Blockchain の仕組み

なぜ Blockchain はどのような仕組みで暗号通貨の基盤技術たり得るのか

2023/09/25

並河秀憲（なびか）

Blockchain 技術の最初の応用が Bitcoin だった

Blockchain の定義

「Blockchain は、電子的な台帳であり、暗号技術を使ってリンクされた Block と呼ばれるレコードの増大するリストの事を指している。2 つの当事者間の取引を効率的かつ検証可能で恒久的な方法で記録することができるオープンな分散型台帳である」Wikipedia

「ビザンチン障害[1]を含む不特定多数の Node を用い、時間の経過とともにその時点の合意が覆る確率が 0 へ収束するプロトコル、またはその実装を Blockchain と呼ぶ」日本 Blockchain 協会（定義 1）

「電子署名と Hash ポインタを使用し改竄検出が容易な Data 構造を持ち、且つ、当該 Data を Network 上に分散する多数の Node に保持させることで、高可用性及び Data 同一性等を実現する技術を広義の Blockchain と呼ぶ」日本 Blockchain 協会（定義 2）

[1] ビザンチン帝国を包囲する敵国 9 人の将軍が攻撃計画について攻撃か撤退を多数決で決定する際に、必ず全将軍一致で攻撃をしないと計画は成功しないとした場合に、裏切り者の将軍（不正な取引）が 1 人でもいたら絶対に攻撃は成功しない。この状況をビザンチン障害という。

Blockchain と Crypto Currency

Bitcoin はその名の通り Blockchain を用いて Internet 上で**貨幣**（Coin）＝ **Crypto Currency** を産み出すことが企図された

Digital Gold と説明されることも多い

- では貨幣とは何か？
- なぜ Blockchain が貨幣となり得るのか？
- Blockchain はどのように活用できるか？

貨幣とは何か

貨幣についての簡潔な説明

「物やサービスとの交換に用いられる「お金」を、経済用語では貨幣、または通貨と呼ぶ。貨幣とは、経済学上は、価値の尺度、交換の媒介、価値の蓄蔵の機能[2]を持ったものの事である」（Wikipedia）

なぜ Bitcoin は Digital Gold と言われるのか

・金の**希少性**、**有限性**、**不変性**が、普遍的な価値を求められる貨幣としての信用をもたらした

・Bitcoin は Digital の世界に金を生み出す試みである

[2] この機能は貨幣に対する信用によってもたらされるが「貨幣に価値があるのは、皆が価値があると信じているからである、なぜ皆は価値があると信じているかは、皆が価値があると信じているからである」（『貨幣論』岩井克人）

Bitcoin に金の性質を付与する

【希少性・有限性】地球上に存在する金は希少かつ有限である

・Bitcoin の最大供給量は 2,100 万枚しかない

・2023 年 5 月 6 日時点で 1,940 万枚弱供給されており、あと 160 万枚 Mining（採掘）されると新たな供給はなくなる

・Mining 報酬は 21 万ブロック毎（約 4 年毎、次回は 2024 年 4 月に予定）に半減する

・簡単に複製できる電子情報の複製を阻止し、個々の Transaction の唯一性をどう担保すればよいか

【不変性】金の性質はたいへん安定しており錆びず腐敗しない

・Bitcoin は物ではなく情報なので検証と承認によって、その情報を揺るぎないものとする

・その上できわめて高い改竄耐性を備えることが出来れば、その不変性は金そのものと同じ信用を生じさせ貨幣として流通する筈である

物理的に存在しないお金

・2022 年末の時点で流通している紙幣は 125.1 兆円、185.9 億枚

・2022 年 9 月末の個人の金融資産 2,005 兆円、このうち現金・預金=「お金」は 1,082.7 兆円（54％）

・したがって個人が持っているはずのお金のうち、物理的に存在し流通している紙幣は 12％弱しかない

では物理的に存在しないお金が

どうやって存在すると言い得、現実に流通しているのか？

・「Bitcoin は Digital の世界に金を生み出す試み」だが物理的な金そのものを作ることは出来ない

・金そのものを作ることは出来ないが、それが誰から誰の手に移動したかという正確な記録 ＝Footprint があれば、通帳の残高から送金、支払いするように利用できるのではないか

お金は

① 金貨や紙幣のような偽造、**改竄がきわめて困難で物理的に流通させることの出来るもの**、でも

② その金額がいつから誰々の元に確かにある、という**記録の形でも存在できる**のである

Database ＞ 分散型台帳 ＞ Blockchain

・ある物事の基礎的な事実を記録しておく帳簿、一般にある事柄のもととなる原簿を台帳という

・銀行に口座を持っていればその Account 毎に通帳が発行される

・通帳は台帳の当該 Account について記載された部分について**管理者が発行**する謄本[3]である

いかにして信頼できる台帳を保守するか？

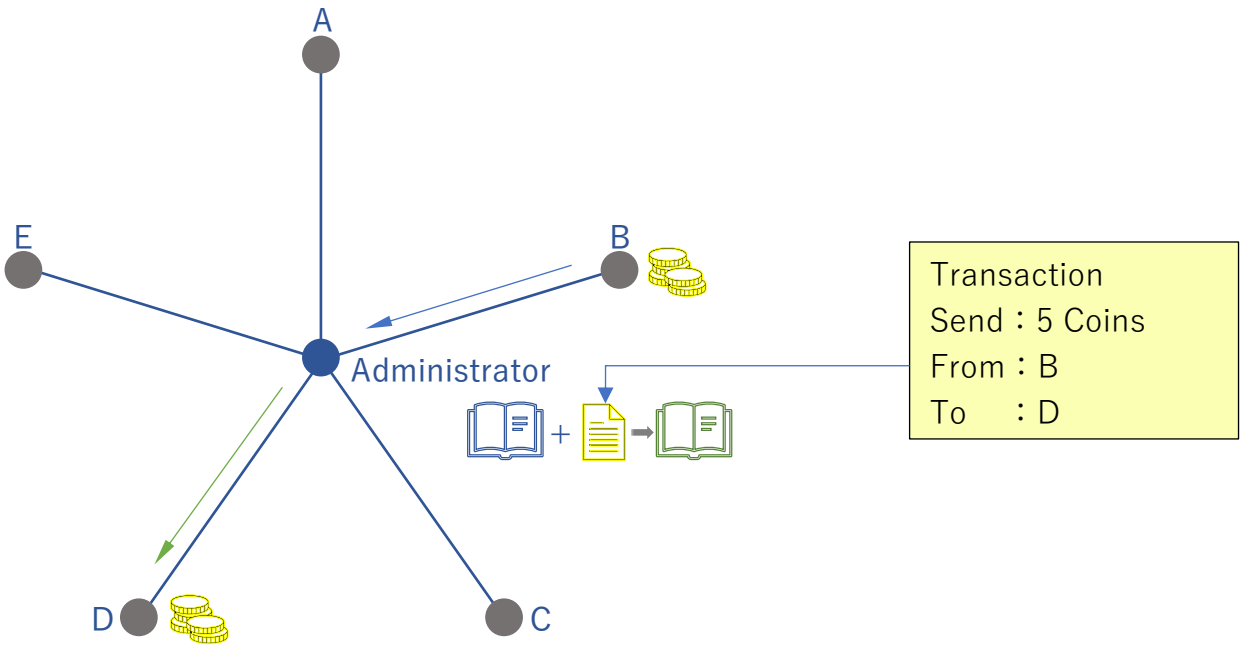
[3] 謄本とは元になる文書の真のコピーであるという裏書または証明が記載された元になる文書のコピー。元になる文書が本物であることを証明するものではなく、元になる文書の真のコピーであることを証明するだけである。

【中央集権型台帳：Database】

・改竄に対応するため銀行は独自の台帳 ＝ Database を管理し、**単独の権限**が、Data の入力、**有効性の保証**、維持といったすべての側面に対して全面的な支配力をもつ

