目白大学向け講義資料

 1

暗号技術と ブロックチェーンの仕組み

2020年10月6日
才所敏明
（株）IT企画・代表取締役社長
中央大学研究開発機構・研究員
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp
https://www.facebook.com/toshiaki.saisho

 2

自己紹介

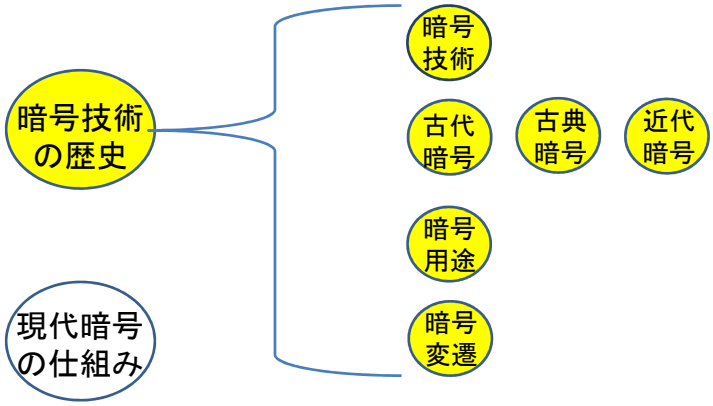
1966年　東京大学・工学部・計数工学科・数理コース
1970年　東芝入社
　社内計算機利用環境企画・構築・活用指導・支援
　　スーパコン～PCを利用した技術開発環境構築・活用推進（1969UNIX）
　　インターネットの企業活動への活用推進（1974Internet　1984JUNET）
　情報セキュリティ研究開発企画・推進、事業支援（1995）
　　暗号技術研究開発・社内事業への活用推進、国プロ企画・受託・推進
2007年　（株）IT企画設立
　事業支援活動（顧問・相談役）：2社（日、米）
　大学教育活動（情報セキュリティ）：九大、目白大
　研究開発活動（研究員）：中央大学研究開発機構
　　暗号・認証、秘密分散、バイオメトリクス、電子メールセキュリティ、
　　IoTシステムセキュリティ、FinTech（仮想通貨、ブロックチェーン）
　　ビッグデータ、AI

本日の説明内容

［1］暗号技術の歴史と現代暗号の仕組み

［2］ブロックチェーンとビットコイン

［1］暗号技術の歴史と現代暗号の仕組み



［2］ブロックチェーンとビットコイン

暗号技術

暗号技術とは

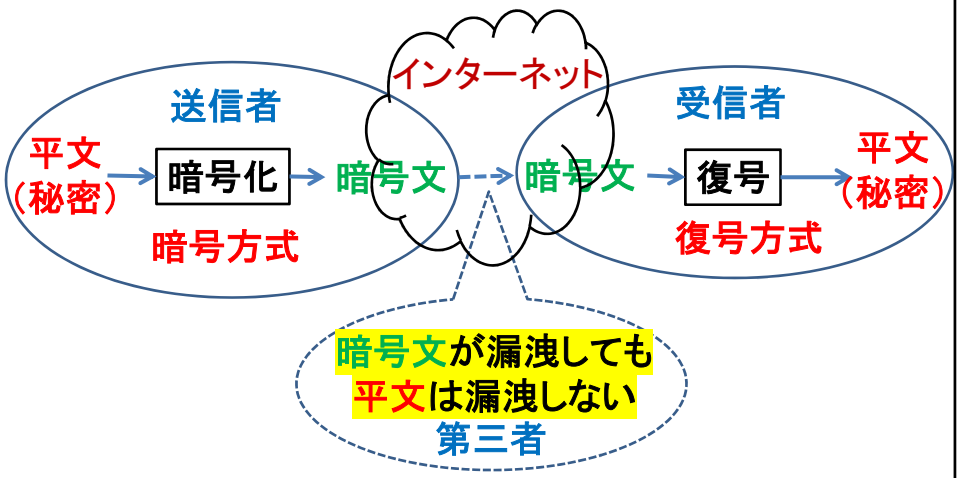
暗号化：一般の人にも理解できるデータ（**平文**）を
特別な知識を有する人しか理解できないデータ
（**暗号文**）へ変換すること

復号：特別な知識を有する人が、
その知識を利用し**暗号文を平文へ変換**する（戻す）こと

暗号技術：暗号化に使用する技術
および復号に使用する技術の総称

暗号技術

暗号技術の利用例　ー秘密の安全な送信ー



➔世界中の人が使用しているインターネットを利用しても、
個人情報やプライバシー情報等の秘密の情報のやり取りが可能

古代暗号

 7

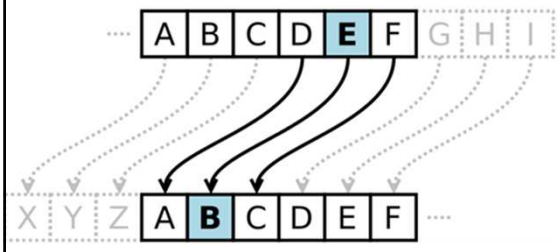
暗号技術発展の歴史　古代暗号

（例1）シーザー暗号（紀元前100年頃）

シェイクスピアの『ジュリアス・シーザー』の

「ブルータスよ、お前もか」のジュリアス・シーザー

アルファベット順で3文字左へ変換



A	T	T	A	C	K
		↓ 暗号化			
X	Q	Q	X	Z	H
		↓ 復号			
A	T	T	A	C	K

古典暗号

 8

暗号技術発展の歴史　古典暗号

外交活動の活発化による暗号の普及期へ

（例1）ノーメンクラター暗号、16世紀ごろ（スコットランド女王メアリ暗号）

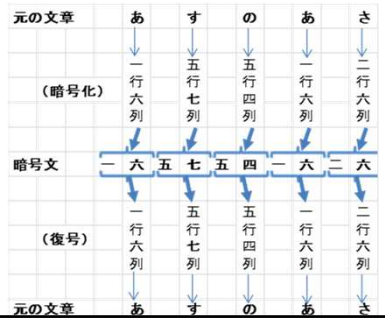
イングランド女王エリザベス暗殺をたくらみ仲間と暗号通信

側近ウオルシンガムの部下が解読、証拠確保、関係者処刑

敵対勢力の暗号化された通信から情報を継続入手するため、
暗号解読の事実を伏せることは、以降の歴史でも良く採られた方法

（例2）上杉暗号（戦国時代、16世紀ごろ）　川中島の戦い（武田信玄）

七	六	五	四	三	二	一	
ゑ	あ	や	ら	よ	ち	い	一
ひ	さ	ま	む	た	り	ろ	二
も	き	け	う	れ	ぬ	は	三
せ	ゆ	ふ	ゐ	そ	る	に	四
す	め	こ	の	つ	を	ほ	五
ん	み	え	お	ね	わ	へ	六
	し	て	く	な	か	と	七



