

Proof of Stake（PoS）

変形・派生実装が多数

例）**Proof of Importance**

- ✓ NEM / Mijin

その他のBFT

- ✓ Ethereum派生系 Tendermint
- ✓ Hyperledger fabric, Miyabi

© 2015-2017 CurrencyPort Limited

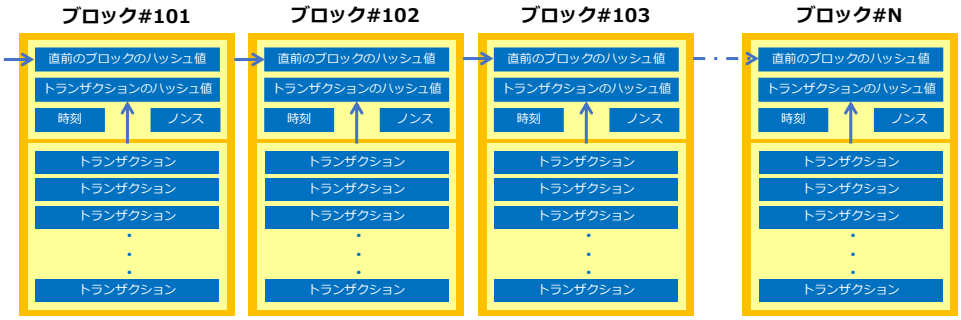
Lesson

ブロックチェーンとは何かを知ろう

ブロックチェーン (Bitcoin) の仕組み

CurrencyPort

合意された、唯一正当な取引記録データをネットワーク参加者全員で共有



全ブロックの整合性が保たれていれば、
全データの正当性が保証される
（ハッシュ値を比較すれば、誰でも検証可能）

© 2015-2017 CurrencyPort Limited

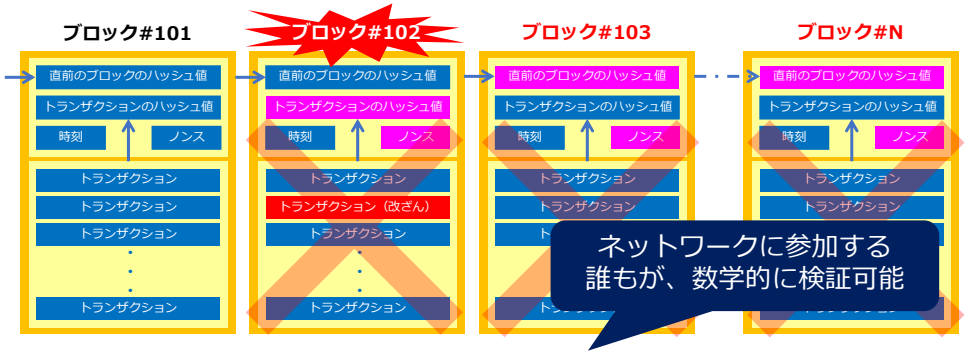
Lesson

ブロックチェーンとは何かを知ろう

ブロックチェーン (Bitcoin) の仕組み

CurrencyPort

途中のデータを改ざんすると、後継のブロックチェーンに矛盾が生じる



後継ブロックのハッシュ値に不整合が見つかれば
途中のトランザクションに改ざんがあったことが検出ができる

© 2015-2017 CurrencyPort Limited

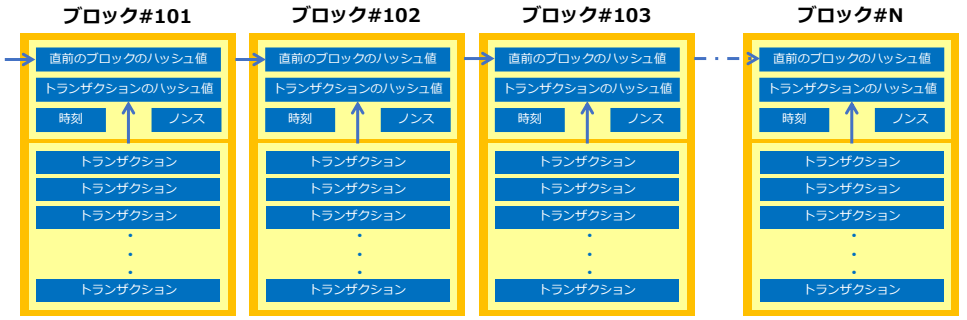
Lesson

ブロックチェーンとは何かを知ろう

ブロックチェーン (Bitcoin) の仕組み

CurrencyPort

データが破損しても、近隣のノードから正常なデータを取寄せて自動回復



不整合状態まま維持することはできない

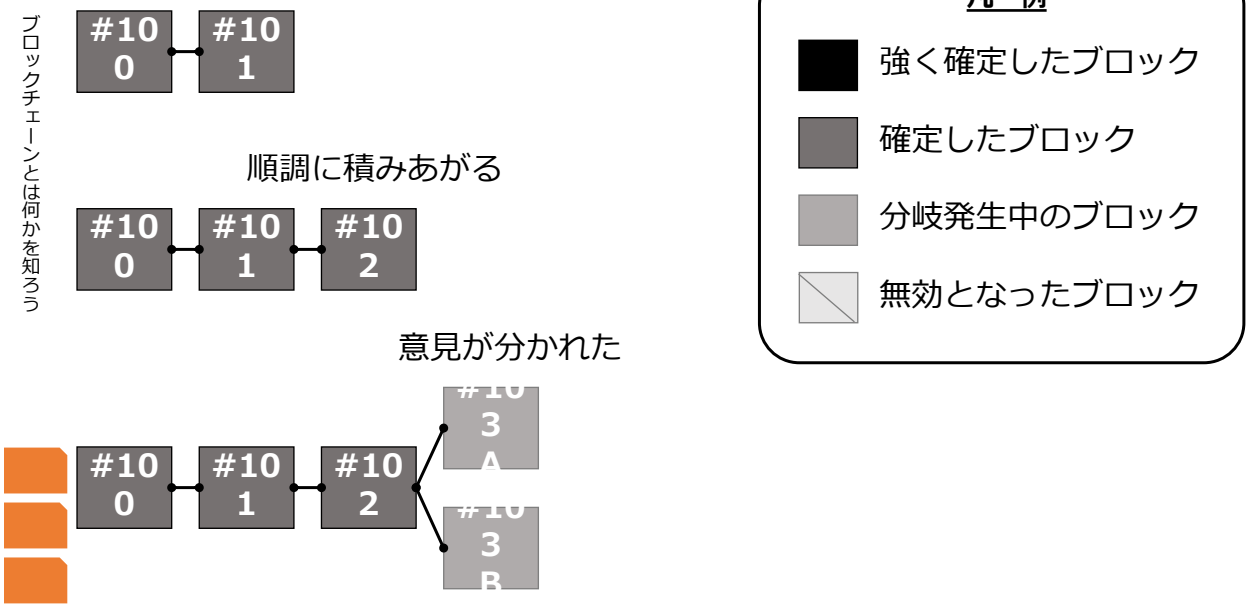
© 2015-2017 CurrencyPort Limited

Lesson

ブロックチェーン合意形成のメカニズム

CurrencyPort

ブロックチェーンとは何かを知ろう

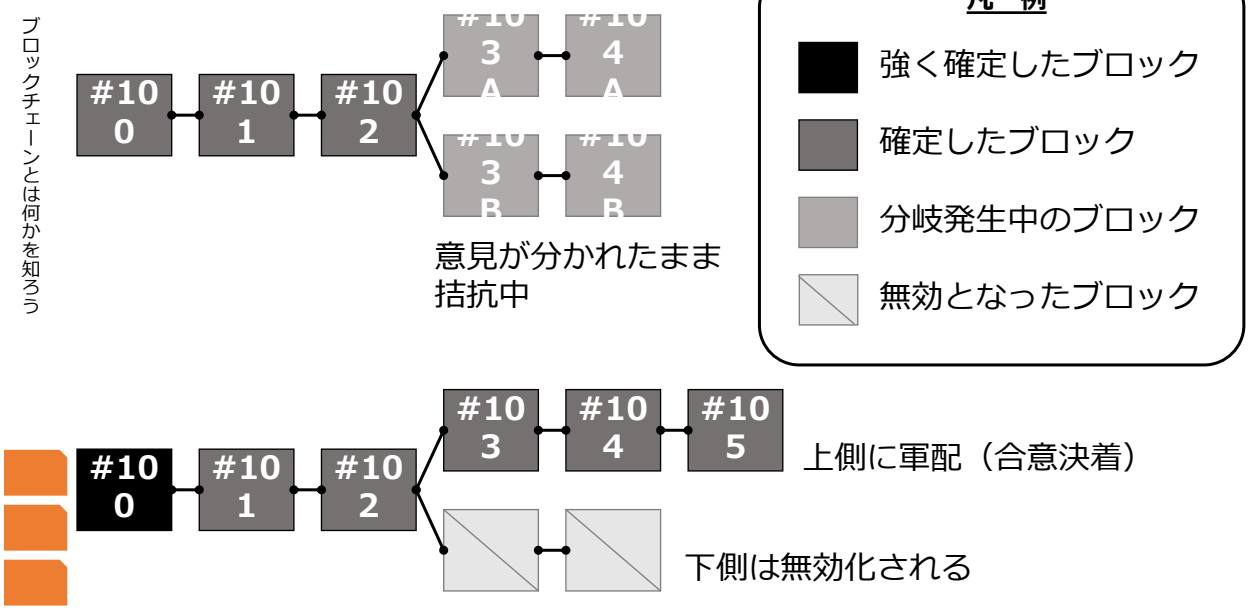


Lesson

ブロックチェーン合意形成のメカニズム

CurrencyPort