・取引履歴の確定や処理順序などは信頼された管理者によって**中央集権的**に管理・決定されている

・Data の整理や統合、活用のために、管理者によって与えられた**権限に依存**して Data の読み取りや書き込み、更新、削除などが行える

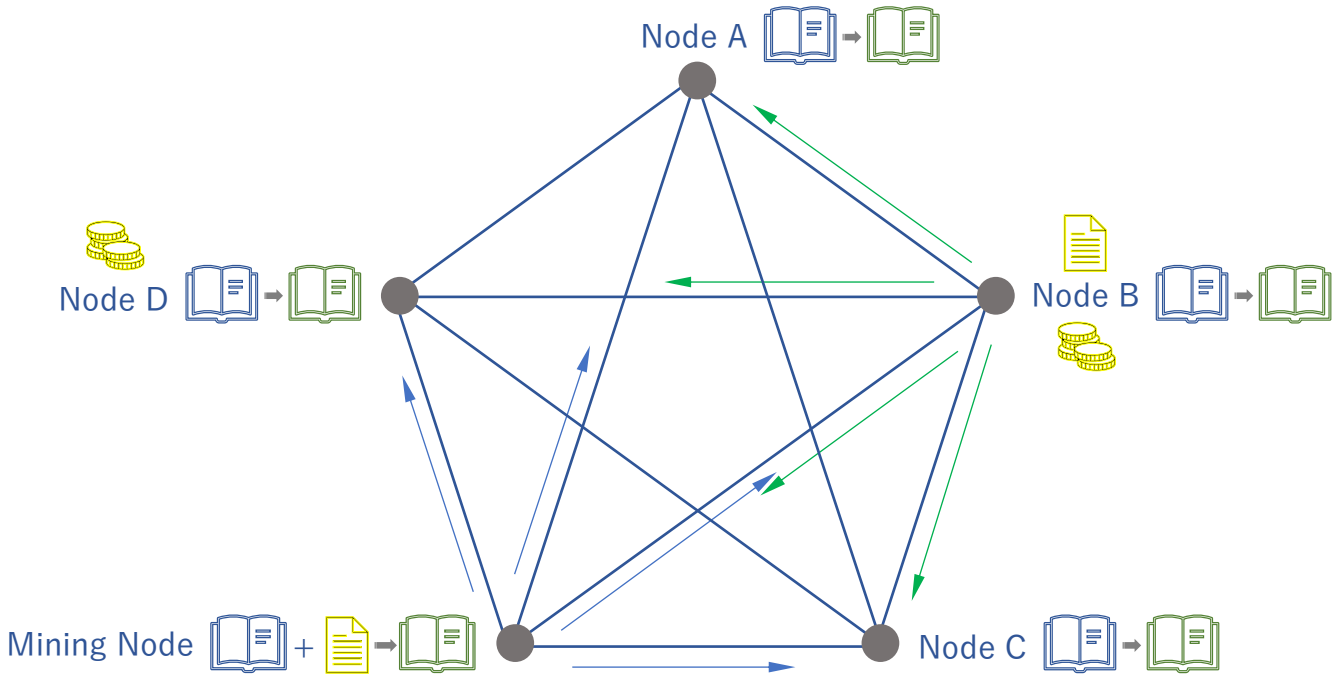


【分散型台帳：Blockchain】

・Blockchain とは基本的に Data の記録と保持に重点を置いた **Database** の一種

・Blockchain は、Network を構成するすべての Node が、台帳の複製を**自律的**に取得または構築できる**分散型**（非集中型）**台帳**の一種であり中央集権的、特権的な Node を必要としない

・Data が記録された Block は P2P[4]（Peer to Peer）Network 上の参加者（Node）全体に分散し検証される



[4] 個々の Computer などの端末（Node）を対等かつ直接につなぎ、全体として Network を構築する通信方式。これに対し、個々の端末（Client）が中央の Server を経由してつながる仕組みが Client・Server 型通信。Blockchain は中央に Server を置かず、管理者も存在しない P2P 技術を利用しデータを分散している。

公開鍵暗号方式の概要

・各 Node は他者の Node の取引情報を含めた全情報を、Blockchain という分散型台帳として所持・管理している

・しかしこのままでは、他者に自分の取引情報・内容が完全に公開されてしまう

・そこで、取引情報の秘匿性を担保するために Blockchain では公開鍵暗号方式という Security が採用されている

・通常の Security System においては、User は一つの鍵、すなわち共通鍵暗号方式を用いる。例えば Online Shop で商品を購入するときも、User は自らの Account に Login する際に Password ひとつで認証する。これが共通鍵である。これは施錠・開錠に同一の鍵を用いることに相当する

・これに対し公開鍵暗号方式では、User は「公開鍵・秘密鍵」の二つの鍵を所有する

【公開鍵】

・情報を暗号化する際に用いられる鍵。施錠に相当する

・公開鍵は他の Node に公開され、他の Node は「誰が情報を暗号化したのか」を把握することができる

【秘密鍵】

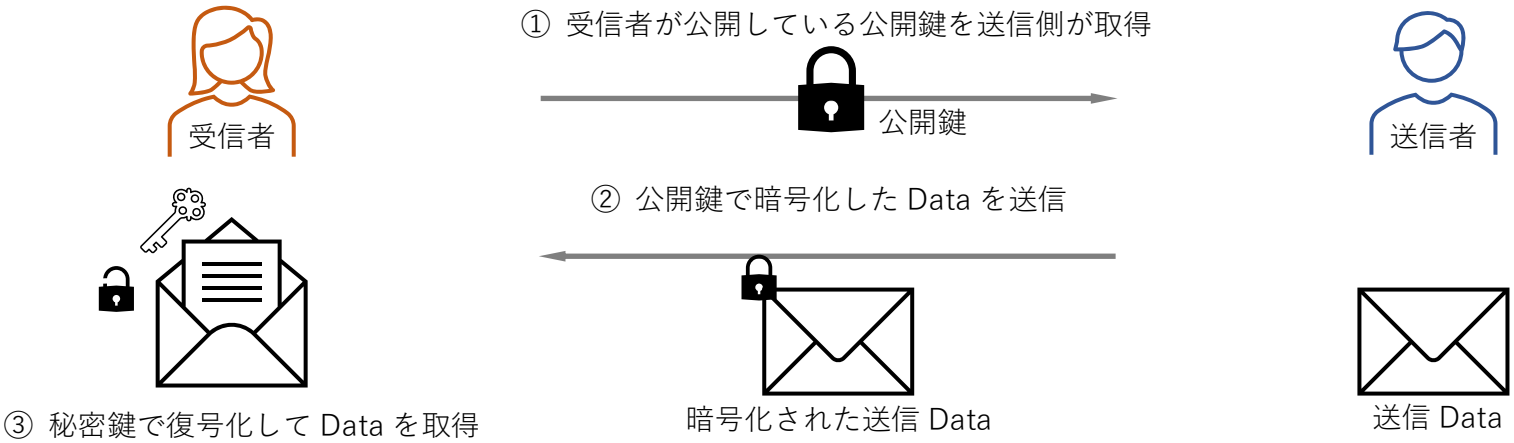
・情報を復号化する際に用いられる鍵。ドアの開錠に相当する

・秘密鍵は他の Node に公開されず、ある Node が特定の Node に向けて送信した「暗号化された取引情報」は、その特定の Node しか復号化することができない

・各 Node はこれら二つの鍵を Wallet と呼ばれる管理 Software に保管し、取引の際に使用する

・送信者は受信者の公開鍵を用いて Transaction 要求を暗号化し、部外者から秘匿する

・正しい受信者のみが、自身の秘密鍵によって Transaction 要求を復号化することができる



Blockchain の矛盾

誰でも台帳を見ることができる ⇔ 誰にも改竄できない

① Blockchain は個人間(P2P)でしか情報交換、連絡できない

② Blockchain は誰でも見ることも書き込むこともできる台帳である ☜ 単一障害点の課題解決

③ 参加する Node すべてによって管理されている ☜ **特定の管理者がいない**
管理者の**信用に依存しない電子取引のシステム**

④ 参加する Node の中には**ビザンチン障害**が含まれる
応答を返さない(オミッション障害)、誤った応答を返す(コミッション障害)
意図の有無にかかわらない
ハードの故障もある

