2021年6月26日

暗号資産

暗号資産って一体何なの？

儲かるの？

危なくないの？

仮想通貨

暗号資産

分散型金融、ＤｅＦｉ（ディーファイ）Decentralized Finance

ウォレット

ブロックチェーン

マイニング

仮想通貨＝暗号資産

改正資金決済法で名称を変更

2020年5月1日施行

Virtual Currency ⇒ Crypt Asset

暗号資産の種類と規模

	名前		1単位の値段	市場規模
1	Bitcoin		￥ 3,761,174	￥71,992,675,153,151
2	Ethereum		￥ 228,891	￥27,180,079,994,025
3	Dogecoin		￥ 32	￥ 4,220,002,874,256
4	Bitcoin Cash		￥ 62,851	￥ 1,164,326,921,141
5	Litecoin		￥ 16,474	￥ 1,083,571,395,837
			.	
			.	
2497	Wild Beast Block		￥ 3	￥ 548,000
2503	Save and Gain		￥ 0.14	￥ 425,074
5268	Dogey-Inu		￥ 0.000001059	NA

出典：CoinMarketCap

ビットコイン BTC

3,850,583円 ▼-2.55%

最終更新：2021年5月24日 15時42分3秒

24時間始値	3,951,345 円
24時間高値	3,979,764 円
24時間安値	3,366,471 円
24時間変動値	▼-100,782.14 円
時価総額	720,704 億円
循環サプライ	18,716,769BTC