ブロックチェーンとは何かを知ろう

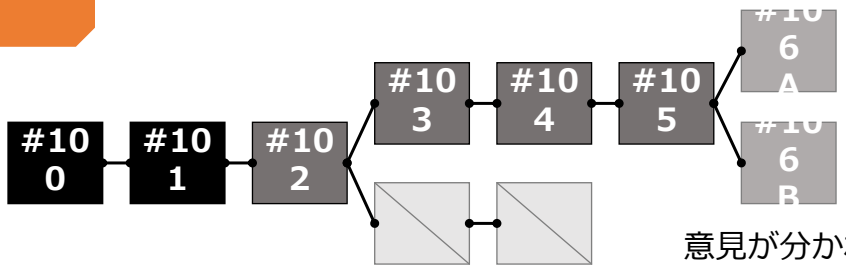


Lesson

ブロックチェーン合意形成のメカニズム

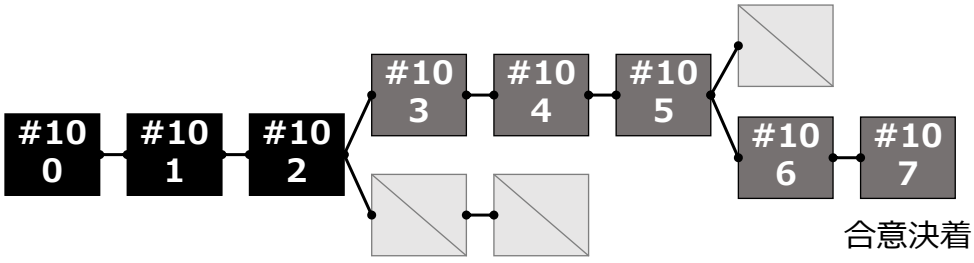
CurrencyPort

ブロックチェーンとは何かを知ろう



意見が分かれた

無効化



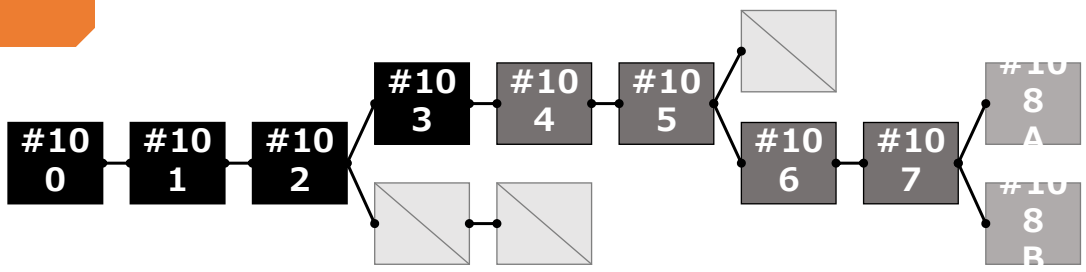
合意決着

Lesson

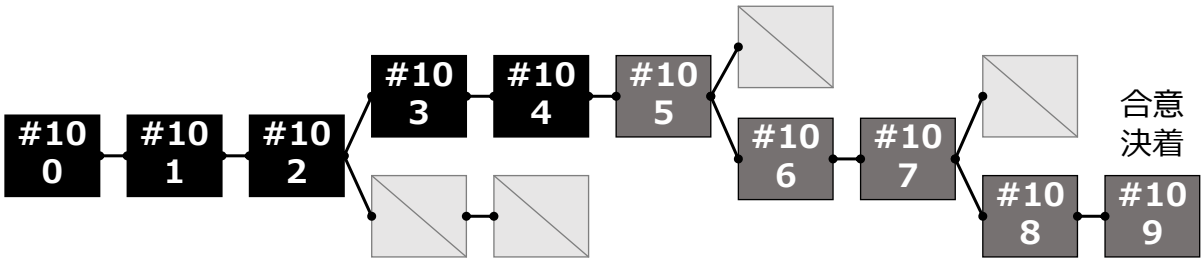
ブロックチェーン合意形成のメカニズム

CurrencyPort

ブロックチェーンとは何かを知ろう



また分岐



合意
決着

CurrencyPort

スマートコントラクトで契約を執行する仕組みを知ろう

- ✓ 送金の目的以外のものをブロックチェーンに記録する方法
- ✓ 契約を自動的に執行する仕組み
- ✓ コンピューターによる合意形成とは？
- ✓ 外部環境の情報を基にする合意形成
- ✓ 機械同士が能動的に合意形成をする未来

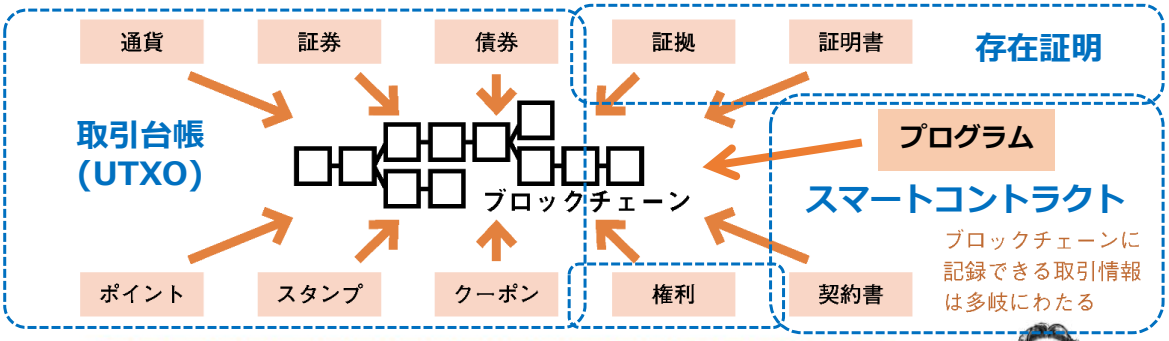
Lesson 02

ブロックチェーンになにを記録するかがカギ

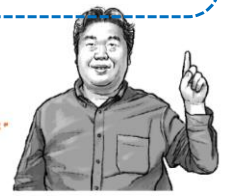
CurrencyPort

ブロックチェーンとは何かを知ろう

▶ ブロックチェーンにはさまざまな取引情報が記録できる 図表01-3



ブロックチェーンの生みの親といわれている「サトシ・ナカモト」氏は、誰にも止められず、誰にも邪魔されない「送金取引」をこのような仕組みに記録できれば仮想通貨が実現できると考えました。それが「ビットコイン」です。



17
13

Lesson 39

スマートコントラクトを知ろう

送金以外を目的とするトランザクション

CurrencyPort

存在証明

▶送金以外を目的とするトランザクションの例 図表39-2

Aさんがある文書の存在証明をしようとした

INPUT	OUTPUT
Aの電子署名と公開鍵	Aのウォレットアドレス
3,000	3,000
	OP_RETURN
	文書のハッシュ値
3,000	3,000

送金の取引

存在証明したい文章

Hash(文章)