⑤ ネットワークの総数：n≥3t+1（n :ネットワークの総数、 t：ビザンチン障害数）
正常に動く機器：m≥2t+1（m：正常に動く機器の総数）

⑥ **分散合意問題**「不特定多数の参加者がいるネットワーク内で、どうやってただ一つの情報に『合意』（Consensus Algorithm）できるか」

Consensus Algorithm について

① PoW（Proof of Work）：Bitcoin
ブロックを生成する為の「ナンス値」を見つけた者にブロック生成の権利をあたえる。きわめて高い計算能力を必要とし、その消費電力はすでに一国の全消費電力を上回る規模になっている。

② PoS（Proof of Stake）：Ethereum
通貨の保有量が多いほどブロックを生成できる確率が高まるコンセンサスアルゴリズム。誰がブロックを生成するかはランダムに決定されるが、計算能力を使った競争は発生しない。ブロック生成作業のハードルが低く、膨大な電力も不要で、承認スピードも速いという特徴がある。反面通貨の流動性が落ちやすいという懸念がある。

③ PoI（Proof of Importance）：XEM（ネム）
PoS の発展型で、保有量に加えて取引回数や取引量など、いくつかの指標を設けてその通貨に対する保有者の「重要度」をスコアリングし、その結果をもとにブロック生成者を決める。

④ PoC（プルーフ・オブ・コンセンサス）：XRP（リップル）
承認作業を行う中央集権的な特別なノード（バリデータ）の 80%以上が Transaction を承認すれば取引ができる。バリデータ同士が承認者として認め合うことによってネットワークが形成され、悪意のあ

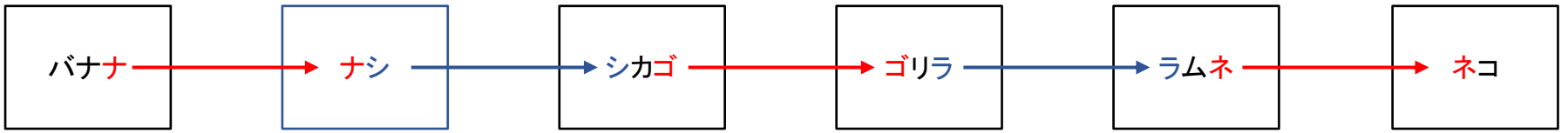
るバリデーターによる不正行為を防いでいる。バリデータの信頼に基づき、管理者の不正を見抜くことができないという理論上の問題を抱えている。限られたバリデーターが承認作業を担当するため、処理スピードが速い。

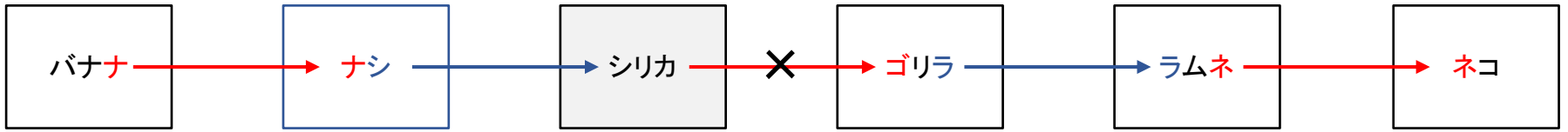
⑤ DPoS（Delegate Proof of Stake）：LSK（リスク）
暗号資産の保有量に応じてブロックの承認権を与える PoS の発展形として、投票によりブロックの承認者を選出する仕組み。取引承認に必要な承認数を減らすことができ、高速なトランザクション処理を実現する。

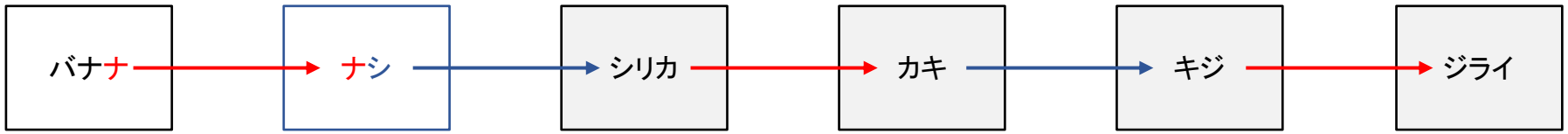
Blockchain は分散性（Decentralization）・安全性（Security）・拡張性（Scalability）の 3 者を同時に成立させることが困難であるという Scalability Trilemma の問題を抱えている。たとえば PoW では安全性および分散性を担保するが拡張性に欠ける。PoS では拡張性はあるものの安全性および分散性に少し不安がある。DPoS では安全性と拡張性は担保されるが、分散性に欠ける。

Consensus Algorithm はこれらの問題に対する各 Blockchain の回答でもある。

Blockchain はしりとりである





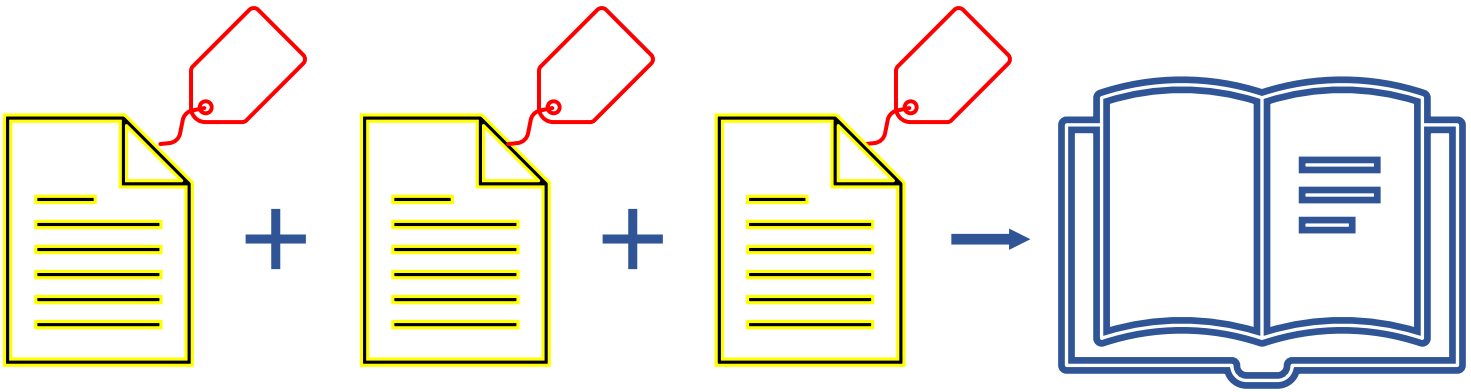


ここで Tag 関数を作ってみる

・Block のすべての要素を Tag 関数によって計算する

・計算された値を Block の Tag にする

・Tag によってその Block を識別する



Block　　Blockchain

・たとえば Block の要素を「取引番号、取引日時、ID 番号、金額」として、すべてを足す

Transaction 73006	73,006
2023 年 5 月 17 日	20,230,517
ID 56719	56,719
23,598 円	23,598
⋮	⋮
Transaction 73018	73,018
2023 年 5 月 18 日	20,230,518
ID 19345	19,345
171,023 円	171,023
	272,500,698

・これを適当な 5 桁の数字 52,371 で割ると 5,203 と余り **14385**[5]