(I)　暗号資産とは

サトシ　ナカモト　？

多分、何人かの団体

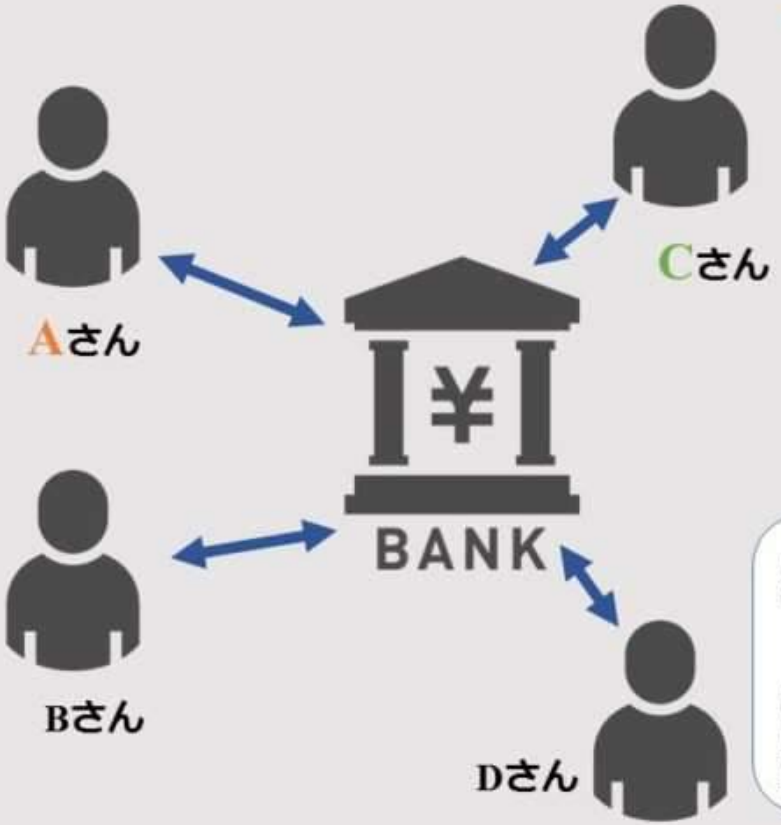
サトシ　ナカモト　2008年10月　「暗号関係ネットページ」に論文投稿

Bitcoin: A Peer-to-Peer Electronic Cash System

Peer-to-Peer （P2P）　「対等な2者間」による電子送金システム、言い換えると

国家や銀行などの第三者機関、**中央管理者のいない**、個人間で直接決済できる電子送金システム

中央集権制とは？



Aさんから Cさんに送金する場合

A→**銀行**

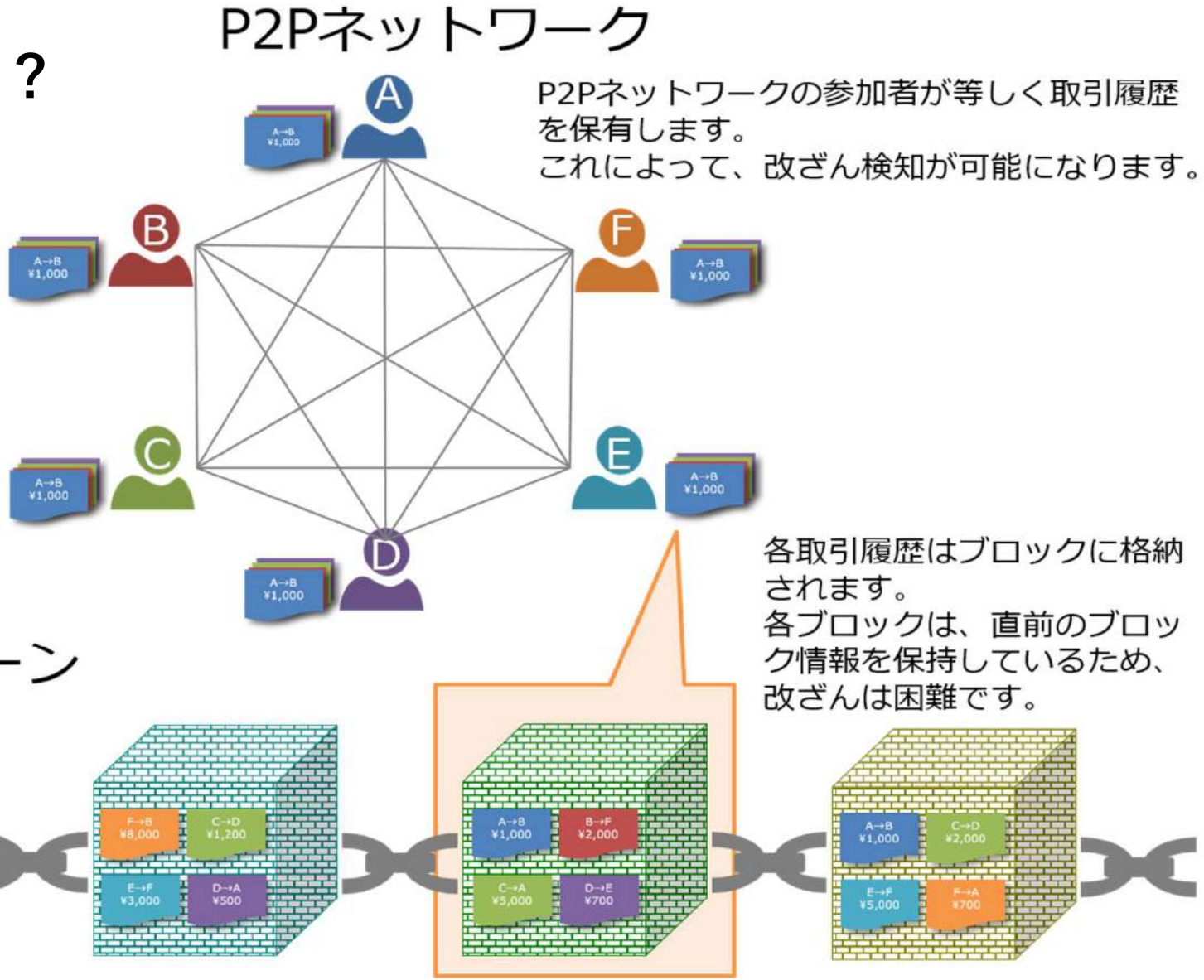
からの

銀行→C

銀行が仲介するので手数料がかかる

銀行のデータが吹っ飛んだら
控えめに言ってもやばい

分散型金融とは？

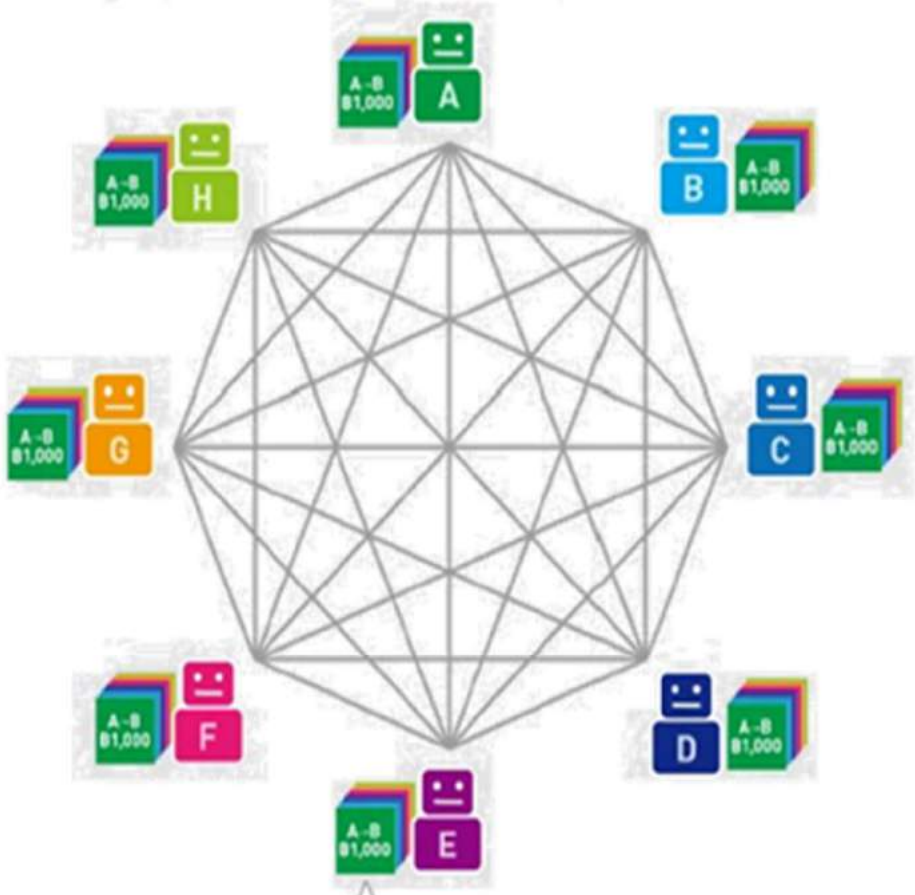

P2Pネットワーク
P2Pネットワークの参加者が等しく取引履歴を保有します。
これによって、改ざん検知が可能になります。
A
B
C
D
E
F
A→B ¥1,000
各取引履歴はブロックに格納されます。
各ブロックは、直前のブロック情報を保持しているため、改ざんは困難です。
ブロックチェーン
C→A ¥5,000
A→F ¥2,000
A→B ¥5,000
F→A ¥4,000
F→B ¥8,000