近代暗号

 9

暗号技術発展の歴史　近代暗号

暗号化・復号・解読は、手作業から機械へ

（例）エニグマ暗号（第2次世界大戦でドイツ使用）

英国の数学者アラン・チューリングのグループが解読、解読できたことは極秘にし、機密情報入手

エニグマ暗号解読の事実は極秘事項として扱われ、ドイツは終戦までエニグマを信頼して使用し続けていた。エニグマ暗号が解読されていたという事実が公表されたのは、解読から20 年以上も経過した1974 年のことであった。

エニグマ暗号機

暗号用途

 10

人類・社会の歴史は紛争の歴史

紛争：敵対する勢力間の争い

紛争当事者は、連携する勢力間での協議・連絡により
敵対する勢力に対し優位に立つことを目指す
➔敵対する勢力への情報漏洩を防ぐため、暗号を利用

一方、敵対する勢力は、その協議・連絡内容の把握により
対立する勢力に対し優位に立つことを目指す
➔敵対する勢力は、対立する勢力の暗号文の解読に注力

＜暗号技術の開発と解読技術の開発の繰り返し＞

暗号に関する熾烈な戦いの勝敗が、紛争の歴史、人類・社会の歴史を形作ってきた！

暗号
変遷

 11

暗号技術発展の歴史　現代暗号

暗号化・復号・解読は、計算機利用へ

コンピュータ/ネットワークの発展により、
軍事的・政治的利用から、産業活動・生活活動での利用へ

多くのベンダ（企業）による応用システム開発➔相互運用性の保証
➔暗号化/復号ソフト開発に必要な暗号方式の公開が必要に

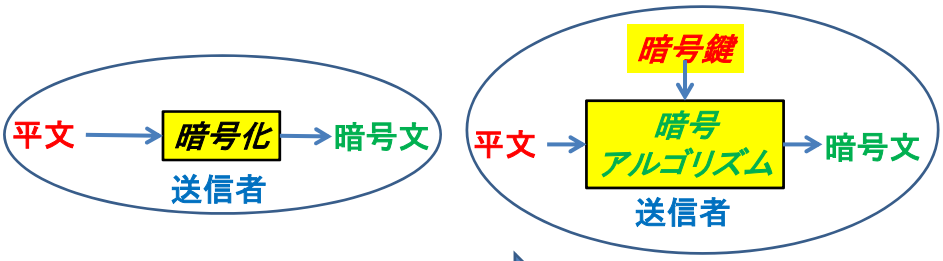
従来は“暗号方式を公開しない”ことで安全性を確保
➔従来とは異なる仕組みで
暗号文の安全性を確保することが必要に！