・この 14385 という 5 桁の数字を Tag とする

[5] mod 関数を使うと簡単。mod は割り算の余りを表す modulo から。

・Blockchain につながっている者は誰でも Block の Tag が 14385 だとわかる

・Block の要素のどれを書き換えても余りの数 ＝ Tag が変化してしまうため改竄は発覚する

・この Tag の特徴は ①**常に 5 桁**になる、②Tag からは**元の数字を見つけるのが困難**である

・しかしこの Tag 関数では例えば金額を改竄し、10,000 円増やせば、Tag は 10,000 増え **2**4385 になるだけなので、併せて ID を **5**6719 から **4**6719 に改竄すると、結局 **1**4385 という同じ Tag ができてしまう

・そこで数字をすこし動かすだけでまったく違う Tag が生成されるように修正する

上記の Tag 関数 ＝要素の和／52,371

修正 Tag 関数 ＝ （要素の和+要素和の下 3 桁から生じた数字）／52,371

・ここで、すべての要素の和の下 3 桁から新しい数字を作ってみる

・たとえば百の位を a 、十の位を b 、1 の位を c として ab^c を作る

・要素の和 272,500,698 の下 3 桁は 698 で、これを実行すると 69^8 = 513,798,374,428,641

・修正 Tag 関数に当てはめると 28668 となる

・すべての要素の和が 1 増え 272,500,699 となると修正 Tag 関数では 04864 となる

・すべての要素の和が 1 変化するだけで Tag は 28668 から 04864 に大きく変化する

・こうして Tag の特徴に③**入力値が少し変わるだけで出力が大きく変化**する、が加わる

Hash 関数の特徴

・いま Tag 関数と書いたものは Blockchain では Hash 関数と呼ばれる

・様々な種類の Hash 関数が存在する

・Hash 関数は以下のような性格を持つ

■出力値から入力値を求められない原像困難性がある（一方向性関数）

■どんな入力値でも必ず同じ桁数（固定長）が出力される

■入力値を僅かに変更しただけで出力値は大きく変化する

■同じ入力値に対して常に同じ出力値を返す（一意に決まる）

■Hash 値の検証は Hash 関数を適用すれば容易だが、条件を満たすような Hash 値の生成はきわめて困難である

・先ほどの 5 桁の事例では 52,371 回に 1 回、同じ Tag = Hash 値が生じる可能性がある

・違う入力値で同じ Hash 値が生じることを Hash 衝突と言い、この可能性が低いことを**衝突発見困難性**といい、これが充分に高いことが Security Level の高い関数となる

・たとえば Bitcoin 等で使われる Hash 値は 32Byte = 256bit ある

・256bit とは 2^256（=16^64）であり、これは約 10^77 である

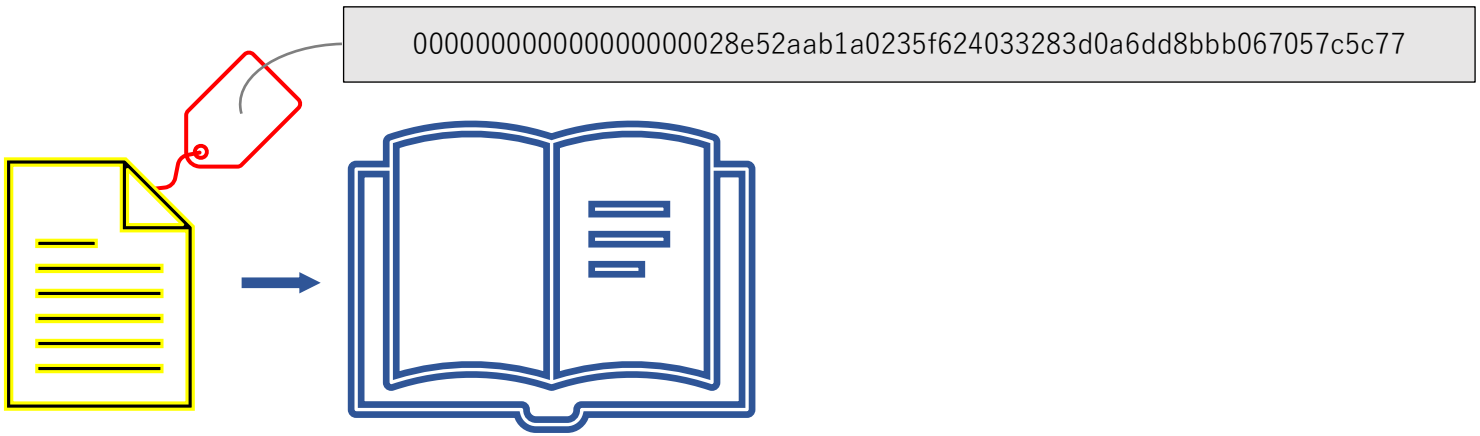
・全宇宙に存在する原子の数は約 10^80 といわれているので、256bit は途方もなく大きな数字を表現できることがわかる

・実際の Hash 値は 16 進数（0～9 と A~F の合計 16 の文字を使う）で 64 桁あり次のように表現される

「**0000000000000000000028e52aab1a0235f624033283d0a6dd8bbb067057c5c77**」

・このように途方もない数があり、同じ Hash 値を改竄によって産み出すことは不可能に近いと考えられている

・Hash 値を Block に持つことで当該 Block の唯一性が担保され、Block の改竄の可能性は困難になる



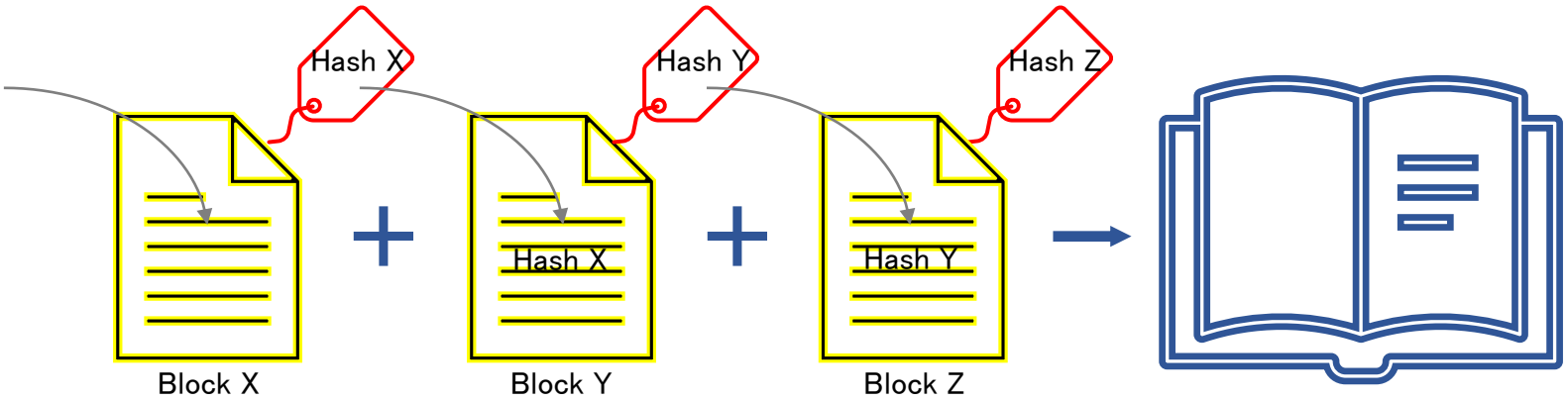
Blockchain はどのように不変性を担保するのか

Blockchain 化による改竄耐性の強化

・Tag を付けて識別していた Block だが、その 1 冊だけを改竄しようと思えば不可能ではない

・先の例のような、たとえば 5 桁の Hash 値だとうまく操作できるかも知れない

・そこで台帳を古いものから順番に並べて一つ前の台帳の Tag をその次に来る台帳に取り込む



・これにより Block X、Block Y、Block Z は独立した Block ではなく、X は Y に、Y は Z に繰り込まれて Chain 状に連結される

・Block X の内容は Hash 値を通して Block Y に影響し、Block Y の内容は Block Z に影響する

・ある Block の改竄に成功したとしても、これに連なるすべての Block の Hash 値が変わってしまうので改竄した Block 以降の全 Block の Hash 値を変更する必要が生じる