送金を目的としなくても、必ず送金の取引は行う必要がある。その場合、自分宛に送金する形をとる

送金以外の拡張機能を利用する目的で作られるトランザクションであっても「送金」の取引は必ず記載されています。

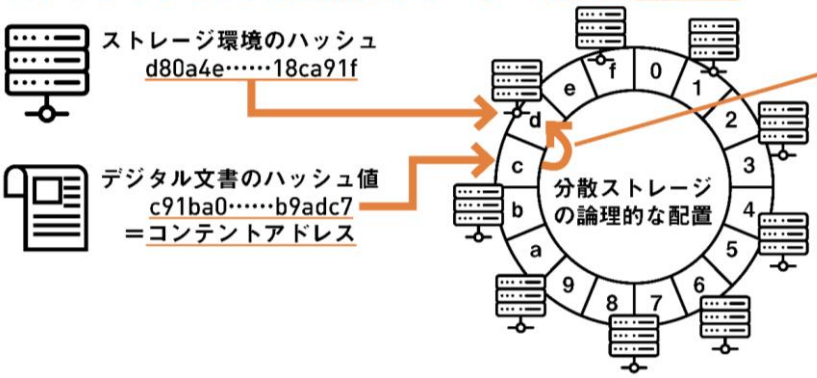
Lesson 57

ブロックチェーンの活用される未来

証憑書類の保管・デジタル文書の真正性証明に活用する

CurrencyPort

▶コンテントアドレスと分散ストレージへの配置 図表57-1



✓ブロックチェーンの応用の幅を広げる分散ストレージ
✓コンテントアドレス

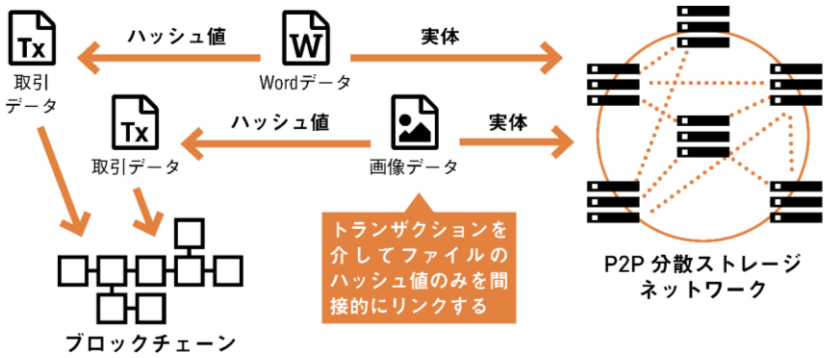
Lesson 28

ファイルのハッシュ値と実態をつなげる「コンテンツアドレス」

CurrencyPort

スマートコントラクトを知ろう

▶ファイルの実体はP2P分散ストレージへ
ファイルのハッシュ値のみブロックチェーンへ 図表28-2



ブロックチェーンに記録したデータは、変更や削除ができないという点に注意が必要です。

ハッシュ値をアドレスとして利用することで、ファイルの特定が可能になる

○「改ざんされては困るもの」の保存に適している

10 6 10 7

Lesson 47

自動的に契約を執行する仕組み

CurrencyPort

スマートコントラクトを知ろう

▶ニック・スザボによるスマートコントラクトの定義 図表47-1

契約行為

契約内容を人のいないところで自動的に履行する仕組みをスマートコントラクトという。そのため、人と人が対面で行う販売行為はスマートコントラクトとはいえないが、自動販売機のような人対機械の販売行為はスマートコントラクトといえる

17 1

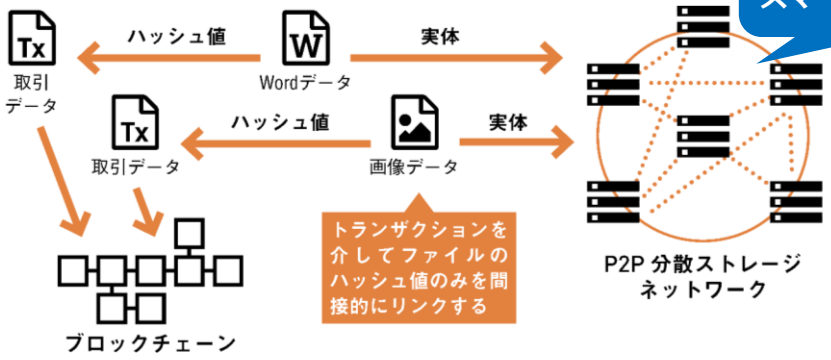
Lesson 28

ファイルのハッシュ値と実態をつなげる「コンテンツアドレス」

CurrencyPort

スマートコントラクトを知ろう

▶ファイルの実体はP2P分散ストレージへ
ファイルのハッシュ値のみブロックチェーンへ 図表28-2



契約とプログラムを結合することができればスマートコントラクトに

ブロックチェーンに記録したデータは、変更や削除ができないという点に注意が必要です。

ハッシュ値をアドレスとして利用することで、ファイルの特定が可能になる

○「改ざんされては困るもの」の保存に適している

10分10秒

Lesson 48

複雑な条件分岐を含む高度なスマートコントラクト

CurrencyPort

スマートコントラクトを知ろう

▶スマートコントラクトをプログラミングできるブロックチェーン 図表48-1

Ethereum
(イーサリアム)

スマートコントラクト開発言語:
Solidity(専用言語)、Python

Hyperledger Fabric
(ハイパーレジャー・ファブリック)

スマートコントラクト(チェーンコード)開発言語:
Go、Java

R3 Corda

スマートコントラクト開発言語:
Kotlin(Javaから派生)

スマートコントラクトでは、使用される言語に関わらず、バイトコード化され仮想マシン上で実行されるため、合意に影響するような環境依存性はなくなります。

17分

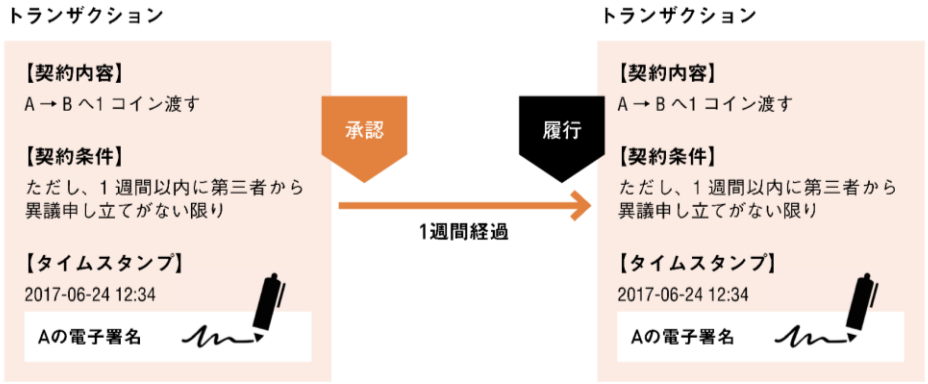
Lesson 47

自動的に契約を執行する仕組み

CurrencyPort

スマートコントラクトを知ろう

▶ ブロックチェーンにおけるスマートコントラクト 図表47-2



トランザクションをブロックチェーンに投かんした時点、承認された時点では、まだ契約条件を満たしていませんが、上記の場合1週間を経過するとその条件が自動的に満たされ、解釈として契約（A→Bへ1コインを渡す）が成立します。

17-2

条件付き支払い

エスクロー

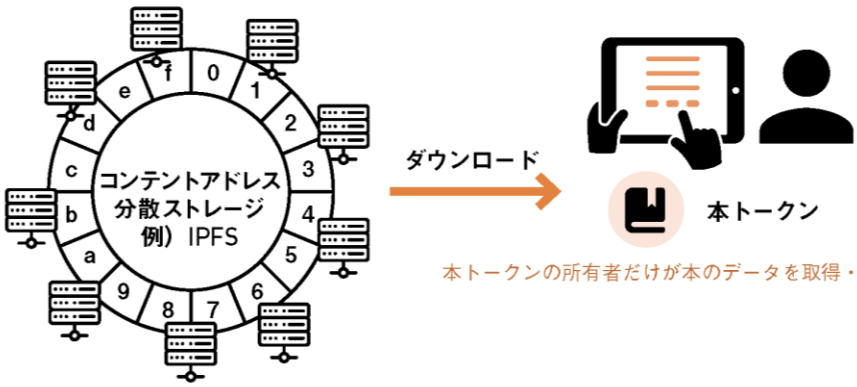
Lesson 61

スマートコントラクトでコンテンツを管理

CurrencyPort

スマートコントラクトを知ろう

▶ トークンを持っている人だけがダウンロードして再生できる 図表61-1



本トークンの所有者だけが本のデータを取得・再生できる

大きなメディアファイルの本体を、IPFSのようなファイルシステムに格納し、ブロックチェーンにはそのアドレスだけを保管するという方法はベストプラクティスの1つです。