C→D ¥1,200
E→F ¥3,000
D→A ¥500
A→B ¥1,000
B→F ¥2,000
C→A ¥5,000
D→E ¥700
A→B ¥1,000
C→D ¥2,000
E→F ¥5,000
F→A ¥700

従来の取引きと信頼性担保システム

第三者機関が取引履歴を管理し、信頼性を担保する

ブロックチェーンでの取引きと信頼性担保システム

ずべての取引履歴を全員で共有し、信頼性を担保する



誰でも参加できる公開された取引システムで個人二者間の決済ができる、
なんて本当に可能でしょうか？

P2P決済を可能にした三つの新技術

1. 「**暗号技術**」　　⇒　**Crypt Asset（暗号資産）と呼ばれる理由**

2. 「**ブロックチェーン**」と呼ばれる、**取引元帳システム**

3. 「**マイニング**」とよばれる、**取引検証システム**

① **暗号技術**　⇒ビットコインの「暗号を使った」送金システム

ウォレット　（財布）以下三つを格納するデータベース（送受信に必要）

1. 秘密鍵　⇒送金内容を「暗号化する」数字列
（1e99423a4ed27608a・・・・・・64個）
2. 公開鍵　⇒暗号化された送金内容を「復号化する」数字列
（03F028892BAD7E・・・・・・・66個）
3. アドレス　⇒銀行でいう所の口座番号に当たる文字数字列
（1DoRian4RoXcnBv9・・・・・・・34個）