暗号
変遷

 12

暗号技術発展の歴史　現代暗号

暗号方式を暗号アルゴリズムと暗号鍵に分離



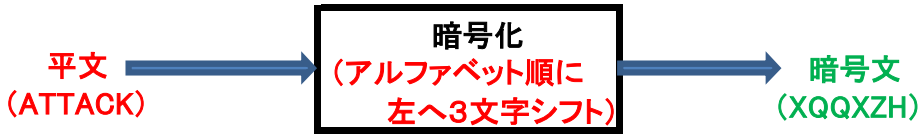
近代暗号までの暗号方式 ➡ **現代暗号の暗号方式**

現代暗号は、暗号アルゴリズムを公開しても
暗号鍵を公開しなければ安全性が確保できるよう、
暗号アルゴリズムが設計されている

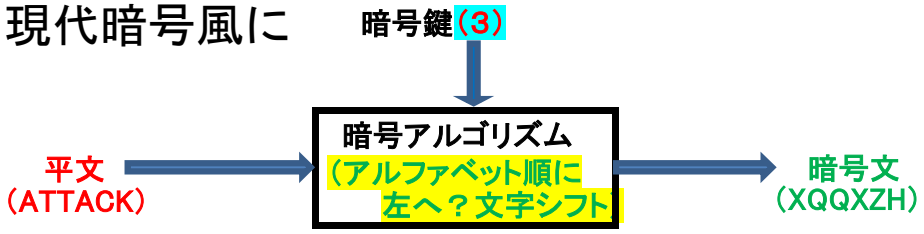
暗号変遷

暗号方式のアルゴリズムと鍵への分離
古代暗号のシーザー暗号の例

原型

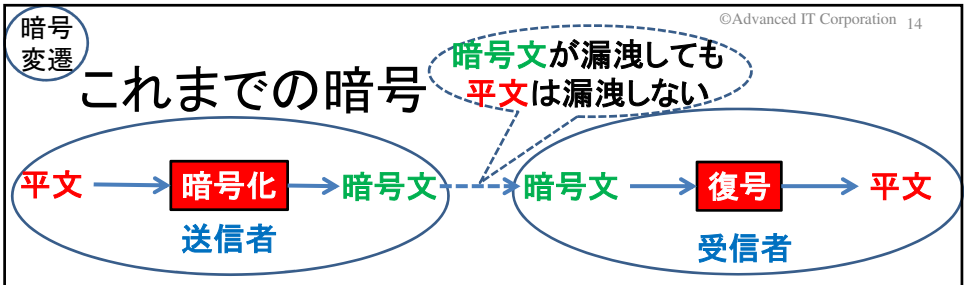


現代暗号風に

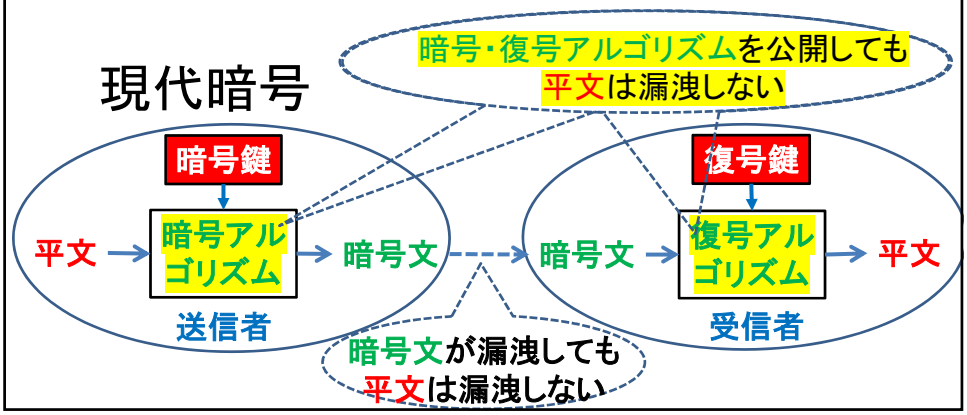


暗号変遷

これまでの暗号

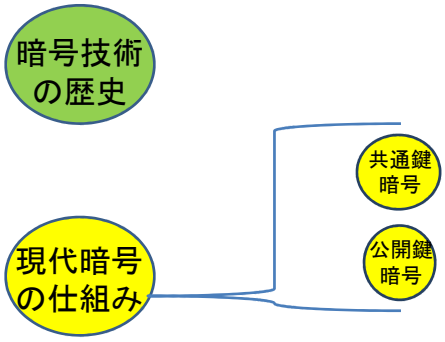


現代暗号



 15

[1]暗号技術の歴史と現代暗号の仕組み



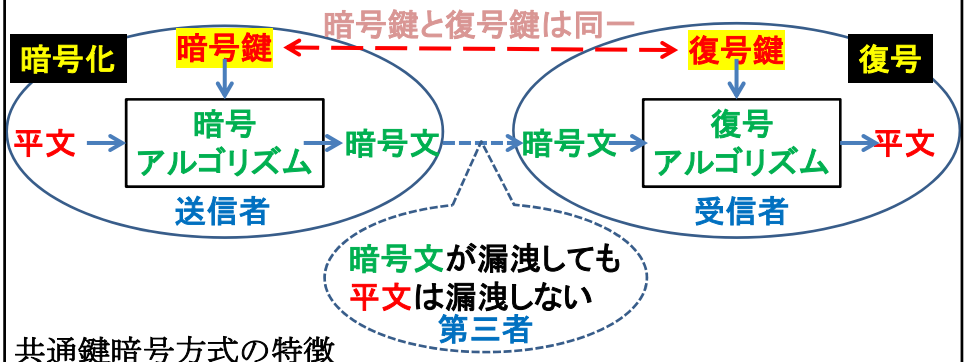
[2]ブロックチェーンとビットコイン

 16

共通鍵
暗号

現代暗号　共通鍵暗号方式

通信内容の秘匿（暗号鍵による暗号化、暗号鍵と復号鍵は同一）



共通鍵暗号方式の特徴

①暗号鍵と復号鍵が同一（共通鍵）

②送信者と受信者で秘密の共通鍵を共有しておくことが必要

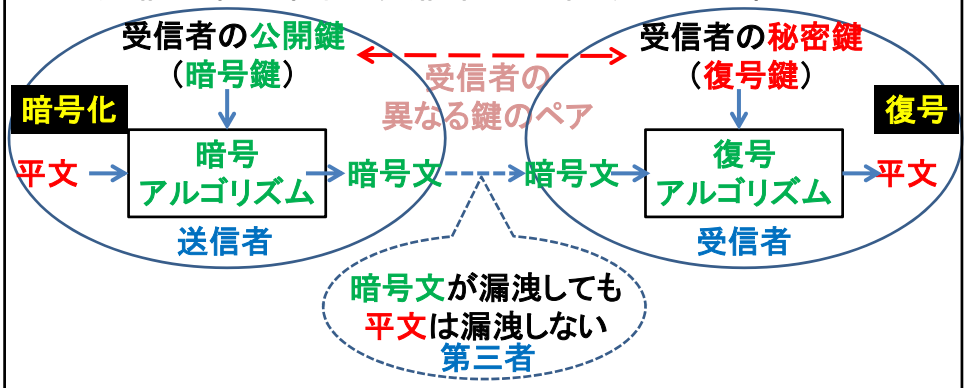
③送信者と受信者は秘密の共通鍵を
安全に保管しておくことが必要

公開鍵暗号

 17

現代暗号　公開鍵暗号方式

通信内容の秘匿（受信者の公開鍵による暗号化）



公開鍵暗号方式の特徴

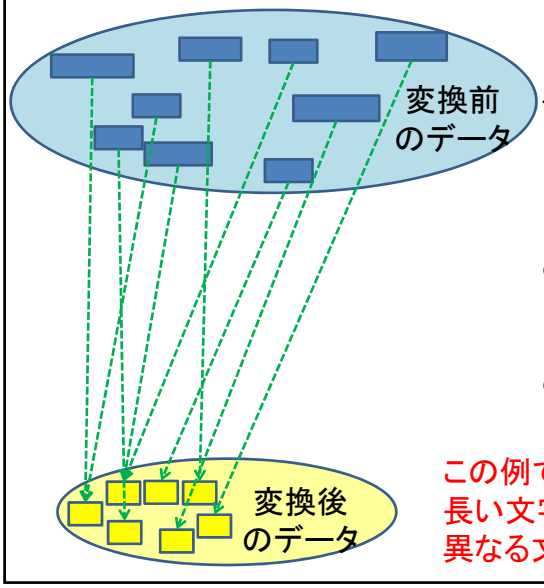
①公開鍵（暗号鍵）と秘密鍵（復号鍵）が異なる
②公開鍵から秘密鍵を計算できない
③秘密鍵は秘密に管理することが必要だが、公開鍵は公開可能
④公開鍵が受信者の正しい公開鍵であることの確認が必要

公開鍵暗号

 18

ハッシュ値

対象となるデータの特徴を一定の長さのデータに変換したもの



＜ハッシュ値の例＞

計算方法：
先頭から1文字おきの
6文字の文字列へ変換

あすのあさにこうげきせよ・・・
➔あのさこげせ

あしたのあさにこうげきせよ・・・
➔あたあにうき

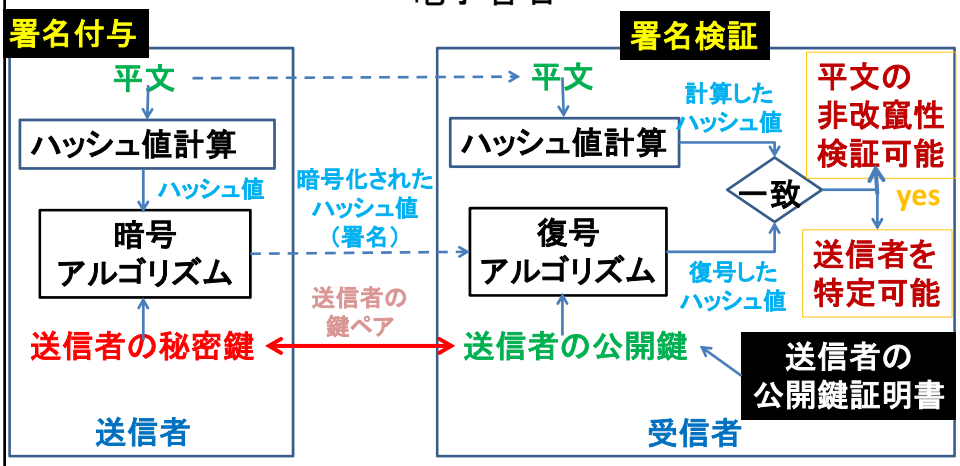
この例では、
長い文字列の特徴を6文字で表現し、
異なる文字列であることを確認できる