208

Lesson 61

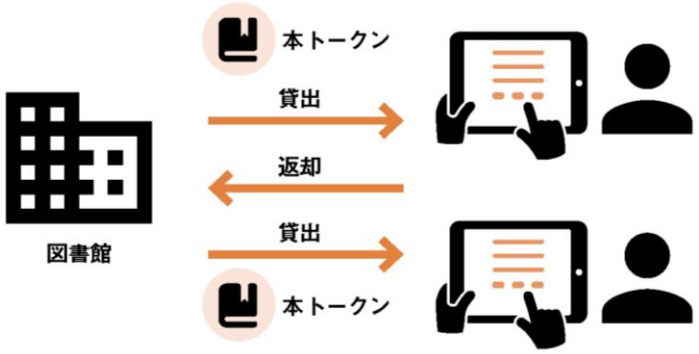
スマートコントラクトでコンテンツを管理

CurrencyPort

スマートコントラクトを知ろう

209

▶図書館で電子書籍を貸し出す 図表61-2



本トークンを図書館に戻すと読めなくなる

このDRM方式を本当に実現しようと思ったら、リーディングシステム（電子書籍リーダー）のレベルでの実装が必要になります。しかしほかのベンダー依存のDRMと異なり、復元手順のプロトコルをオープンにしても問題がないのが重要なポイントです。

Lesson 65

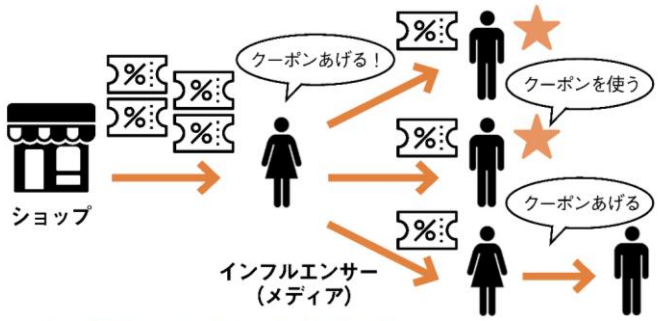
ブロックチェーンで広告技術が新たな革新を得る

CurrencyPort

ブロックチェーンの活用される未来

210
211

▶クーポンが転々流通するイメージ 図表62-1



クーポンの形態としてはQRコードなどが考えられる

友達の多い、いわゆる「インフルエンサー」をうまく組織して、彼らにクーポン配布を委任する仕組みができれば、効率的にクーポン配布ネットワークが構築できそうです。

✓ウォレットアドレスは会員登録を必要とせず計算で生成できる
✓クーポンの転々流通具合を可視化できる（広告追跡）

利用者は、会員登録なしにクーポンウォレットを持てる

CurrencyPort

アプリのインストール後、初回起動時に面倒な会員登録や複雑な設定は不要

ダウンロード
&
インストール

ウォレットのアドレスを自動生成

《処理手順》
1．ランダムな秘密鍵を生成
2．秘密鍵から公開鍵を生成
3．公開鍵からウォレットのアドレスを生成
4．秘密鍵はクライアント内に安全に保管

※秘密鍵生成時のエントロピーを増加させる目的で、
インストール時にミニゲーム等をさせると、より安全になります。

利用開始OK!

会員でなくても、クーポンを贈りあったり、使ったりできる。

※もちろん、後からJCB会員との紐づけすることもできます。

CurrencyPort © 2015 - 2016 CurrencyPort Limited 69

オファーの引き渡しの方法は大きく２つ

CurrencyPort

１．対面で送信相手にウォレットアドレスを提示してもらう

直接会ってアプリからQRコードを提示

Skype等を使って画面にQRコードを映す

２．非対面でメッセージングツールを利用しオファーを送る

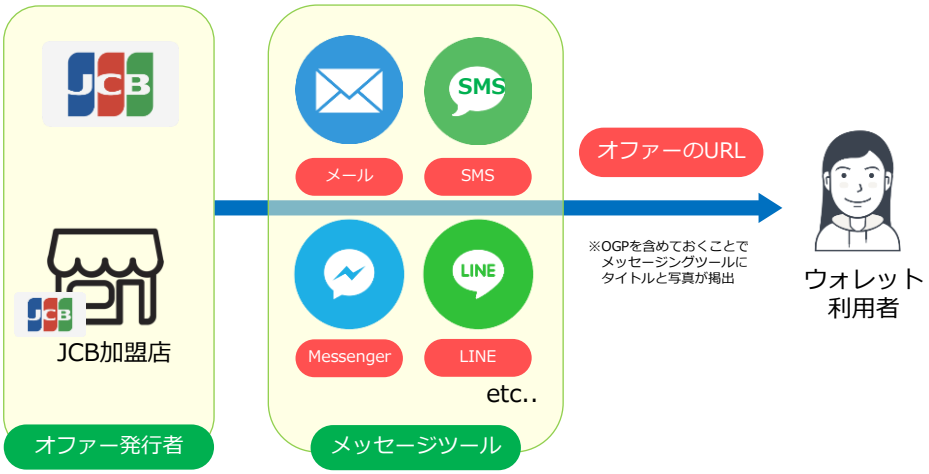
メール　SMS　Messenger　LINE　etc..