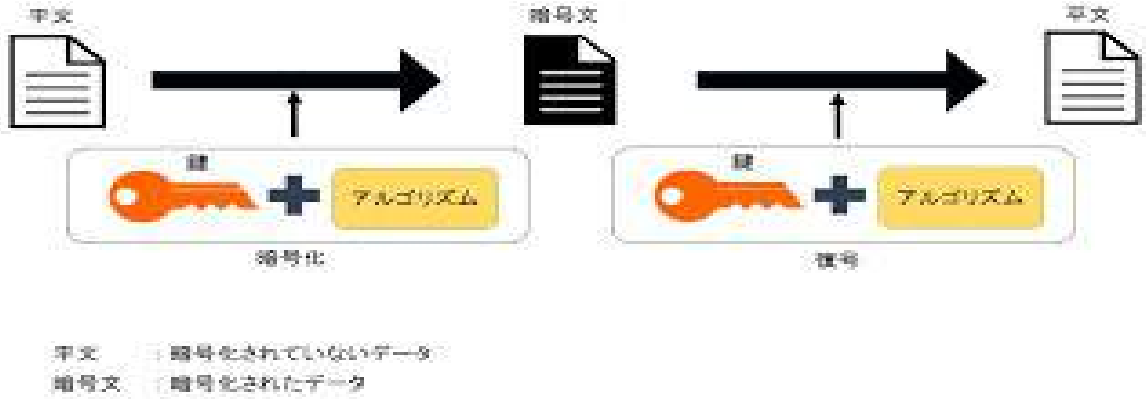
①　暗号技術
2018年コインチェック事件

「**秘密鍵**」を盗まれて、
会社から570億円盗まれた！

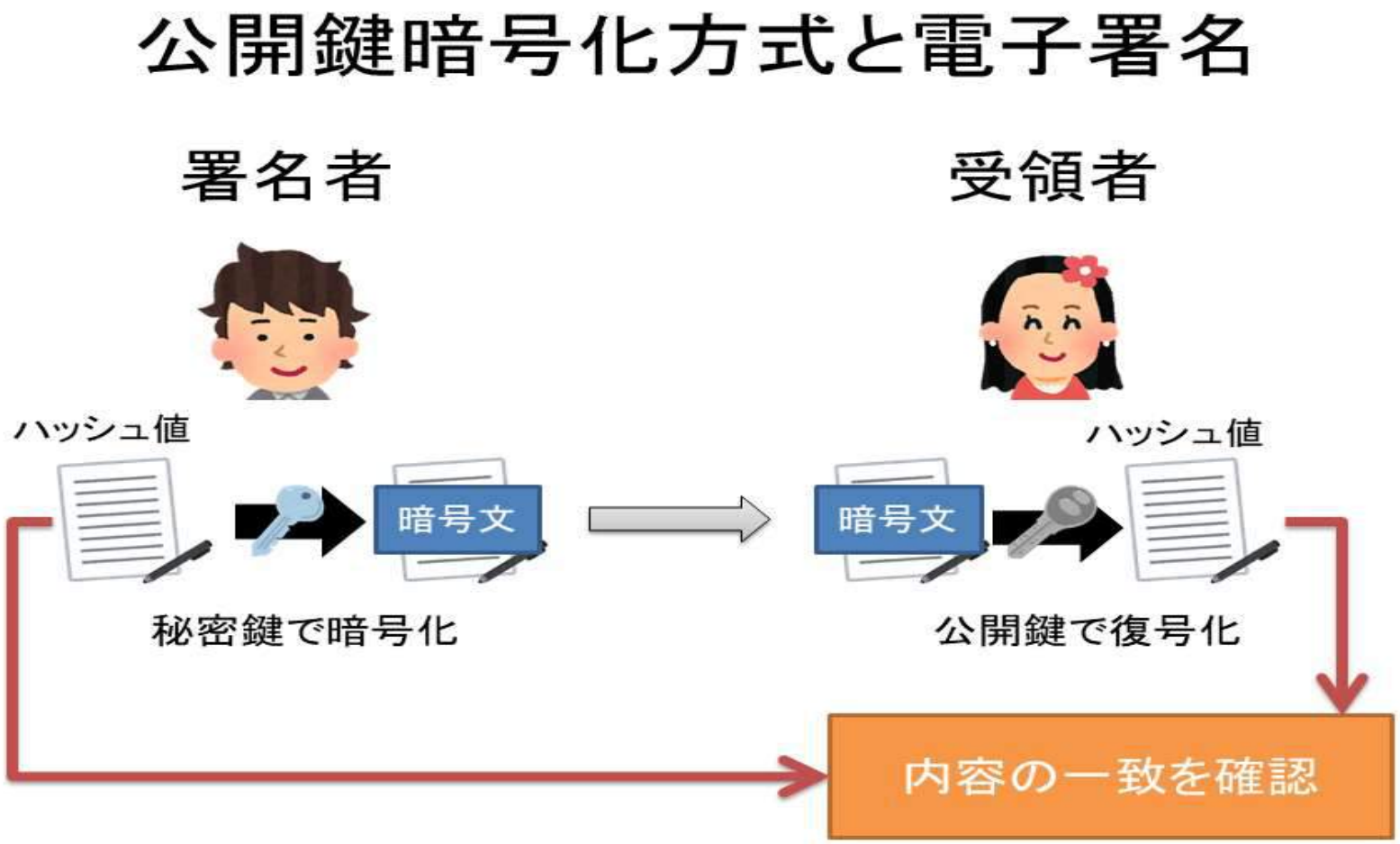
①　暗号技術

秘密鍵から一方方向関数を使って公開鍵を作る。 **公開鍵**から一方方向関数を使って**アドレス**を作る。

秘密鍵Aで暗号化する。　　公開鍵Aで復号化する。Aによる送金と本人確認できる。

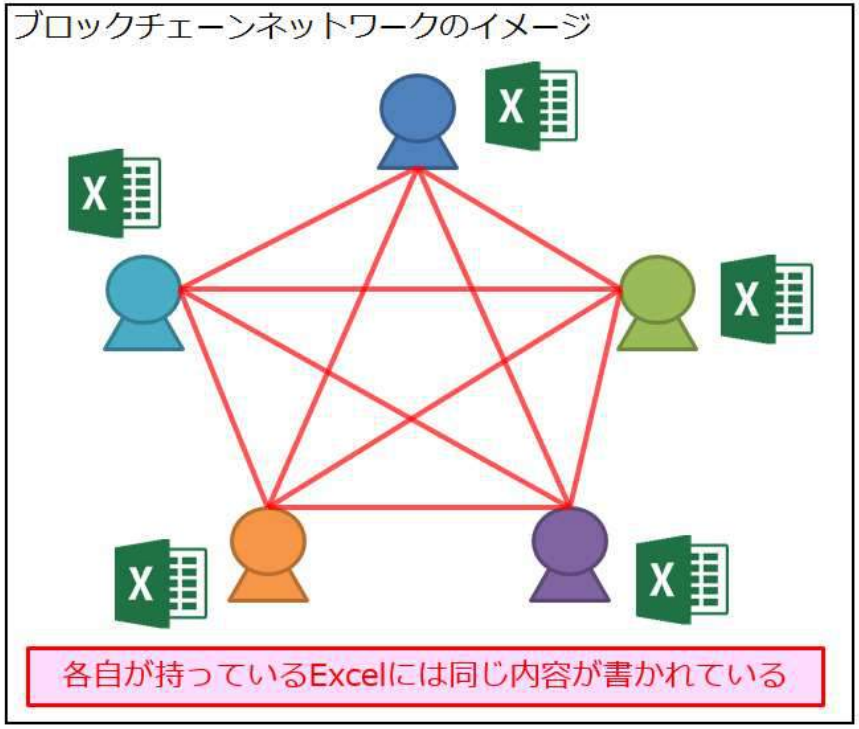


① **暗号技術**


公開鍵暗号化方式と電子署名
署名者
受領者