公開鍵
暗号

 19

現代暗号　公開鍵暗号方式

電子署名

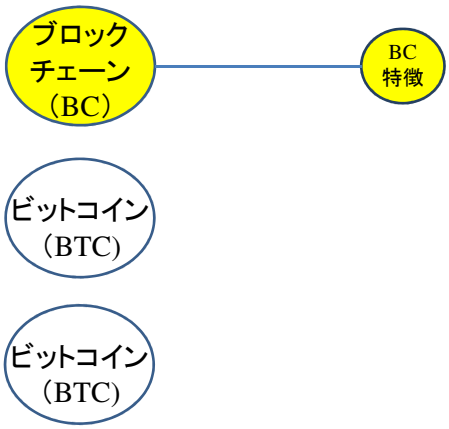


署名検証により、
　平文が改ざん（変更）されていないことの確認、
　　および署名者（送信者）の特定が可能

 20

［1］暗号技術の歴史と現代暗号の仕組み

［2］ブロックチェーン（BC）とビットコイン（BTC）

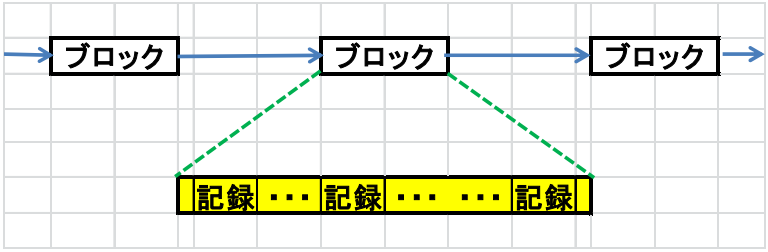


BC
特徴

 21

ブロックチェーン

取引・支払等の記録を（複数）格納しているブロックの連鎖



ブロックチェーンの特徴

（1）中央管理組織の無い記録技術

（2）記録消失の危険性が極めて低い記録技術

（3）過去の記録の改ざんが難しい記録技術

BC
特徴

 22

ブロックチェーンの特徴（1）
中央管理組織の無い記録技術

中央管理組織による記録：

専門組織がデータの確認・記録・管理を担当

専門組織の運用負担が必要➔データの確認・記録・運用コスト大

1か所で集中管理➔攻撃や故障によるシステム停止のリスク大

1か所に権限集中➔中央管理組織の独断による運用のリスク大

ブロックチェーンによる記録：

参加者が必要な役割を担当

運用負担は参加者が分担➔運用コストも参加者で分担

多数のノードで構成される分散システム➔システム停止のリスク小

公平なルールで運用➔コンセンサス（合意形成）アルゴリズム

参加者による登録データの検証と合意形成方法

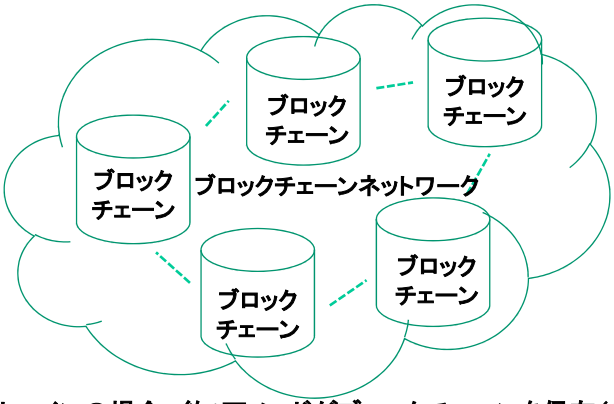
ブロックチェーンへの登録者の選定方法

BC
特徴

 23

ブロックチェーンの特徴（2）
記録消失の危険性が極めて低い記録技術

記録が多数のノードで重複し保管・管理されているため



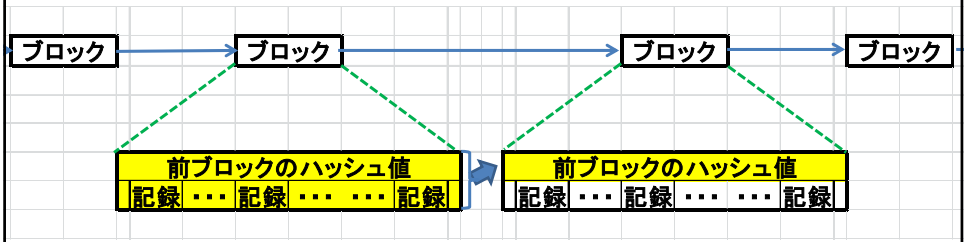
参考：ビットコインの場合、約1万ノードがブロックチェーンを保有（2019年2月時点）
データ量：210GB＋5～10GB/month

BC
特徴

 24

ブロックチェーンの特徴（3）
過去の記録の改ざんが難しい記録技術

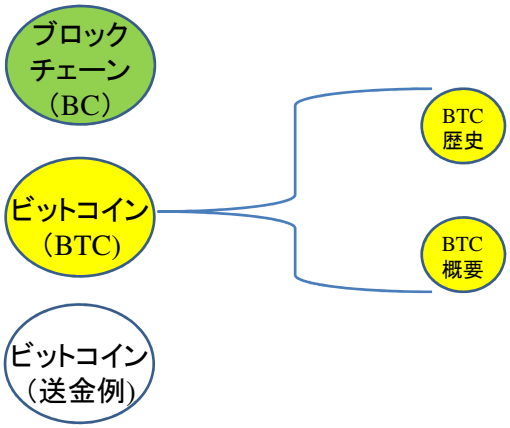
過去の取引・支払等の記録の情報（ハッシュ値）が
以降の記録に反映されているため



ハッシュ値：対象となるデータの特徴を一定の長さのデータに変換したもの。
対象となるデータが1ビットでも変われば、ハッシュ値も変わる。
参考：ビットコインのブロック高は、58321（2019年7月1日頃）

[1]暗号技術の歴史と現代暗号の仕組み

[2]ブロックチェーン(BC)とビットコイン(BTC)



BTC
歴史

ブロックチェーンの例としての
ビットコインブロックチェーンの紹介

ブロックチェーン技術を
最初に具現化したのが暗号資産ビットコイン！

ビットコインの歴史

2008年10月　サトシ・ナカモトがインターネット上で論文発表

2009年1月　ビットコインソフトウェアが開発され運用開始
（その直後に、最初のトランザクションが発行された）

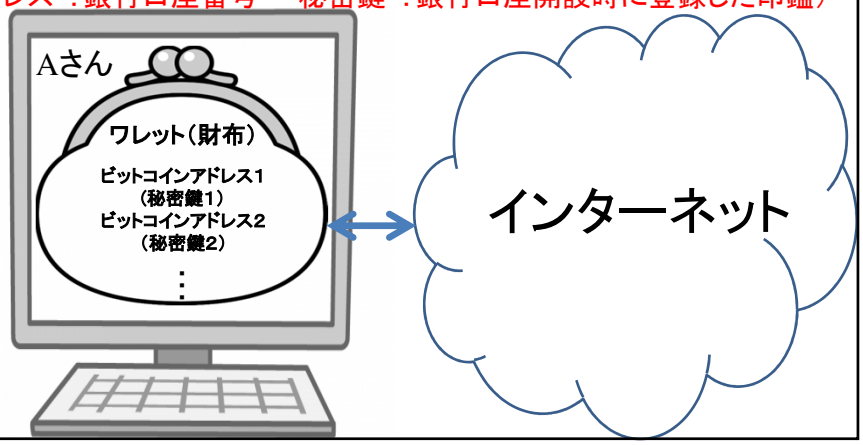
2010年5月22日　現実世界で初めて決済に使用された
「ピザ2枚(約25ドル)＝1万BTC」で取引が成立(1BTC≒0.2円)
1BTC≒107.5万円:2019年9月21日 ➔ ピザ1枚　約54億円！