CurrencyPort © 2015 - 2016 CurrencyPort Limited 70

オファーの引き渡し操作（クーポンを贈る）

CurrencyPort

例）メッセージングツールを使用して、オファーのURLを送る。

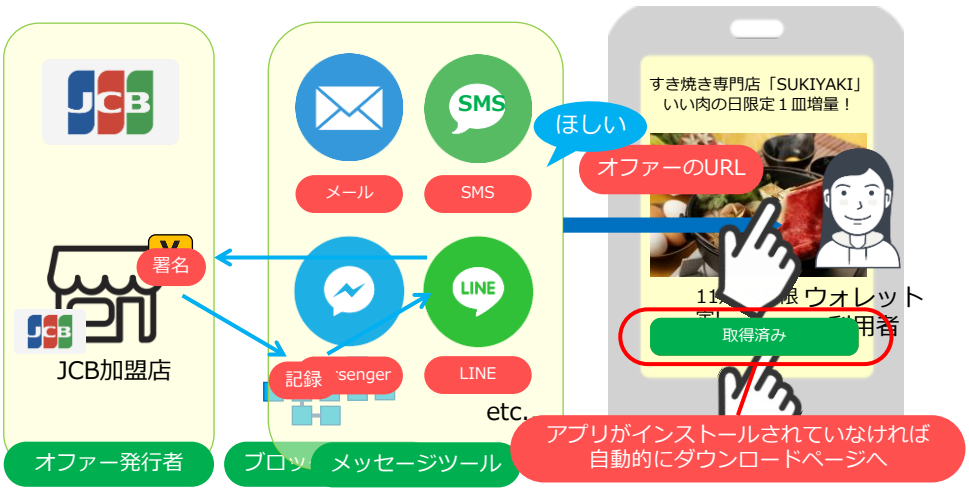


CurrencyPort © 2015 - 2016 CurrencyPort Limited 71

オファーの引き渡し操作（クーポンを贈る）

CurrencyPort

例）メッセージングツールを使用して、オファーのURLで送る。

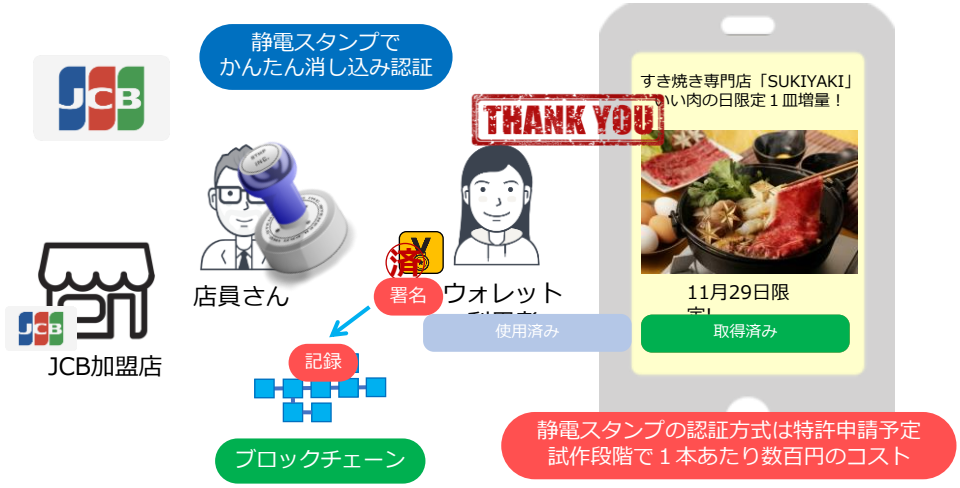


CurrencyPort © 2015 - 2016 CurrencyPort Limited 72

オファーの消し込み操作（クーポンを店頭で利用する）

CurrencyPort

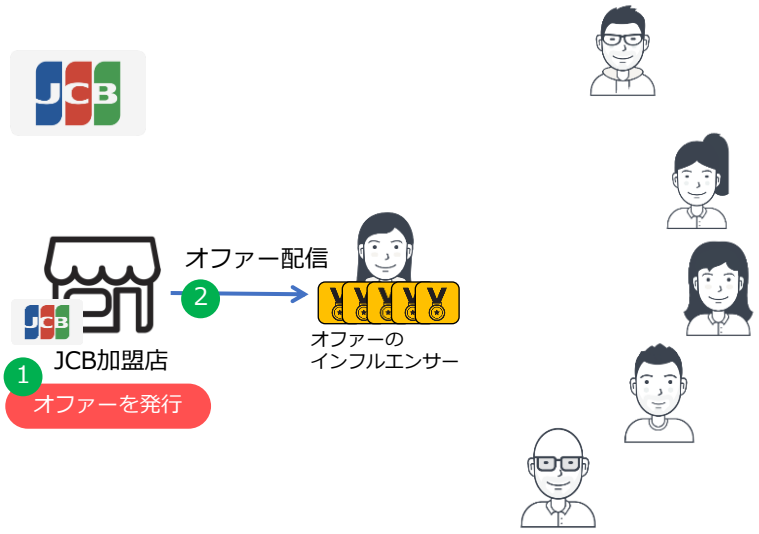
例）利用者はアプリでクーポンを見せるだけ、お店側はスタンプを押すだけ。



© 2015 - 2016 CurrencyPort Limited

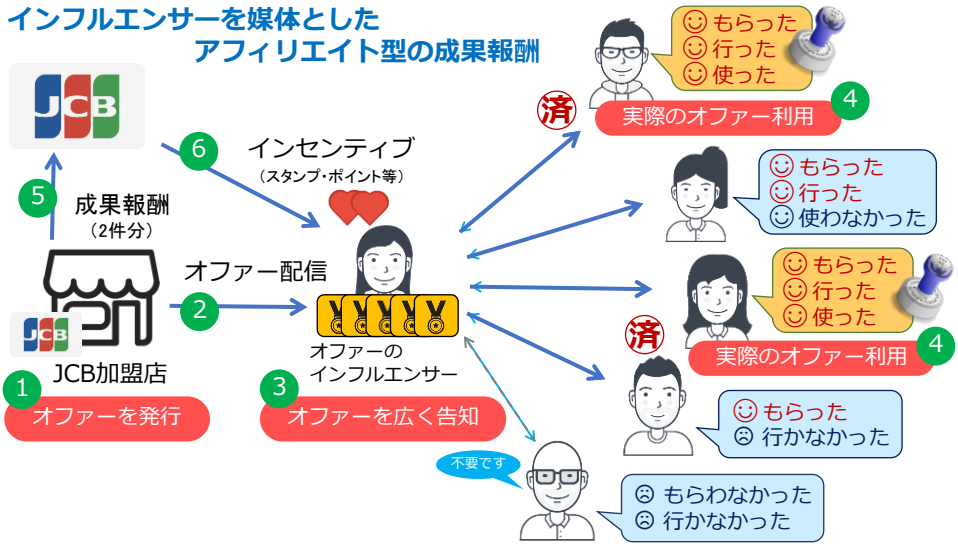
オファーの拡散方法とインセンティブ

CurrencyPort



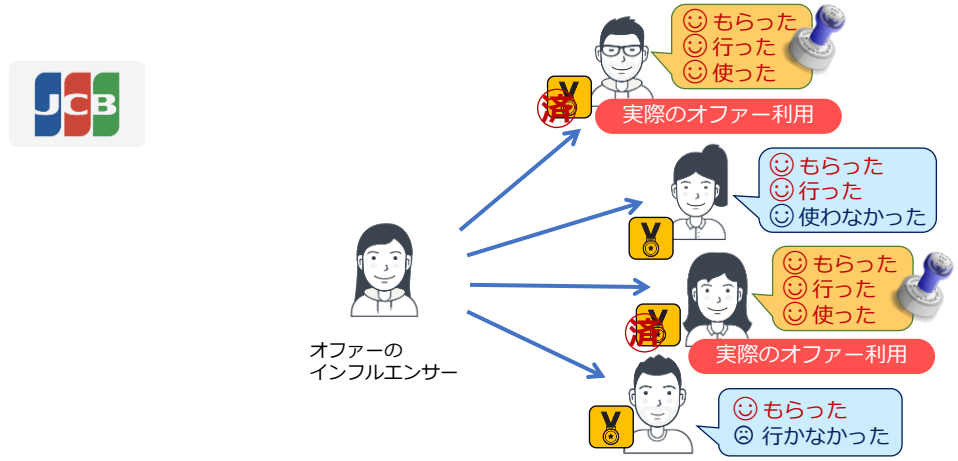
© 2015 - 2016 CurrencyPort Limited

オファーの拡散方法とインセンティブ



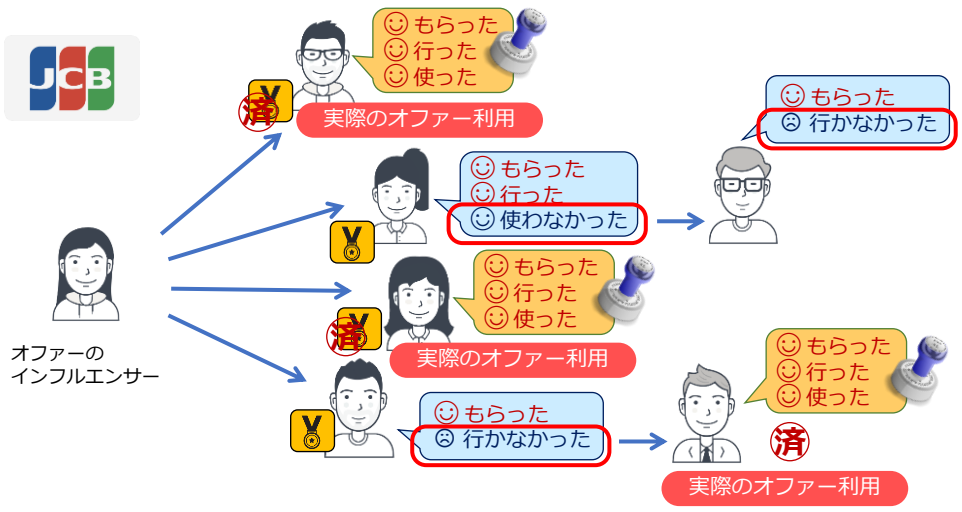
© 2015 - 2016 CurrencyPort Limited

未使用のオファーは転々流通させることができる



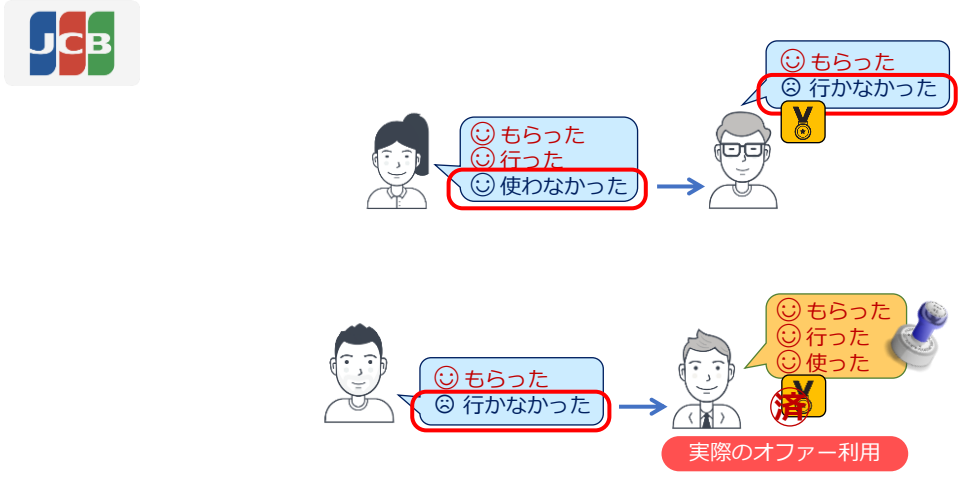