ハッシュ値
暗号文
秘密鍵で暗号化
ハッシュ値
暗号文
公開鍵で復号化
内容の一致を確認

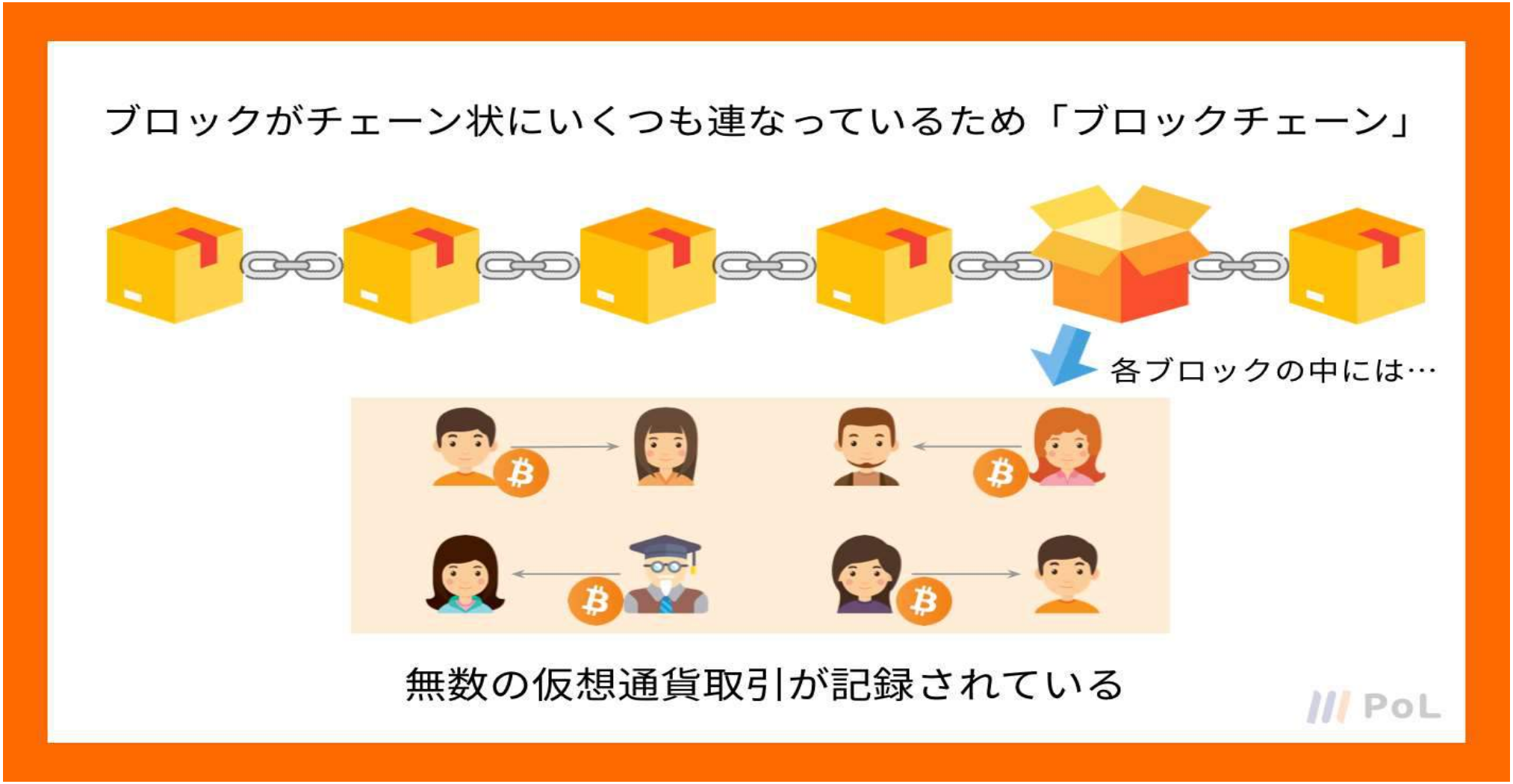
2. 「**ブロックチェーン**」と呼ばれる、**取引元帳システム**

分散型台帳システム　　ノードの皆が持っている取引台帳に全取引が記録されている。



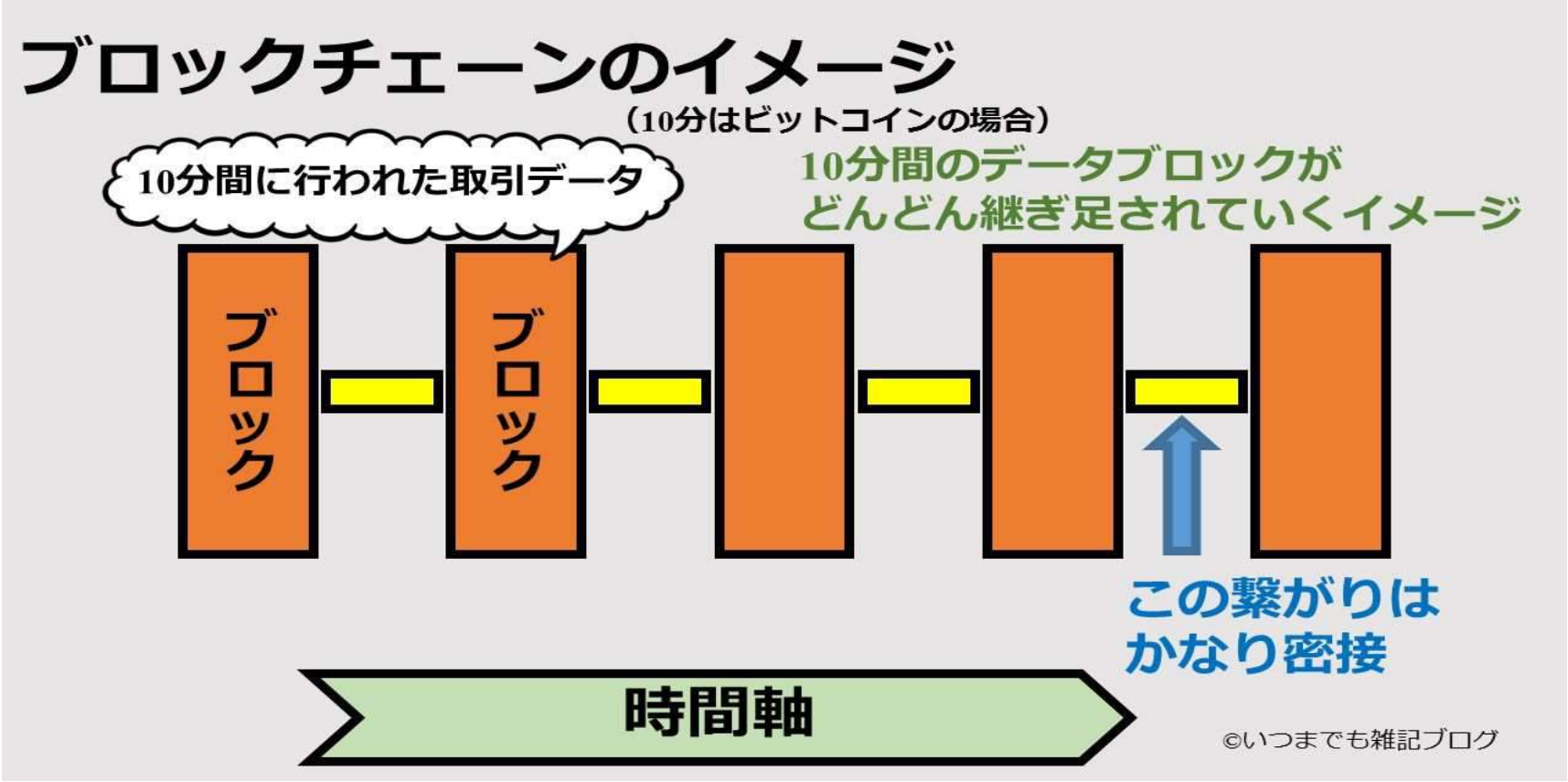
Distributed Ledger System

2. 「**ブロックチェーン**」と呼ばれる、**取引元帳システム**

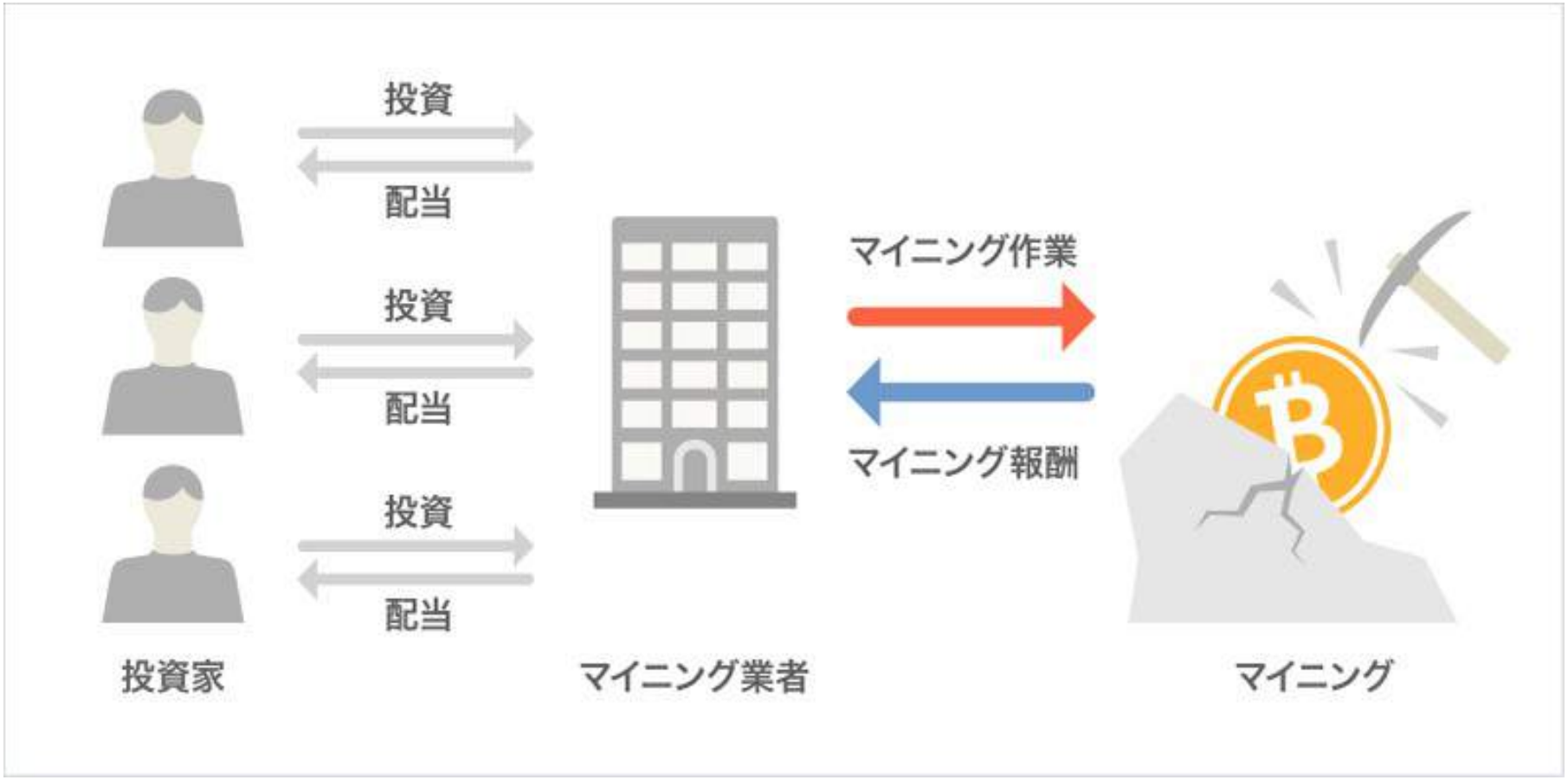