・なお Bitcoin の場合、約 10 分に 1 つの割合で新しい Block が生成されるように調整される Algorithm となっている

・また分岐が生じても、より長く Block を積み重ねたところ ＝ 最も多く Mining Power を注ぎ込んだ Chain が Main Chain となるため、少数の改竄者が Main Chain を維持することは現実的に不可能となる

・この困難性を敷衍するため以下に Mining を説明する

Mining の機能

■中央銀行の紙幣の発行に似た新しい暗号通貨の産出、通貨供給の役割を持つ

■不正な Transaction や Double Spend から Blockchain の System を保護する

■産出された暗号通貨を Incentive として Blockchain に処理能力を提供する

・Mining は要求された条件の出力値が生ずる Nonce を掘り当てることである

・Mining が成功すると新しい Block が生成され、新しい暗号通貨が発行される

・では Nonce とは何か（Number Used Once の略）

・Hash 関数の入力値に対して出力値は想定できない

・固定された入力値に可変値を加えて、要求された条件の出力値が生ずるまで可変値を更新し続けることが Mining である

・この可変値を Nonce という

・いいかえれば要求された条件 ＝ Difficulty Target を下回る Hash 値を生じる Nonce を計算する事が Mining である

・次の表は「高崎経済大学は面白い」という文字列に Nonce（01～16 の数字）を付し SHA256 という Hash 関数を適用して Hash 値を求めたものである

入力値：固定値+Nonce	Hash 値
高崎経済大学は面白い 00	ae9cca622e6dc07454835eda20a95c7d48dca346601e92fa16d76d01f31809e2
高崎経済大学は面白い 01	1dcb5fe3183a8ea01beae35825d399dd87a33832513693bf51f528a79241ceb9
高崎経済大学は面白い 02	27816c52182f0be6dfa8b43a4eb5deab5a5424cdc148e64500b24d2e4270e55b
高崎経済大学は面白い 03	27816c52182f0be6dfa8b43a4eb5deab5a5424cdc148e64500b24d2e4270e55b
高崎経済大学は面白い 04	0079a3057cc8c213bb4a71523e07bf4b9c9226ef83e448d3f05ad96f0d99a043
高崎経済大学は面白い 05	ca20eddfa4f6b68951cbb760707b985dfeff332fc4ab616adaa96df8e211a2bd
高崎経済大学は面白い 06	baa721e03d059964b9566febb54a21c25b2f2a9b08fa33df6b759f7fca5294fe
高崎経済大学は面白い 07	fa2c44ba0310b00bce56c35dfefbdd473105e32ace67d7ec29df76e45ac44ac5
高崎経済大学は面白い 08	67e915d9516168e1203447f6cd41ad13055db5b53916ce98293d0b13ecd2123f
高崎経済大学は面白い 09	0b3e996bab16fb3500afc552903c246f87877cea0edb7ffd4c173b71adc5b343
高崎経済大学は面白い 10	41ddb478c8bfebc46d6f23b6e352632dc4c28699a998ee8873b5aac90304bd39
高崎経済大学は面白い 11	4470f137d218ba642b5e6e716f21ed43a335b7e3c9773cfb7b48274fe62b16dc
高崎経済大学は面白い 12	0e30df706d1aa1746ecc6d6da13a0e306822e693a013a87cb7d6c48cdf9f32a3
高崎経済大学は面白い 13	729d41ab822d62711e92ae99d70aa1f2edf092a0929b97703e174dd5e6f6fdb3
高崎経済大学は面白い 14	489afc4609603224e2543c00db8719ef0906f2c25ddc66da67d617362388c007
高崎経済大学は面白い 15	5ced57e32963f8473daf22e9055334deb8b6419eb55fd2ad598db4b75ab8f169
高崎経済大学は面白い 16	32f6496ae061b2f8a1a1ed4df3ad1f181f4e5c2f1fc5225e3af82936ceaee5f4

・Hash 値は 16 進法で 64 桁の数字であるから、先頭の文字が 0 になる確率は 16 回に 1 回であり、先頭から 2 桁が 00 となるのは 256 回に 1 回しかない

・ここでは「高崎経済大学は面白い」に Nonce「04」を加えた時「先頭から 2 文字が 00」という小さな数字が生じている

・先頭から 3 桁を 0 とするためには確率的に 4,096 回に 1 回しかその数字が生じず、4 桁だとその 16 倍、5 桁だと更にその 16 倍となり飛躍的に計算回数が増える

・こうしてより小さな数になるほど計算回数が増え、Nonce を掘り当てる困難性は上がる

・この困難性を Difficulty という

・2023 年 5 月 5 日の Bitcoin の場合、Difficulty Target は Hash 値の先頭から 19 桁 0 が続く程度の小ささで、Difficulty は 48,005,534,313,578 で次の Block を生成するために 48 兆回、SHA256 で Hash 計算する必要がある事を示す（灰色文字は chatGPT の回答）

・また Hash Rate は 343.07 EH/s（E はエクサで T テラの 100 万倍、3.4 垓、垓は 1 兆の 1 億倍）となっている（Hash Rate が 1H/s であれば、1 秒間に 1 回の SHA-256Hash 計算を実行できる）