BTC
概要

ビットコイン概要

 27

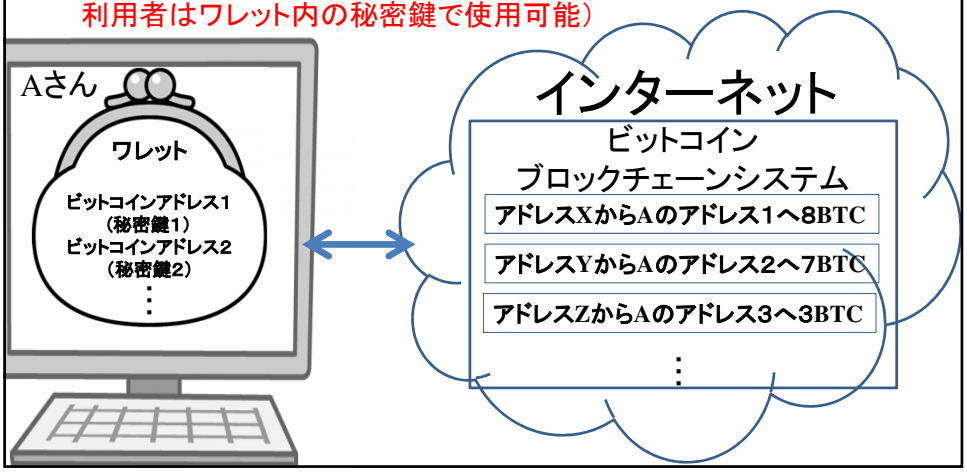
（1）利用者は、複数のビットコインアドレスを保有
　各アドレスに暗号資産（価値）が割り当てられ、アドレスはワレットで管理
　ビットコインアドレスは、利用者の公開鍵から生成されるハッシュ値
　利用者は、ビットコインアドレス（公開鍵）に対応する秘密鍵を保有
（アドレス≒銀行口座番号　秘密鍵≒銀行口座開設時に登録した印鑑）



BTC
概要

 28

（2）資産（BTCの量）は、ビットコインアドレスに割り付けられている
　資産の所有者は、ビットコインアドレスに対応する秘密鍵の保有者
（ビットコインシステム≒銀行
　保有資産はブロックチェーン上に記録、
　利用者はワレット内の秘密鍵で使用可能）

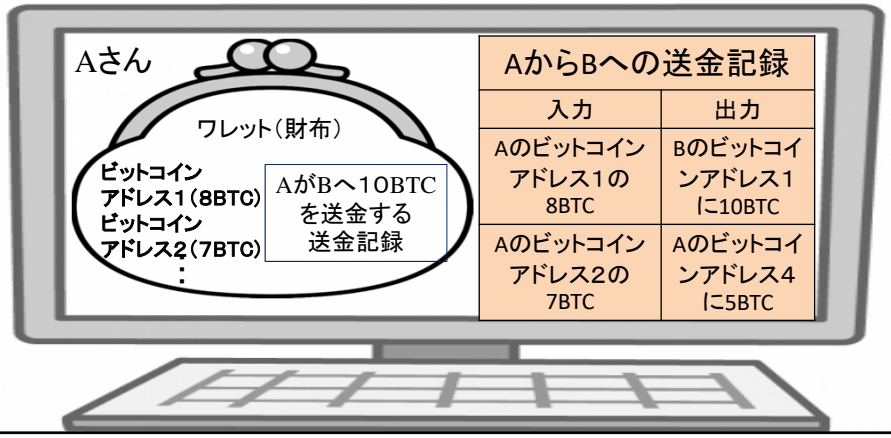


BTC 概要

 29

ビットコイン概要

（3）誰かに資産の一部を渡す場合は、
それに見合うBTCが割り付けられているビットコインアドレスを集め
受取者のビットコインアドレスへの移譲を
送金記録（トランザクション）としてブロックチェーンに登録する

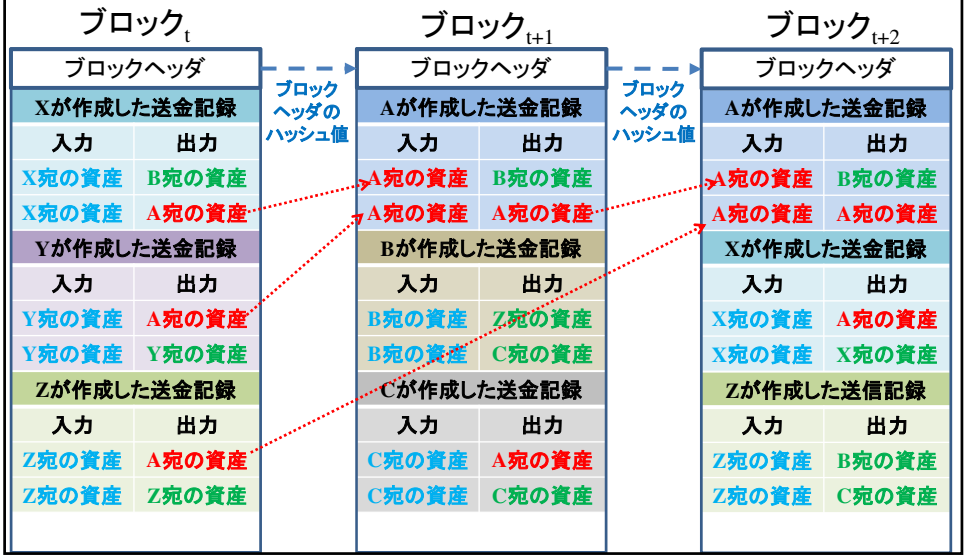


AからBへの送金記録	
入力	出力
Aのビットコイン アドレス1の 8BTC	Bのビットコイ ンアドレス1 に10BTC
Aのビットコイン アドレス2の 7BTC	Aのビットコイ ンアドレス4 に5BTC