2. 「**ブロックチェーン**」と呼ばれる、**取引元帳システム**

取引台帳の中身⇒マイニングで承認されたブロックが繋がって行く。



3. 「**マイニング**」とよばれる、**取引検証システム**



3.　「マイニング」とよばれる、**取引検証システム**

「マイナー」（採掘者）が採掘に成功すると一定の報酬が得られるという仕組み。

マイニングに使われる、「**ハッシュ関数**」とは？

任意の長さの文字、数字、文章を入力 ⇒**ハッシュ関数**　⇒一定の長さのデータを出力する

おいしいリンゴを食べた。　⇒ハッシュ関数　⇒36

おいしいバナナを食べた。　⇒ハッシュ関数　⇒55

うまいリンゴを食べた。　⇒ハッシュ関数　⇒89

数字から元の文章に戻すことは出来ません。一方向。

3. 「**マイニング**」とよばれる、**取引検証システム**

① 直前のブロックのハッシュ値

② 未処理の送金依頼をハッシュ化したハッシュ値

③ ナンス（任意の数字）

④

更にハッシュ化したハッシュ値
（64桁の英数字列）を求める。

①と②は固定、
③が変わるとハッシュ値が変わる。

③に代入　26958743654・・・・・　⇒ 56v9854R k 2P・・・・（64桁）

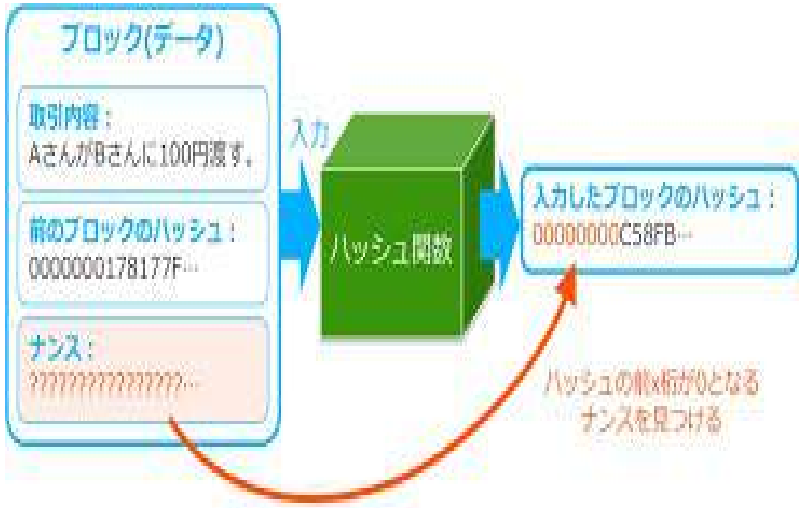
③に代入　89654523608・・・・・　⇒ 09865 c 56B9a・・・・（64桁）