© 2015 - 2016 CurrencyPort Limited

未使用のオファーは転々流通させることができる



CurrencyPort
© 2015 - 2016 CurrencyPort Limited
77

未使用のオファーは転々流通させることができる

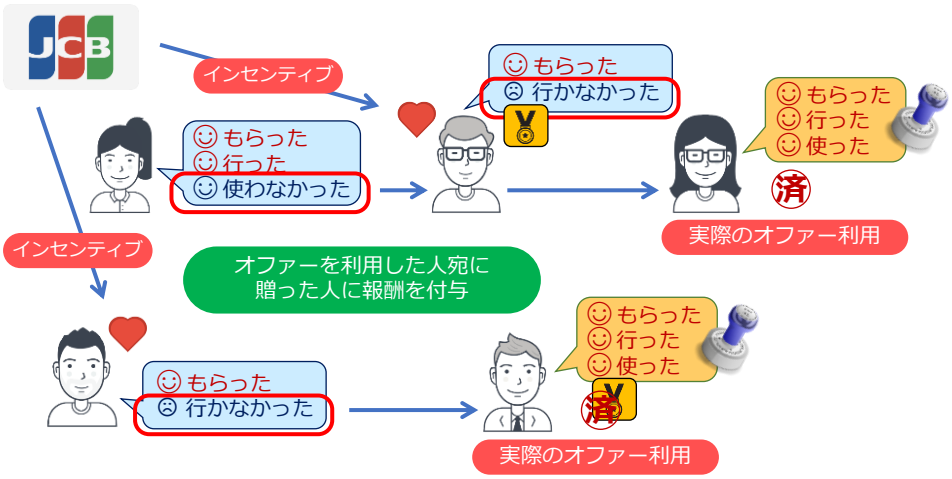


CurrencyPort
© 2015 - 2016 CurrencyPort Limited
78

オファーの転々流通を促す追跡型インセンティブ

CurrencyPort

自分で利用しないオファーは、使ってもらえそうな人に贈るとお得に！



© 2015 - 2016 CurrencyPort Limited

期待できる効果

CurrencyPort

仮想通貨技術を応用したオファー転送によって

- ✓ 本当にクーポンを利用したい人にオファーが到達する
- ✓ オファーの利用率向上が見込める
- ✓ オファーの転々流通ぐあいを可視化して追跡できる
  ⇒ **マーケティング施策に利用可能**
- ✓ JCBカードを持っていない潜在層にもリーチする

© 2015 - 2016 CurrencyPort Limited

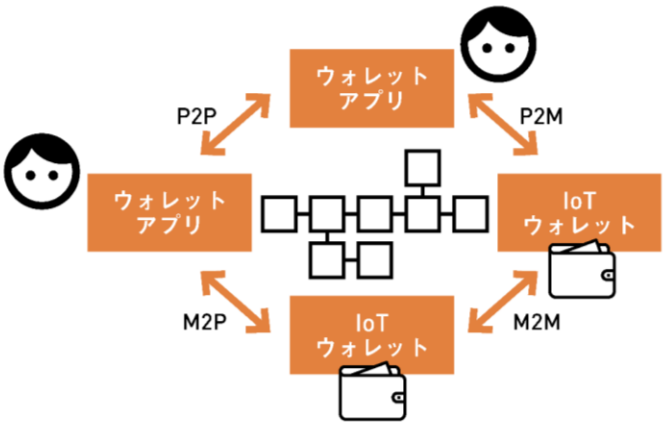
Lesson 50

マシンがスマートコントラクトを利用するとどうなるか？

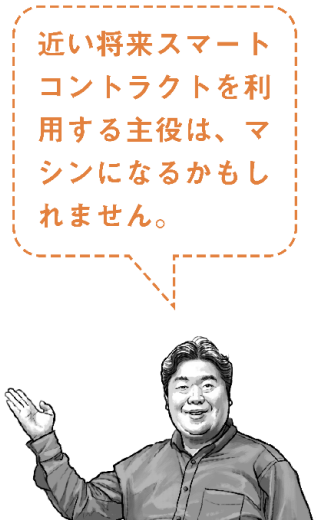
CurrencyPort

スマートコントラクトを知ろう

▶マシンが自律的にサービスを提供する 図表51-1



スマートコントラクトによって、P2P（People to People：人と人）だけでなく、P2M（People to Machine：人と機械）、M2M（Machine to Machine：機械と機械）の取引が当たり前になる