・いずれにせよ、この莫大な計算能力を投入しないと Nonce を掘り当てることは出来なくなっており、改竄の可能性を限りなくゼロに近づけている

Blockchain の仕組み

■一定の Transaction（取引）の集まりを Block に記載する

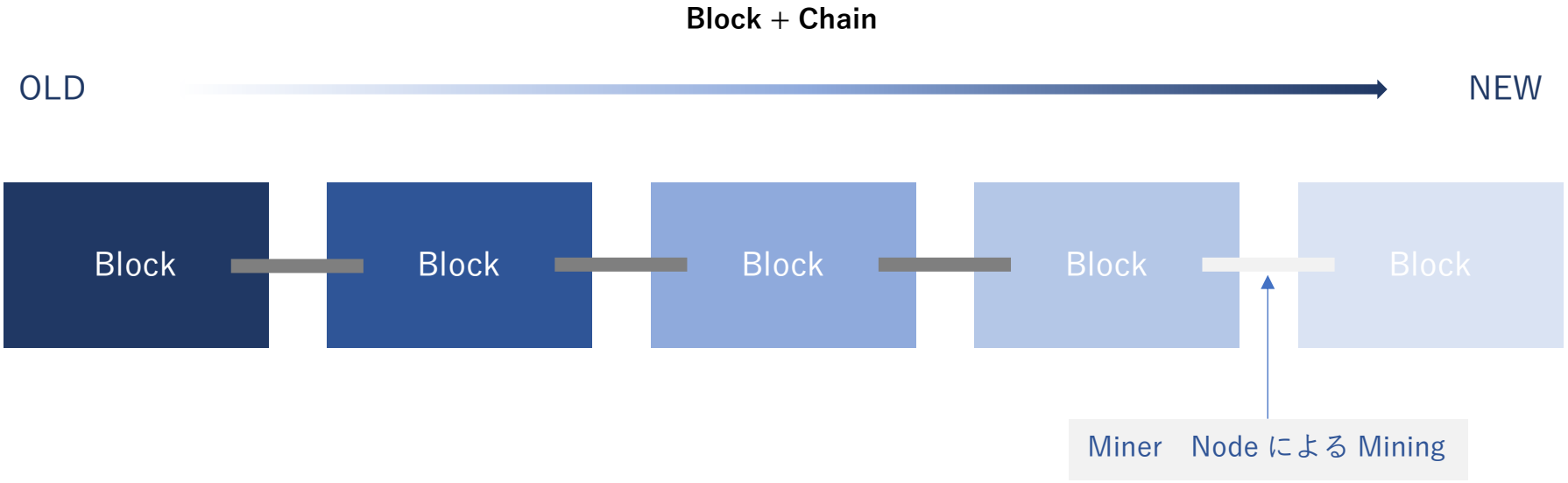
■Block は時系列に積み上がっていく

■Block 毎に Header を付ける

■Header には Block に含まれる Transaction の内容が反映されている

■Header には一つ前の Block から生じた Hash 値が記録される

■すべての Block は誰でも見ることが出来る



Block がつながる仕組み

・Block は **Header** と多数の **Transaction** で構成される

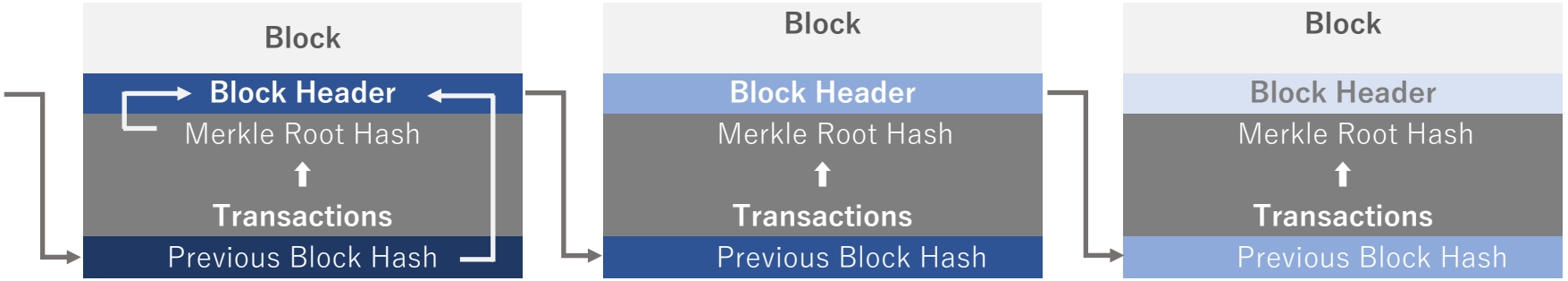
・Header には前の Block の Hash 値と、この Block の **Merkle Root Hash** が含まれる

・生成された Block の Header から次の Block の為の Hash 値 Previous Block Hash が計算される

・この Hash 値が Difficulty Target の指定する閾値を下回るような Nonce を計算する

・Nonce が見つかると新たな Block が生成される

・Nonce を見つけた Miner は新しく生成された Bitcoin と Transaction の手数料を得る

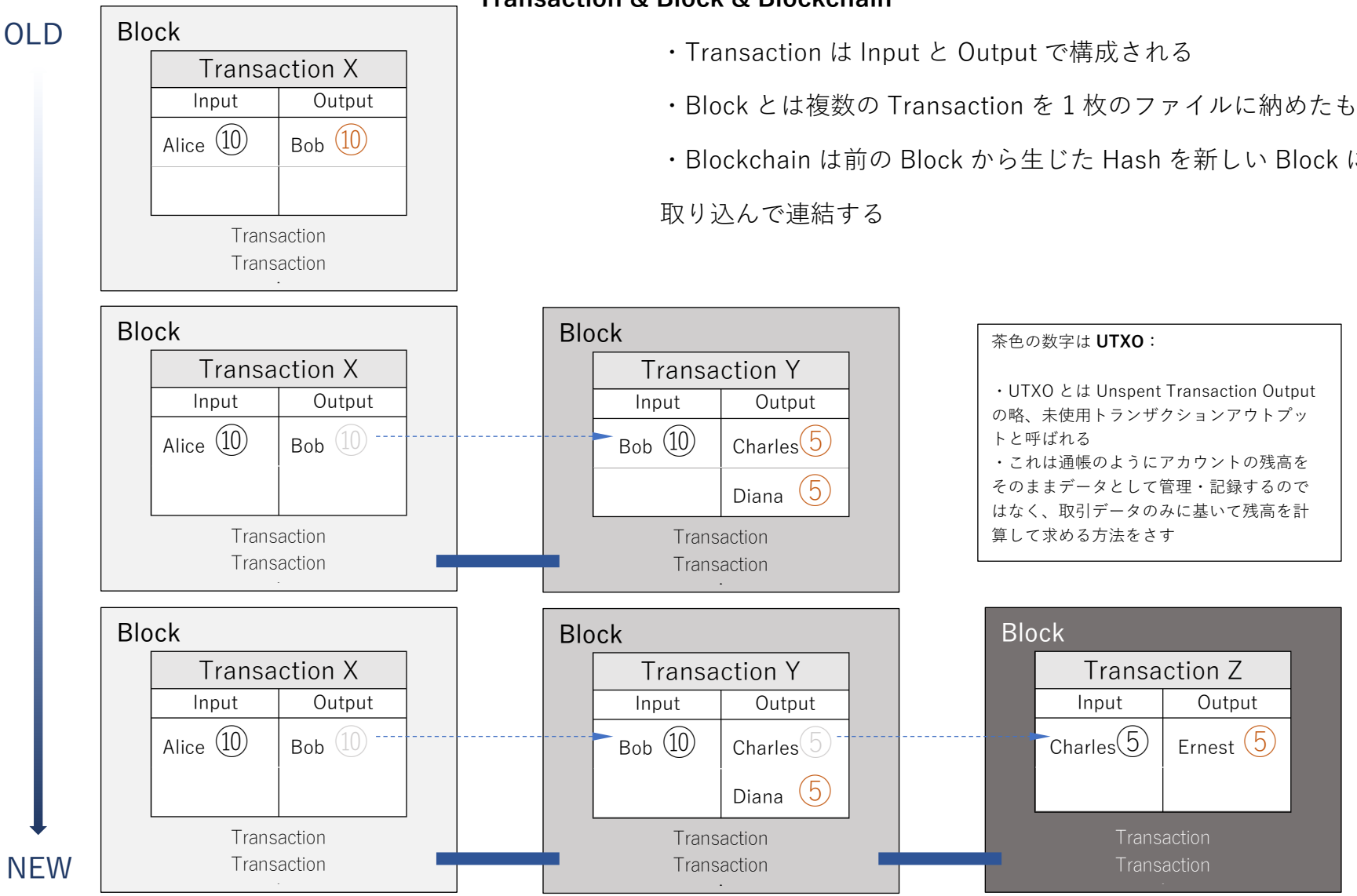


Transaction & Block & Blockchain

・Transaction は Input と Output で構成される

・Block とは複数の Transaction を 1 枚のファイルに納めたもの

・Blockchain は前の Block から生じた Hash を新しい Block に取り込んで連結する



茶色の数字は **UTXO**：

・UTXO とは Unspent Transaction Output の略、未使用トランザクションアウトプットと呼ばれる
・これは通帳のようにアカウントの残高をそのままデータとして管理・記録するのではなく、取引データのみに基いて残高を計算して求める方法をさす

Block (1MB)		
Block Header (80Byte)		
Hash of Previous Block's Header	直前の Block の Header から得られる Hash 値	00000000000000000028e52aab1a0235f624033283d0a6dd8bbb067057c5c77
Time Stamp	Block の生成 Unixtime	64639D74 (=2023/5/17 0:12:52)
nBits	Difficulty Target	30c31b18
Nonce	Difficulty Target を下回る数値を見出すと block が生成される Nonce を求めるのが Mining	fe9f0864
Merkle Root Hash	この Block のすべての Transaction から得られる Hash 値	bb039c3a0465d6809f459f26244a616a1402ab74aa0aa787f94cebf2c73d08c4
Transactions		

Block Header の主な内容

・Block Header には表のような内容が記載されている

・前の Block の Hash 値と Merkle Root Hash を比較すると明らかな相違が見出される

・Mining はこのような Header の Hash 値を生成させる Nonce を見出す作業である

Block の生成・Blockchain への連結までのフローの再整理

・各 Node が Input と Output を指定した Transaction の内容を Blockchain の Network に送る

・同一時間帯内に行われた全 Node の全 Transaction を一つの Block に格納する

・Block には、Transaction 情報だけでなく、Block Header という Block 識別子が格納されている

・Block Header を入力値として、Hash 関数処理によって Hash 値が生成される

・この Hash 値が、Blockchain が要求する Target に収まったとき、その Block は正しい Block として認証され、既存の Block chain に最新の Block として連結される