③に代入　59621463914・・・・・　⇒ 0000000005a6・・・・（64桁）
先頭に19桁の0が並んだ！やったー！

3. 「**マイニング**」とよばれる、**取引検証システム**

一番早く見つけた人は6.25ビットコインの報酬が貰える。

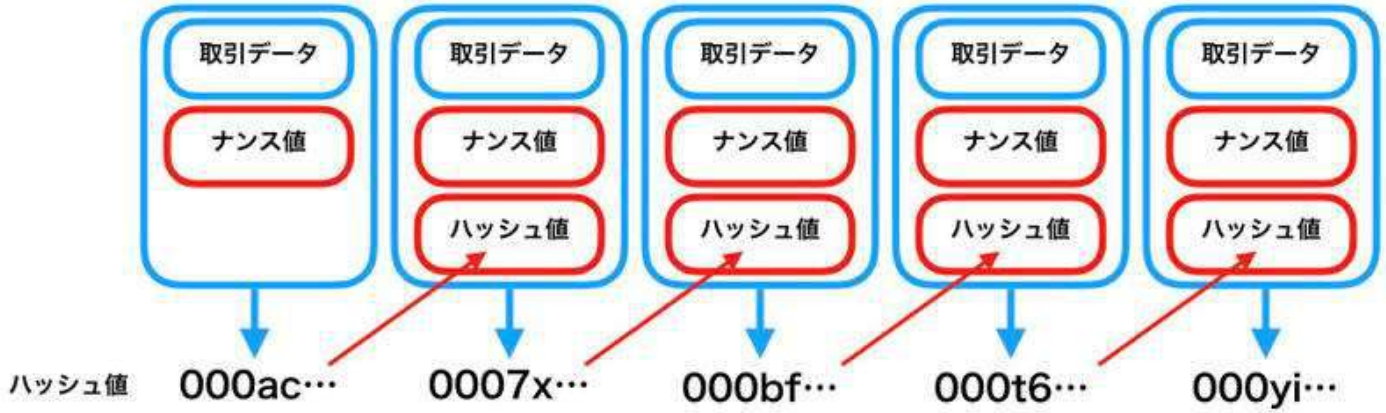
新しいブロックが出来る。（10分毎に1ブロック）



3.　「マイニング」とよばれる、**取引検証システム**

これがマイニングの為の工場です。答えとなるハッシュ値を求めるために計算を繰り返します。

3. 「**マイニング**」とよばれる、**取引検証システム**



改ざんしようとして、どこかの取引を書き換えると、そのブロックのハッシュ値が変わり、
その前のハッシュ値を書き換えなければならない。次のハッシュ値も変えなくてはならない。

その前のハッシュ値が変わると、またその前のハッシュ値を変えなくてはならない。
その次のハッシュ値を変えると、又次のハッシュ値を変えなければならない。

マイニングで儲ける方がまし、となる。従って改ざんは不可能。

（1）ビットコインは「対等な二者間の送金システム」
そして、中央管理者のいない「分散型金融システム」

（2）三つの新技術で改ざんできない公開取引元帳システムを可能にしている。
①暗号　②ブロックチェーン　③マイニング

① 公開されたシステムなので、送信者と受信者の間は「秘密鍵」「公開鍵」などの暗号で本人確認をする。

② 確認された送金情報は、ブロックチェーンという公開された元帳に記入される。
一つのブロックには約2,000件の取引が格納され、10分毎に新しいブロックがつながれてゆく。一つのブロックを固める為に、マイニングという作業が行われる。

③ マイニングは、1）前のブロックの「ハッシュ値」と2）新たな数百～2,000件の取引を「ハッシュ化」したもの、と3）「任意の数字」の三つを再びハッシュ化。

出力されるハッシュ値で、先頭に0が19個並ぶ64桁の英数字（答え）を求める。
最初に答えを得る「任意の数字」を見つけた人にビットコインが新規発行される。
この作業で今までのブロックと新たなブロックが繋がり、
過去の取引の改ざんが不可能になる。

(II) 暗号資産の根源的価値

10年前はタダ同然　⇒　1ビットコインが4百万円

どうしてそんな高値でも買うの？　そんなに価値があるの？

三つの特徴

①　匿名性が高い	送金人、受取人ともにアドレスという記号
②　個人間で直接決済ができる	個人から個人へ直接スマホやPCで送金
③　国際間決済ができる。	国境を越えた送金が瞬時にできる。

最も利用されそうな使途　**資本逃避やマネーロンダリング**

(II) 暗号資産の根源的価値

例えば、中国の政治家の賄賂。　銀行送金は出来ない。アメリカの親族に暗号資産で送る。

2013年　キプロス経済危機　ロシアマネーが国外逃避

その時は1BTCが5ドルから250ドルへ上昇した。（500円から2万5千円へ50倍の値上がり）

2015年　中国人民元の急落。資本逃避が起こった。

2015年には300ドルだったが2017年には1万9千ドルへ。（3万円から190万円へ63倍）

2017年、中国は暗号資産交換所を禁止。

(II) 暗号資産の根源的価値

FATF(Financial Action Task Force) 国際活動作業部会

マネーロンダリングの防止を目的とした政府間組織

犯罪にビットコインが使われた最近の事例

「コロニアル・パイプライン」のランサムウエア攻撃

身代金をビットコインで要求、身代金は支払われた。ところが・・・・。

FBI関連の秘密チームが犯人の「秘密鍵」をハッキングし、身代金を回収した。

(II) 暗号資産の根源的価値

アンダーグラウンド的な需要に加えて、新しい投資対象としての需要も。

1）今年2月、イーロン・マスク氏（テスラ社）がビットコインに15億ドル投資することを発表。

2）欧米の投資家や金融機関の暗号資産投資を開始

3）6月9日　エルサルバドルがビットコインを法定通貨に決定

(II) 暗号資産の根源的価値

ビットコインは2140年に発行が停止されるようにプログラムされている。

暗号資産の根源的価値と新たな投資資金の流入、デフレ的な構造からみると、
長期的にはまだ上昇すると見る人が多い。

ある人は10万ドルとか14万ドルと予想。（10〜15百万円）

リスク要因は政府の規制。

暗号資産交換所で口座登録すれば5〜6千円から購入できる。

今後の見通し　No Guaranteeです！

ご清聴ありがとうございました。