BTC 概要

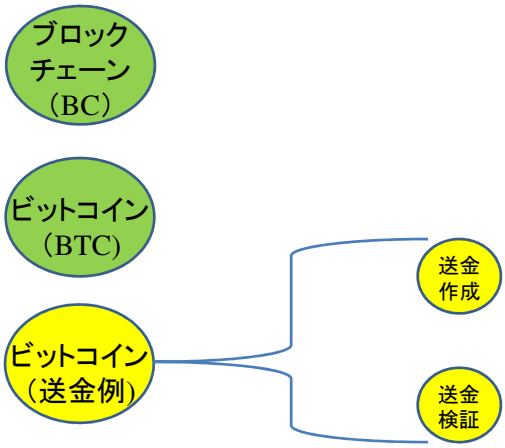
 30

ビットコインブロックチェーンにおける トランザクション（送金記録）例



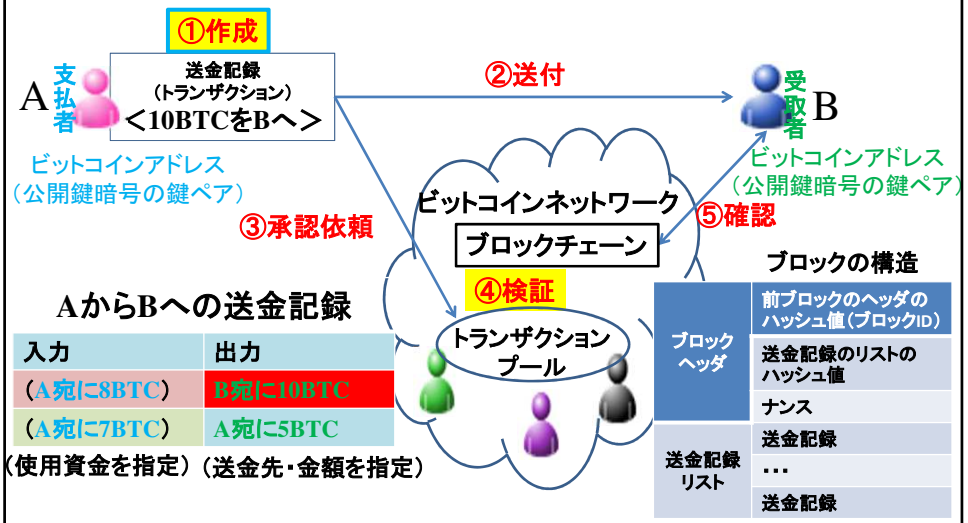
[1]暗号技術の歴史と現代暗号の仕組み

[2]ブロックチェーン(BC)とビットコイン(BTC)



送金作成

AからBへの10BTC送金の流れ



AからBへの送金記録

入力	出力
(A宛に8BTC)	B宛に10BTC
(A宛に7BTC)	A宛に5BTC

(使用資金を指定) (送金先・金額を指定)

受取者(送金先)の指定には、受取者のビットコインアドレスを使用
支払者の使用資金は過去の送金記録内の自分宛の出力の未使用分

送金作成

 33

①支払者Aによるビットコイン送金記録の作成

支払者のビットコインワレット(財布)内で送金記録を作成

利用者A,Bは、あらかじめワレット(財布)を保有
公開鍵暗号方式の楕円暗号の秘密鍵(と公開鍵)、および
公開鍵から生成されるビットコインアドレス(27～34文字)を管理

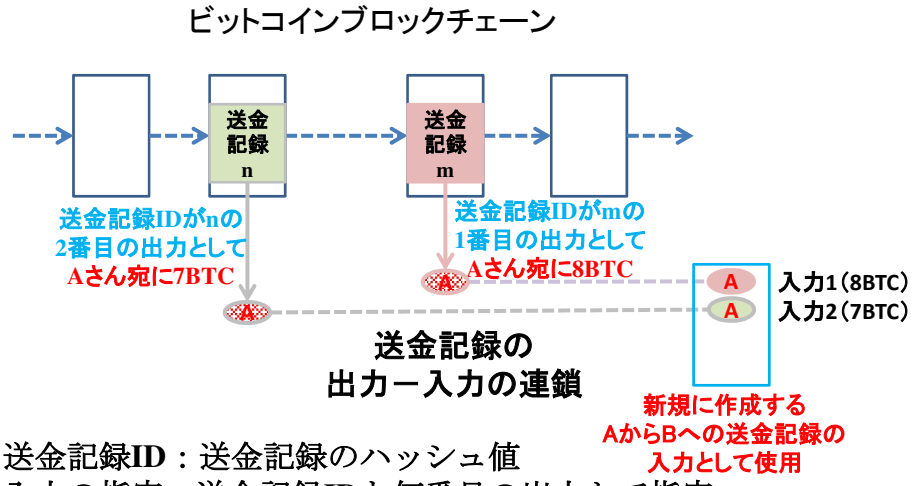
(1) 支払者Aは、送金に使用する資産を確認
受取者として支払者Aのビットコインアドレスが
指定されている(自分宛の)未使用の資産を確認

(2) 支払者Aは、B宛の送金記録を作成
使用する資産、送金先(受取者Bのビットコインアドレス)および
送金額により、送金記録を作成

送金作成

 34

(1)送金に使用する資産を確認



送金記録ID：送金記録のハッシュ値
入力の指定：送金記録IDと何番目の出力かで指定

送金作成

 35

(2)送金記録の作成

XからAへの送金記録(ID=m)

入力	出力
	A宛に8BTC

YからAへの送金記録(ID=n)