・Hash 処理において、入力として操作可能なのは Block Header のうち Nonce と呼ばれる入力値のみであり、それ以外は既存の Block chain や格納する Transaction の情報によって一意に定まる既定値である

・Nonce の入力値の入れ替え操作を繰り返し閾値に収まる Hash 値を目指す（莫大な計算力の投入）

・閾値に収まる Hash 値が得られると、新しい Block として Chain に連結される

Blockchain の既存技術にはない性格

■取引情報の改竄・Hacking が困難：Blockchain を用いた取引情報管理は、従来の Server/Client 型の一極集中情報管理に比べて、以下のような複数の要素によって改ざんを二重三重に困難なものとしている

・**各 Node がそれぞれ Blockchain を管理するという分散性**により、改竄するには全 Node の情報を改竄する必要がある

・取引情報は Blockchain として過去～未来全ての情報と連結しているため、改竄するにはそれら全てとの整合性を保たねばならない

・Consensus Algorithm によって**正しい取引情報を取捨選択する確実性が向上**している

・Hash 計算の負荷がきわめて大きく、計算能力とかかる費用からも改竄を不可能にしている

■情報資産と所持者の関係を自動的に紐付けできる

・管理者・仲介者による信頼保証に基づく既存の資産取引とは異なり、Blockchain で Smart Contract によって、資産とその所持者・所持資格を第三者の仲介なく紐付けることができる

・これによって仲介手数料などを大幅に節約できると同時に、取引のための前処理(身元確認など)、後処理(契約成立後の履行の監視など)を省くことができる

Smart Contract とは何か

・Bitcoin の Blockchain は情報を載せ管理する台帳に過ぎなかったが、たとえば **Ethereum** という Blockchain Platform は情報管理だけでなく、**情報処理をも実行できる台帳**として発展させた

・この「処理も含めた情報の管理形態」のことを **Smart Contract** と呼ぶ

・Wikipedia によると

1. 契約の検証、執行、実行、交渉を意図した Computer Protocol
2. 第三者を介さずに信用が担保された Transaction を処理できる
3. 契約条件が満たされたときに自動的に実行する Computer Code に契約を Digital 化する

・これらは暗号通貨に留まらない Blockchain の活用領域を生む

・従来契約に必要だった第三者の仲介や、身元確認などの諸々の処理は簡略化される

・分散型アプリケーション（**DApps**）を Blockchain 上で稼働させられる

・分散型金融（**DeFi**、Decentralized Finance）の Platform となる

・非代替性トークン（**NFT**、Non-Fungible Token）と呼ばれるユニークで不可分なトークンの作成が可能である

・また Ethereum は汎用コンピュータとして設計され、仮想マシン（Virtual Machine）が動かせる

Blockchainは何に活用できるか？

・東京大学公共政策大学院は次の活用分野があることを提言している

カネ分野	中央銀行発行 Digital 通貨
	資金調達
	徴税
モノ分野	Supply Chain Management（SCM）
	信用情報の管理（Smart Property）
	広告の運営管理
	所有権管理・知財管理
ヒト分野	デジタル ID
	投票

・中央銀行発行 Digital 通貨（Central Bank-issued Digital Currency、CBDC）

・日銀は次の頁で取り組み方針を示している　https://www.boj.or.jp/paym/digital/index.htm

・SCM への Blockchain 活用は以下を参照

https://www.nttdata-gsl.co.jp/related/column/what-is-scm.html

・たとえば Digital 化が可能な資産は全て Blockchain 上で管理できるが、資産全般のこのような管理形態を Smart Property と呼ぶ

・Blockchain で管理できる可能性がある対象の例

資産の種類	例
一般	エスクロー取引、担保付取引、第三者裁定、複数者取引
金融取引	株、未公開株、クラウドファンディング、債券、投資信託、デリバティブ、年金保険、年金
公的情報	不動産登記、自動車登録、事業者登録、結婚証明、死亡証明
ID	運転免許、IDカード、パスポート、有権者登録
民間	借用証書、ローン、契約、賭け、署名、遺言、信託、エスクロー
各種証明	保険証名、所有証明、公証
有形資産の鍵	家、ホテルの部屋、レンタカー、自動車利用
無形資産	特許、商標、著作権、予約、ドメイン名

・活用事例は検索をかけると大量に見つかるが株式会社 digglue が比較的丁寧に紹介しているので参考に

自動車業界編　1	https://baasinfo.net/?p=2681
自動車業界編　2	https://baasinfo.net/?p=2520
GE Aviation	https://baasinfo.net/?p=1745
航空業界編	https://baasinfo.net/?p=3500
スターバックス	https://baasinfo.net/?p=1283
Xiaomi	https://baasinfo.net/?p=1090
LVMH	https://baasinfo.net/?p=1197
サプライチェーン（まとめ）	https://baasinfo.net/?p=19
不動産	https://baasinfo.net/?p=2142
電力	https://baasinfo.net/?p=2313
医療	https://baasinfo.net/?p=2260
ゲーム	https://baasinfo.net/?p=2191
貿易	https://baasinfo.net/?p=2299
交通機関	https://baasinfo.net/?p=1530

まとめ

■ **Blockchain と暗号通貨**

① Blockchain の最初の広範な応用は、暗号通貨として企図された Bitcoin だった

② Bitcoin は Digital Data を通貨として機能させるために、金を模倣した

③ 金は希少性、有限性、不変性を持つ

④ Bitcoin は Blockchain 上にこれらの性質を組み込んだ（希少性、有限性は Algorithm によって定められ、不変性は下記の改竄不可能性によって担保されます）

■ **Blockchain は分散型台帳システム**

① Blockchain は銀行や企業のような集権的管理者のいない、誰でも参加できる分散型 Network（Peer to Peer）上で稼働する

② Blockchain は取引を記録した Block を時系列に並べ、各 Block のすべての内容を反映した Hash 値でつなぎ合わせている

③ Hash 関数は内容を秘匿した形で Data の唯一性を証するものでなければならない（出力値から入力値を求められない原像困難性、同じ入力値に対して常に同じ出力値を返す、異なる入力値に対しては常に異なる出力値が生じる）

④ 分散型の Network と Hash 関数による Block の連結で Data は恒久的に記録され、その改竄は事実上不可能

■ **Blockchain の活用**

① Digital 化が可能な資産は全て Blockchain 上で管理できる（Smart Property）

② さらに Ethereum（イーサリアム）という Blockchain Platform によってたんなる Data 管理だけでなく、Program をも実行できるようになった（Smart Contract）

③ これにより多様な契約を Blockchain 上で実行できるようになった

④ さらに分散型 Application（DApps）を動かし、分散型金融（DeFi、Decentralized Finance）の Platform や、非代替性 Token（NFT、Non-Fungible Token）も生まれている

（参考）　高崎経済大学学生へのコメント

Blockchain と SDGs の関係について資料では触れませんでしたが、簡単に説明します。Blockchain は Network 上で分散して管理、稼働しているため、集権的に動いている Database と違い、点検や事故によって停止することもなければ Data が消失することもありません。この一点だけでも持続可能性の高さを証明できます。

さらに資料に Link を示していますが、例えば Starbucks は Fair Trade を重視しています。小規模農家を保護し高い品質を維持するために、コーヒー豆の生産や流通の過程を詳細に Trace して、事前の合意、基準に適合した Supply Chain が維持されているか監視する必要がありました。Blockchain は各流通段階のきわめて精緻な追跡を可能にすると共に Smart Contract を組み合わせることで、事前の契約に従った取引を自動的に実行します。これは SDGs に寄与した好例です。