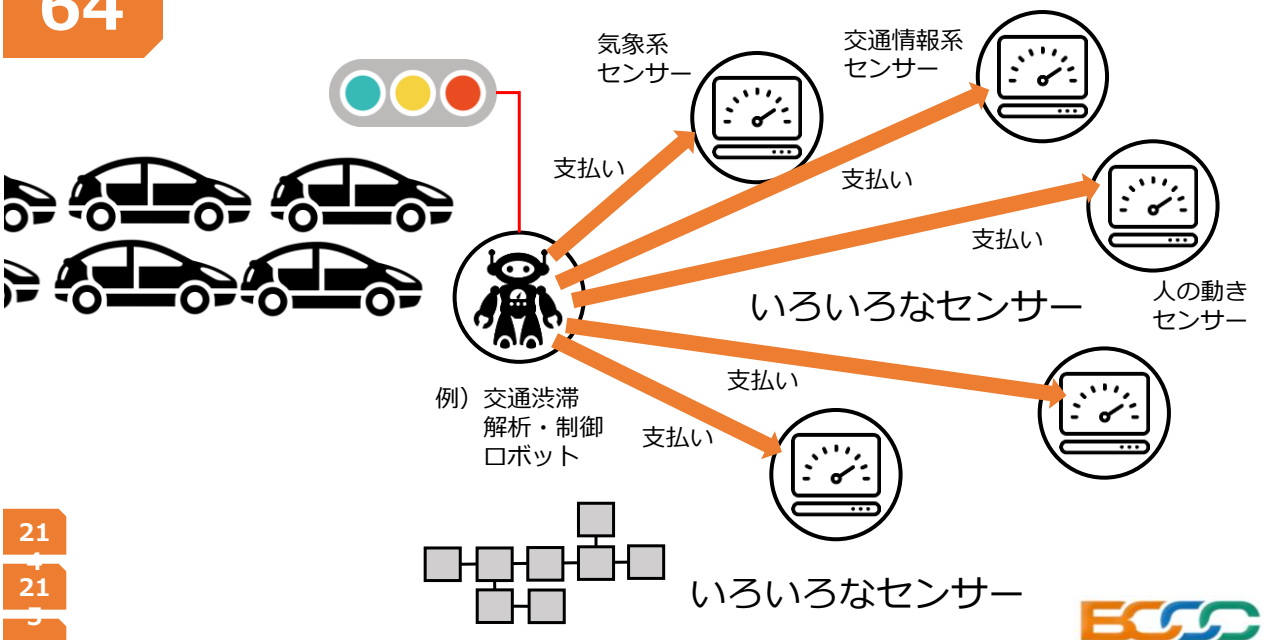


186

Lesson 64

マシン対マシンの支払いが普通になる未来

CurrencyPort



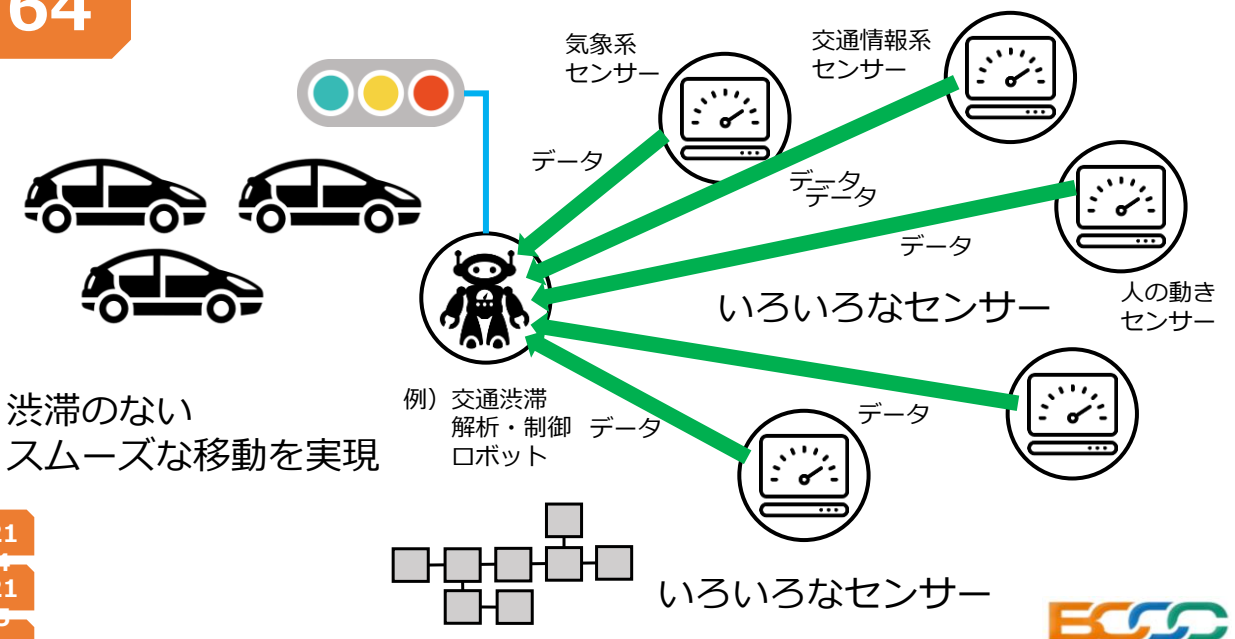
Blockchain Collaborative Consortium

21
21

Lesson 64

マシン対マシンの支払いが普通になる未来

CurrencyPort



21
21

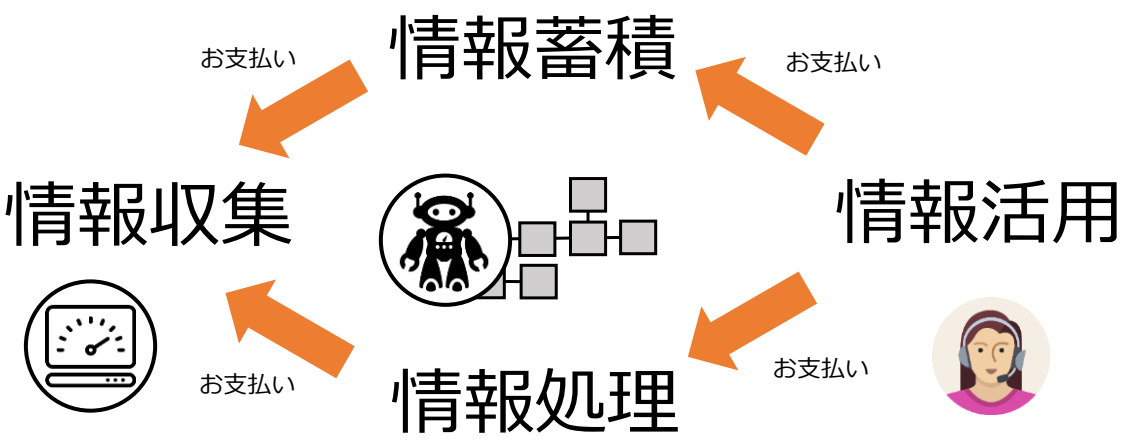
Blockchain Collaborative Consortium

Lesson 64

スマートシティ・IoT
「自律分散差社会」のエコシステム

CurrencyPort

ブロックチェーンの活用される未来



21
21

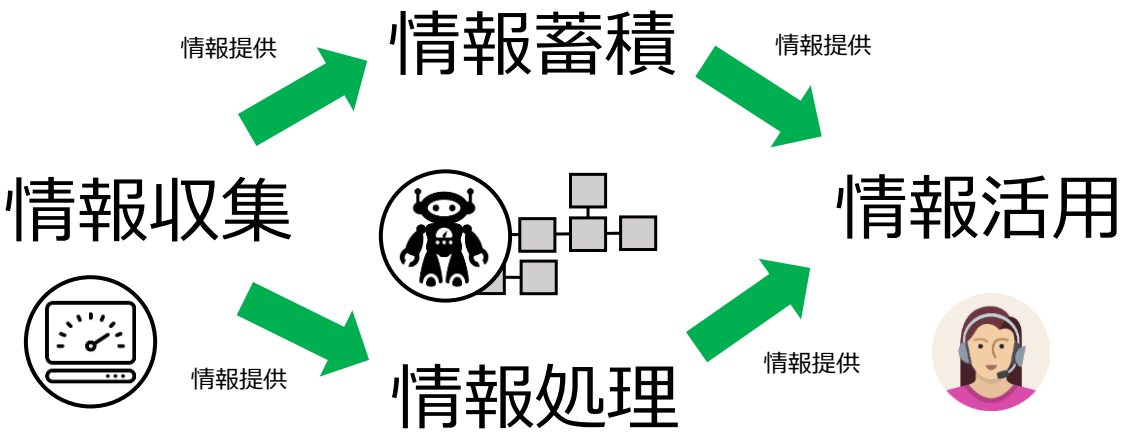
Blockchain Collaborative Consortium

Lesson 64

スマートシティ・IoT「自律分散差社会」のエコシステム

CurrencyPort

ブロックチェーンの活用される未来



21
21

Blockchain Collaborative Consortium

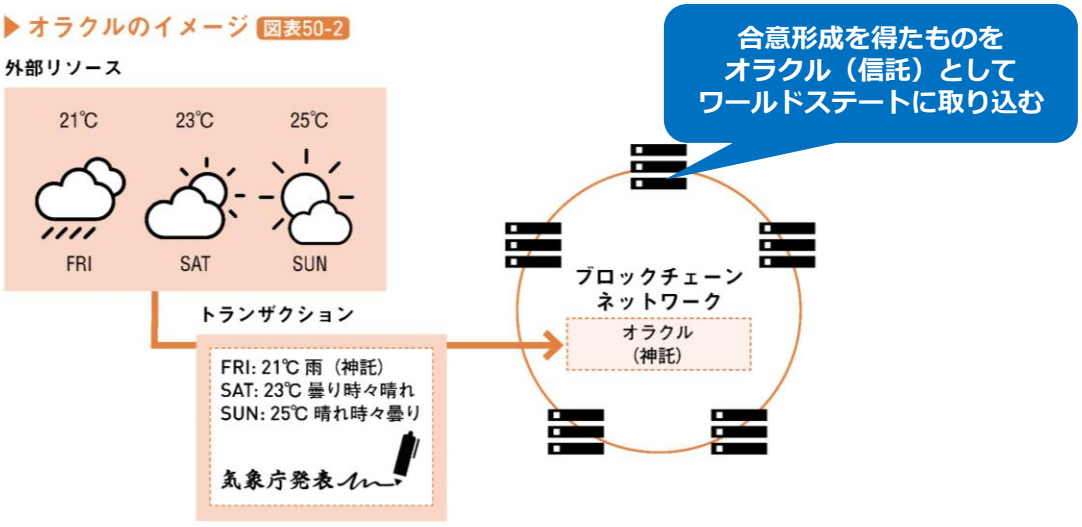
Lesson 50

第三者提供の情報リソースを「オラクル」（信託）と考える

CurrencyPort

スマートコントラクトを知ろう

▶ オラクルのイメージ 図表50-2



外部リソースはトランザクションから登録して、合意を得たものを「オラクル」とする

184

Lesson 48

ワールドステート（世界の状態）

CurrencyPort

スマートコントラクトを知ろう

▶ワールドステートはすべてのスマートコントラクトから参照できる情報 図表48-2

ブロックチェーンのネットワークに参加しているノードが一斉に計算して合意

スマートコントラクトにおける合意結果は、「ワールドステート」と呼ばれ、ブロックチェーンに記録されると、ほかのスマートコントラクトと共有されます。

175
176

Lesson 48

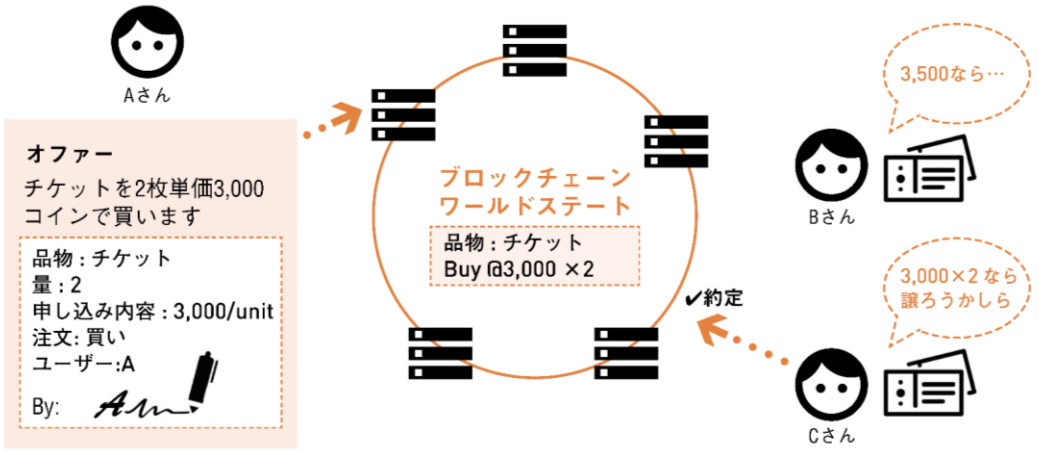
ワールドステートの合意で中央集権的組織が不要となる取引の例

CurrencyPort

DEX

スマートコントラクトを知ろう

▶ワールドステートを応用したチケット取引所の例 図表48-3



トランザクションにオファーを書き込んでワールドステートに投かん。ほかの参加者が契約を自動的に約定

177

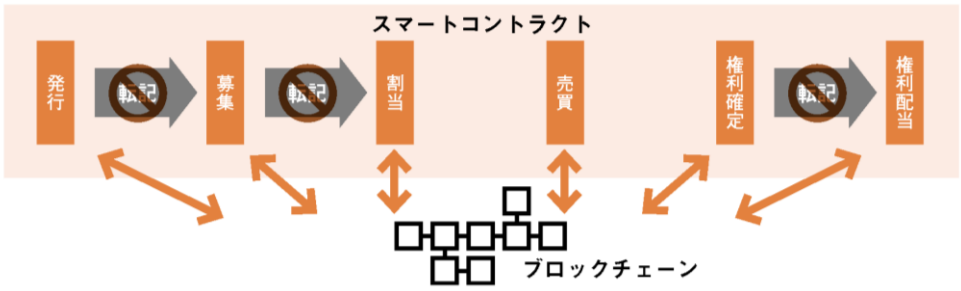
Lesson 56

スマートコントラクトとの相性が良い証券分野での活用

CurrencyPort

スマートコントラクトを知ろう

▶ブロックチェーン技術の台頭によって消える「リコンサイル(転記)業務」 図表56-1



証券業務では、発行から配当までを1つの分散システムで構築できる。
そうなるとリコンサイル（転記）業務は事実上なくなる