入力	出力
	A宛に7BTC

新規に作成する
AからBへの送金記録

入力	出力
(A宛に8BTC)	B宛に10BTC
(A宛に7BTC)	A宛に5BTC

注1：送金記録IDは、
送金記録のハッシュ値
注2：使用資金は、送金記録IDおよび
何番目の出力かにより指定

送金作成

 36

作成された送金記録

使用する送金記録ID=m

入力		出力	
入力元	所有権	出力金額	出力先
		8	Aのアドレス

使用する送金記録ID=n

入力		出力	
入力元	所有権	出力金額	出力先
		7	Aのアドレス

出力先(送金先)は、
新たな受取者(B、A)の公開鍵から生成される
ビットコインアドレス(公開鍵のハッシュ値)で指定

Aが新たに作成する送金記録

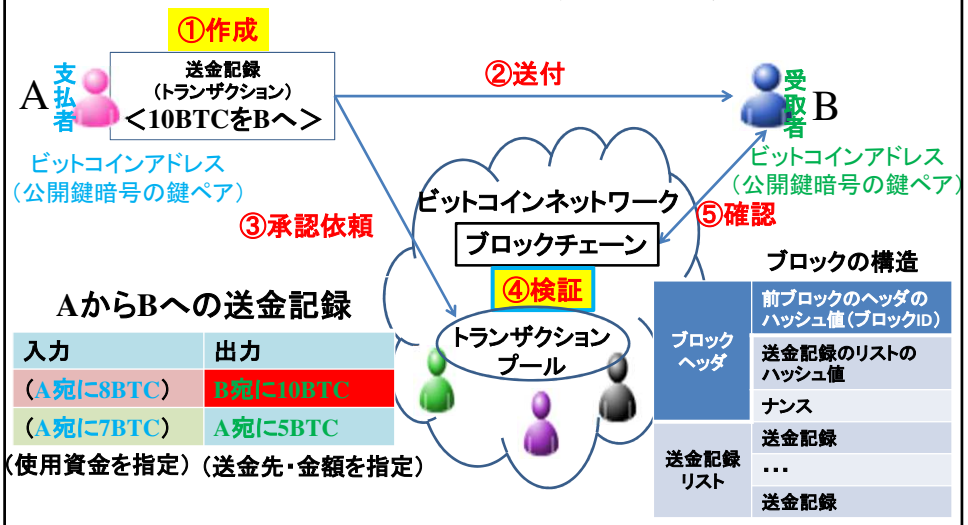
入力		出力	
入力元	所有権	出力金額	出力先
ID=m Out=1	公開鍵(256ビット)、署名	10	B
ID=n Out=2	公開鍵(256ビット)、署名	5	A

署名は所有者だけが保有する秘密鍵
により作成(楕円曲線暗号の利用)

送金検証

 37

AからBへの10BTC送金の流れ



受取者（送金先）の指定には、受取者のビットコインアドレスを使用
支払者の使用資金は過去の送金記録内の自分宛の出力の未使用分

送金検証

 38

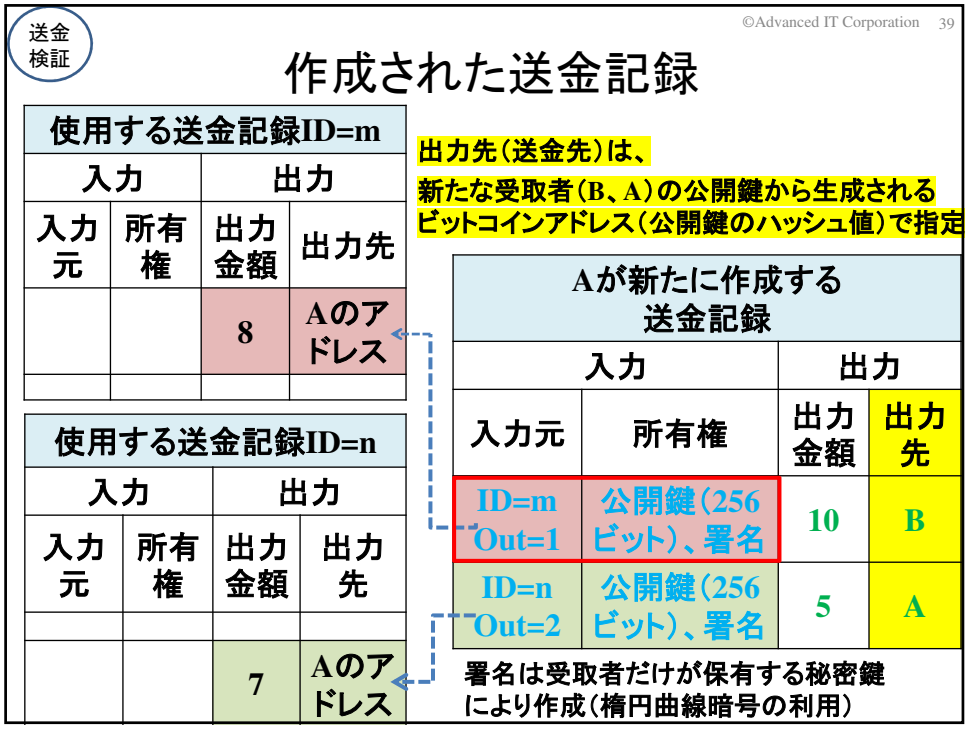
④送金記録の検証（ブロックの構成）

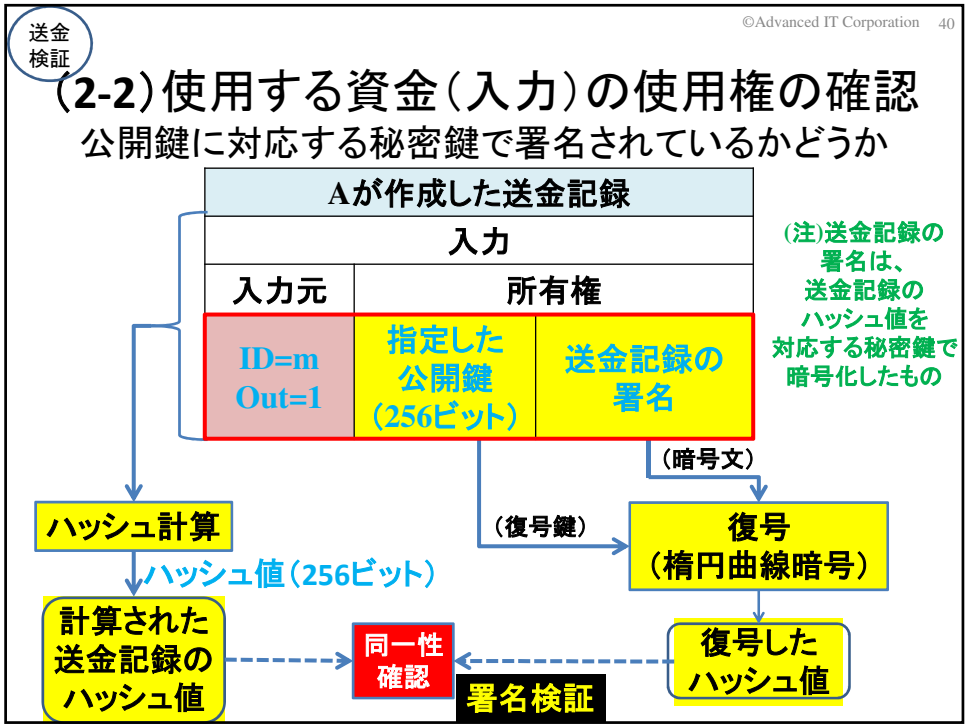
＜トランザクションプール＞
ブロックチェーン未検証の送金記録の集まり

(1)ブロックを構成する送金記録（トランザクション）を選定

(2)選定した送金記録の妥当性を検証（確認）
(2-1)使用する資産（入力）は未使用かどうかの確認
(2-2)使用する資産（入力）の使用権の確認
(2-3)使用する資産（入力）の合計と
提供する資産（出力）の合計の一致の確認