レポートの中には、暗号通貨が信用できない、という意見が散見されましたが、それは Blockchain の信頼性とは無関係なものだということを繰り返しておきたいと思います。たとえば誰もが手元の 1 万円札は信じているはずです。それは財布の中に入っています。でもその財布を落としてしまいました。その時、一万円札なんて信用できない、なんていう人はいませんよね？Hacking について触れた人もいましたが、これは Bitcoin の価値を損ねる行為ではありません。人の財布からお金を抜き取る行為なのです。Hacking というのは Blockchain に対する攻撃ではなく、あなたの財布の脆弱性に対する攻撃なのです。財布を落とすのは底の浅いポケットに大きな財布を入れていたからです。

授業では The DAO 事件についてもすこし触れましたが、これも暗号通貨の価値を破壊したものではありません。Blockchain 上に書かれた Program の誤りによって多額の暗号通貨が流出したのでしたが、これは Blockchain ではなく Program の作成者に帰責されるものです。

ただし、ここで、ひとつ重要な注意があります。Blockchain は分散型で動いていますから、その Node にはすべてが善良な人であるわけでもなく、また善良であるけれどもミスばかりする人も含まれています。そういう悪い人や未熟な人が加わっていても Blockchain は正しい

Block だけを積み上げていくようになっています。これは資料の冒頭の定義に書いた定義 1 の「ビザンチン障害」があっても合意は覆らないという内容です。Bitcoin の場合なら何の問題も生じません。ところが Ethereum 等のように Program が Blockchain の内容となっている場合、悪意ある人が自分にお金がどんどん流れ込むような仕掛けをしないとも限りません。あるいは Program 自体に Error がある場合もあり得ます。そのようなものでも記述が適正であれば Blockchain に乗ってしまうのです。The DAO 事件はまさにそういうものでした。したがって DApps、DeFi 等はその背景に誰がどんな意図を持って存在しているのか見極める必要があります。これはきわめて難しいことです。見知らぬものに安易に飛びつかないようにしなさい。これは暗号通貨や Blockchain の価値とはまた別のしかし大きな問題です。

貨幣が貨幣であるのはそれが貨幣であると人が信じているからと説明しましたが、だから暗号通貨や Blockchain を信じていない人に安全なものだと啓蒙する必要があると書いた人がありました。その必要はありません。ドルが貨幣ではないなどと誰も考えていないはずですが、日本でドル払い出来るお店はほとんどありません。しかし世界中でドルは使われています。輸出企業は大量のドルを稼いでいます。暗号通貨も Blockchain もすでに、それなしでは経済がうまく動かないほど普及しています。わたしたちの身近にないだけです。貨幣は使えるところで使われればいいのです。

物理的に存在しないお金がどうやって存在すると言い得、現実に流通しているのか？という問いに興味を持った人も多くいました。経済学部だと信用創造ということを学んでいると思いますが、それを想い出して下さい。A さんが 100 万円を銀行に預けます。銀行は預金者の 1 割が引き出しに来ると統計的に知っているので 10 万円を手元に置いて 90 万円を B 社に貸し付けます。A さんの通帳には 100 万円の記載があり、B 社の口座にも 90 万円がある事になります。B 社の口座を預かっている銀行はまた C さんに 81 万円を貸し出しました、、、と続けていくと A さんの 100 万円は最終的に 1,000 万円となって社会を巡ることになります。銀行から銀行に支払いがされるだけで紙のお札がなくても自動車が買えたりします。最初にあったお札は 100 万円だけだったのですけれど。

Hash 関数を説明するために「Tag 関数を作ろう」という説明をしました。何人かの人が Tag 関数というものがあると誤解されていました。これは商品についている Tag になぞらえて、記載された Data を識別する数字をどのように作るか説明するため、便宜的に「Tag 関数」と名付けたものに過ぎません。

資料の 29 頁に「前の Block の Hash 値と Merkle Root Hash を比較すると明らかな相違が見出される」とのみ記載して、説明を付していませんが、これは二つの Hash 値を実際に見比べてもらおうとしたからです。同じ Hash 計算を行っているのですが、前の Block の Hash 値は 0 がいくつも並んでいます。これは Block Header の Data に可変値である Nonce を加えて 0 が指定された個数並ぶような出力値を探したからです。どのような Nonce を加えれば 0 が指定個数並ぶようになるのか？この Nonce を見つけることが Mining です。そしてこの 0 の数が少なければ計算は簡単に、多ければ計算量が飛躍的に増える仕組みを使って、Mining の難易度を調整します。この難易度のことを Difficulty といいます。この難易度は、Network につながったすべてのデバイスの計算能力に応じて変化し、約 10 分に 1 つ Block が生成されるスピードに調整されています。Blockchain の処理速度は遅い、という指摘をした人がありましたが、これは Block の生成にあえて時間をかけて合意（Consensus）を得ようとしているからです。この Mining の仕組みに莫大な計算量を投入するのを PoW（Proof of Work）といいます。じつは Consensus Algorithm には PoW のほかにも PoS（Proof of Stake）等複数のものがあります。Blockchain は分散型で処理が進むため、この正しい合意を得る仕組みを如何に Program するかがきわめて重要になります。

暗号通貨が法定通貨に取って代わることはないだろうとお話ししましたが、何人かの方がこれに同意されていました。実際は途上国で Bitcoin が法定通貨として使われたりしていますからすこし複雑な話になります。とはいえ、たとえば Bitcoin で日本の予算が組まれることはあり得ません。それは Bitcoin が金を模倣したからです。金は有限ですが、通貨発行量が有限だと財政を組み立てられません。金本位制に復帰する国がないことも何故だか考えてみて下さい。そして金は通貨ではなく Commodity です。日本語では「商品」です。通貨と商品がどう違う

のか研究すると面白いと思います。なお授業では暗号通貨と呼称しましたが、法律では暗号資産と言います。仮想通貨という呼称は無くなるのではないかと思います。暗号資産という呼称を法が採用したのは、通貨ではないという側面を強調したかったからかも知れません。

何人かは暗号通貨を株のようなものだ説明していました。暗号通貨を Token といいますが、この Token が、それが発行される Blockchain 上で議決権の証となる事を知っているからだと思います。このことについて詳細な説明をする余裕はありませんが、Crypto Currency と Security Token は同じものではありません。暗号通貨は暗号通貨であり、たんに Token ですが、Security Token は債権や議決権の持分を表しており、本来区別されるべきものです。Security Token は Smart Contract が出来ないと Blockchain に乗らないのです。金融商品取引法等を調べられるとすこし理解が進むと思います。

過度な期待に同調せず学ぼう

・暗号資産が法定通貨を代替することは出来ないのではないか

・NFT は現実の世界にあるモノと直接には結びついていない

・「いくつかの DeFi プロトコルは「ポンジ・スキーム[6]のようなもの」」であり「DeFi は本人確認ルールや資金洗浄防止ルールとは甚だしく相容れないものである」（Wikipedia）のも事実である

一般に、世間からの認知度が低い段階にある新興技術は、わずかな事件、事故があると信頼を損ない社会受容性を大きく低下させる傾向にありますが、これは Literacy の向上によって解決される問題です。例えば、Ethereum を用いた自律分散組織 DAO3 が 2016 年 6 月に不正攻撃を受けて崩壊し、Blockchain の信頼性は大きく揺らぎました。しかし、この脆弱性は Blockchain 技術にあるものではなく、それを利用するにあたっての DAO の Program にあり、Blockchain の問題ではありませんでした。Blockchain という基盤技術はそれ以降も問題なく運用されています。

これまで述べてきたように Blockchain には多くのきわめて優れた機能があります。これは SDGs にも大きく寄与するものです。ですから知識を得ましょう。知らずに拒絶するのではなく、十分に理解して警戒すれば、大きな可能性を開拓できます。

[6] ポンジ・スキームは、投資詐欺の一種。後発投資者から集めたカネで先行投資家に収益金を支払うことで、破綻することを前提に騙し取る詐欺の手法。詐欺師チャールズ・ポンジ（Charles Ponzi）の名に由来。