証券としての価値の一生、つまり、証券が生まれて死ぬまでのいっさいを、ブロックチェーンを使って記録管理できるため、従来分断されていた各業務は１つのスマートコントラクトによって置き換えが可能になってしまいました。

198

Lesson 65

スマートコントラクトをシェアリングエコノミーに応用する

CurrencyPort

スマートコントラクトを知ろう

▶シェアリングエコノミーへの応用イメージ 図表65-1

たとえば民泊の場合、「部屋の鍵を開ける権利」をトークンに持たせることができる

216

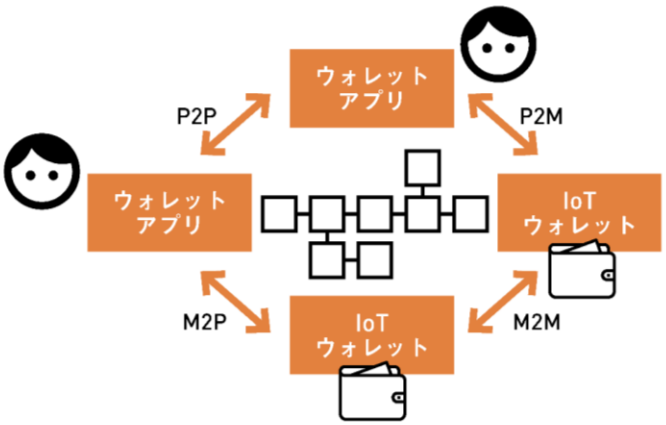
Lesson 50

マシンがスマートコントラクトを利用するとどうなるか？

CurrencyPort

スマートコントラクトを知ろう

▶マシンが自律的にサービスを提供する 図表51-1



スマートコントラクトによって、P2P（People to People：人と人）だけでなく、P2M（People to Machine：人と機械）、M2M（Machine to Machine：機械と機械）の取引が当たり前になる

近い将来スマートコントラクトを利用する主役は、マシンになるかもしれません。

186

Lesson 66

トークンで電子投票システムを実現する

CurrencyPort

ブロックチェーンの活用される未来

名は体を表す

何を実現するかを端的に

実現可能性を確認します

絵などを使ってわかりやすく表現

社会的意義を確認します

ここでは、どう収益化するのかが考えられていれば、収益性の高さはあまり気にしなくて良いです

誰に対するサービスですか？ペルソナ化

潜在的な市場規模 BtoB / BtoC などわかれば尚良し

ブロックチェーンに関する理解度を特に重要視します

タイトル	オンライン電子投票システム	チーム名	電子立国実現党

この企画によって達成したいこと・目的 (What)

電子立国の実現のため、
まずは、国政選挙投票制度の電子化が必須と考えた。

- 投票所に行かずとも、投票できる仕組み
- 投票〆切後、即時開票も可能となる仕組み

なぜ、この企画が必要なのか？社会的背景や課題 (Why)

選挙投票率の低下は民主主義の根底を揺るがす大きな問題である。
その原因には、投票所に行く面倒くささがあげられる。
投票日に限らず、期日前投票にしても、投票を自宅で完了できる仕組みはできるはずだ。

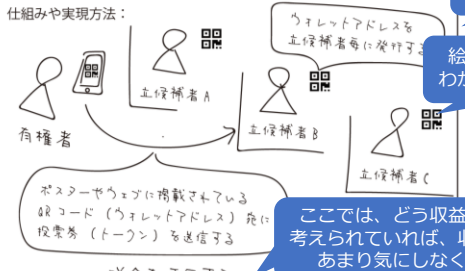
ターゲット・どんな人のために

18歳以上の投票権を持つすべての国民

有権者全員が積極的に選挙の投票に参加できるようにするため。

どのようにやるのか？ (How)

仕組みや実現方法：



収益化モデル：税金を活用する。
ただし、オンライン電子投票が実現すれば、選挙運営の効率向上により、投票担当従業員より軽減されるはずだ

ブロックチェーンやDLTの特性を利用するポイント

選挙権をブロックチェーン上のトークンとして発行し立候補者をウォレットと見立てて記録することで、二重投票を防止しながら「1人1票」を確実にできる。
課題として残る「有権者管理」と「匿名投票」の実現という相反する要求については、リング署名という暗号技術を用いて工夫すれば、クリアできそう。

21 ○ 21