(3) ブロック構成条件を満たす数値（ナンス）の計算

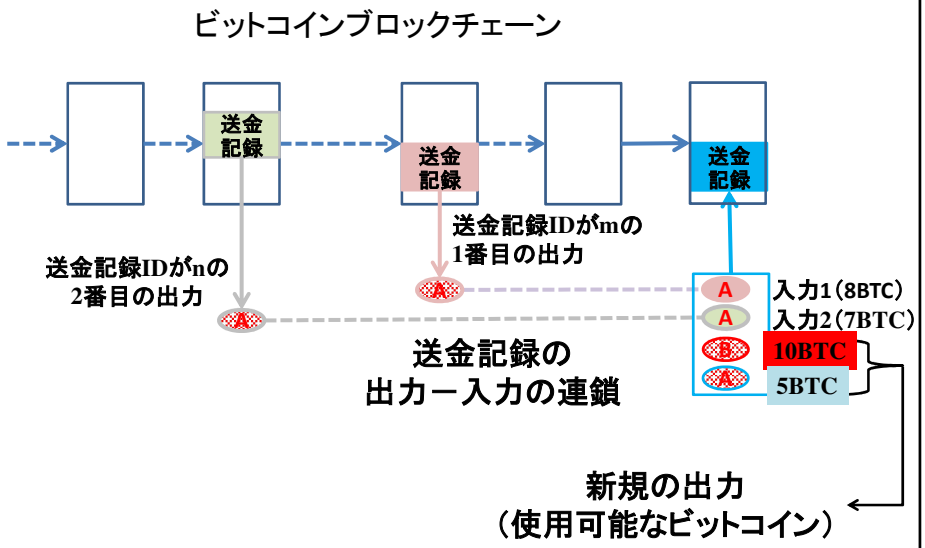

送金検証
©Advanced IT Corporation 39
作成された送金記録
使用する送金記録ID=m
入力
出力
入力元
所有権
出力金額
出力先
8
Aのアドレス
使用する送金記録ID=n
入力
出力
入力元
所有権
出力金額
出力先
7
Aのアドレス
出力先（送金先）は、
新たな受取者（B、A）の公開鍵から生成される
ビットコインアドレス（公開鍵のハッシュ値）で指定
Aが新たに作成する
送金記録
入力
出力
入力元
所有権
出力金額
出力先
ID=m Out=1
公開鍵（256ビット）、署名
10
B
ID=n Out=2
公開鍵（256ビット）、署名
5
A
署名は受取者だけが保有する秘密鍵
により作成（楕円曲線暗号の利用）


送金検証
©Advanced IT Corporation 40
(2-2)使用する資金（入力）の使用権の確認
公開鍵に対応する秘密鍵で署名されているかどうか
Aが作成した送金記録
入力
入力元
所有権
ID=m Out=1
指定した公開鍵（256ビット）
送金記録の署名
(注)送金記録の署名は、送金記録のハッシュ値を対応する秘密鍵で暗号化したもの
（暗号文）
（復号鍵）
ハッシュ計算
ハッシュ値（256ビット）
復号（楕円曲線暗号）
計算された送金記録のハッシュ値
同一性確認
復号したハッシュ値
署名検証

送金検証

 41

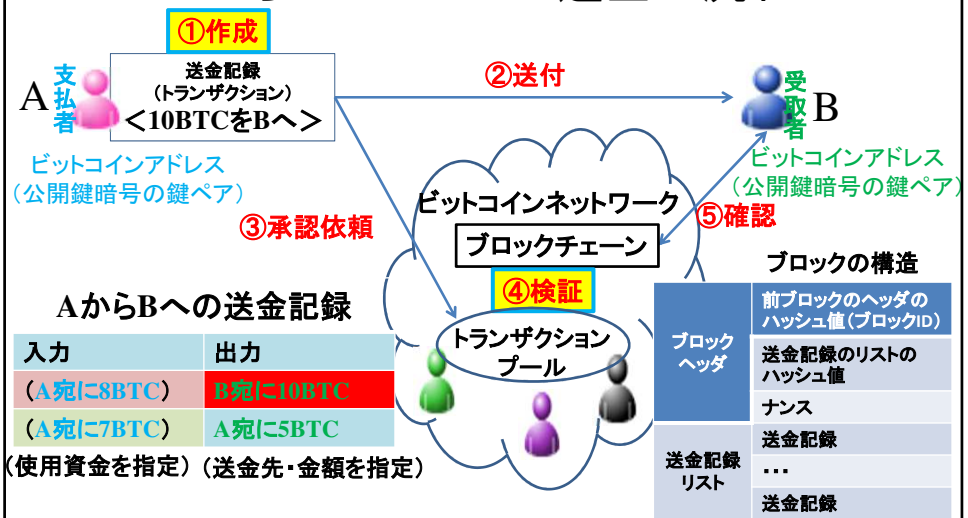
送金記録のブロックチェーンへの登録



送金検証

 42

AからBへの10BTC送金の流れ

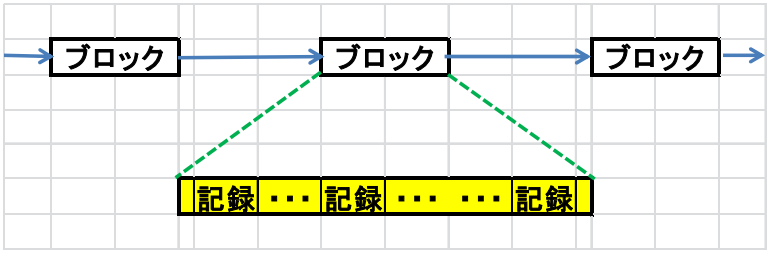


受取者（送金先）の指定には、受取者のビットコインアドレスを使用
支払者の使用資金は過去の送金記録内の自分宛の出力の未使用分

まとめ

ブロックチェーンとビットコイン

取引・支払等の記録を（複数）格納しているブロックの連鎖



（1）中央管理組織の無い記録技術

➔ 検証者による送金記録のブロックチェーンへの登録

（2）記録消失の危険性が極めて低い記録技術

➔ 1万を超えるノード（コンピュータ）による重複管理

（3）過去の記録の改ざんが難しい記録技術

➔ 送金記録の改ざんは

以降のブロック全てを改ざんしないと成功しない

まとめ

おわりに

（1）暗号技術

①暗号は紛争を優位に進めるための道具として活用

暗号に関する熾烈な戦いの勝敗が、

紛争の歴史、人類・社会の歴史を形作ってきた！

②コンピュータ/ネットワークの発展により、

産業活動・生活活動での活用拡大

暗号技術の活用により便利なサービスが次々と社会へ

（2）ブロックチェーン技術

①ブロックチェーン技術も暗号技術の活用により誕生し発展

②暗号資産（仮想通貨）は社会にインパクトを与えた

最初のブロックチェーン技術の応用

③ブロックチェーン技術は、第2のインターネット

と言われるほど、今後の発展が期待されている技術

終