企業の資金調達手段としての暗号資産：政策・規制研究の展望

山　本　達　司*

Ⅰ　は　じ　め　に

現代において，暗号資産（crypto assets）の経済規模は膨大である。2023 年 8 月 12 日において，暗号資産の世界シャアトップ 10 だけでも，その時価総額は 10,110 億 US$ 以上であり[1]，これは 2022 年のオランダの名目 GDP 9,936 億 US$（世界 18 位）を上回っている[2]。

一方，世界には革新的な技術をもつベンチャー企業が，数多く存在している。そのような企業は，企業年齢が若く，小規模企業であることが多いため，資金調達方法に大きな制約があると考えられる。このような企業にとって，暗号資産は迅速に資金調達を行う 1 つの有用な手段となる可能性がある。

暗号資産に国境はない。世界中のインターネットでつながった個人・法人が，銀行を仲介することなく，1 日 24 時間，絶え間なく暗号資産の送金取引を行っている。これは企業にとって，世界中から資金を調達できる可能性を意味する。例えば，新株予約権付社債を暗号資産建で発行できれば，暗号資産保有者は社債投資を行うと同時に，新株予約権を行使して株主になることもできる。つまり，企業にとっては社債による資金調達と株式による資金調達の両方が可能となる。

革新的な技術をもつベンチャー企業の資金調達が，このような手段で容易になれば，その企業の製品が社会に広まることにより，社会の利便性が向上するとともに，大きな経済効果をもたらし，社会全体が幸せになると考えられる。これを実現するためには，

---

* Yamamoto, Tatsushi

1　2023 年 8 月 12 日 14 時（日本時間）のデータである。（データ出典：https://coinmarketcap.com/）

2　https://www.globalnote.jp/post-1409.html

人々が安心して暗号資産取引を行う環境を整備することが不可欠である。具体的には，次の３つが重要であると考えられる。

第一に，暗号資産価格の長期的安定である。暗号資産は決済手段であり，基本的にマイニング報酬のみによって供給量が増加する。そして，暗号資産には供給限度が決められている。そのため，供給限度に達した暗号資産には，もはやマイニング報酬が支払われることはなく，決済手段としての機能が大きく低下する。このとき考えられる１つのシナリオは，暗号資産価格の暴落である。これを回避する政策を提示することが，長期的かつグローバルな課題である。

第二に，暗号資産価格の短期的ボラティリティの軽減である。一般に暗号資産価格のボラティリティは高い。この性質は，リスク愛好的な投資家，あるいは暗号資産のハイリスク・ハイリターンの性質を利用してヘッジを行う企業などには選好される。しかし，大多数のリスク回避的な投資家を暗号資産取引に参加させ，暗号資産市場を継続的に発展させるためには，暗号資産価格の短期的なボラティリティを低める仕組みが必要である。暗号資産取引に国境はない。そのため，これはグローバルな短期的課題である。

第三に，暗号資産に関する会計規制・監査制度の整備である。世界中の投資家から暗号資産による資金調達を行うためには，企業は自社の財務状況を適切に開示する必要がある。しかし，それだけでは十分でない。暗号資産による資金調達を促進するためには，各国が暗号資産に関する会計規制・監査制度を整備し，企業のディスクロージャーに信頼性を付与することが重要である。これは，ローカルな短期的課題である。

暗号資産の技術は日々進歩し，そのスピードは非常に速い。そのため，長期的課題，短期的課題のいずれについても，グローバルな課題，ローカルな課題のいずれについても，技術発展の後追いの解決方法は有効でない。むしろ，暗号資産取引の基本的な構造を前提とし，暗号資産取引という大きな枠組みに対して，緩やかな方針を示すことが重要である。そこで本研究では，これらの課題を解決するための研究アプローチを模索することにしたい。

Ⅱ　暗号資産の取引構造

本節では，次節以降の議論のために，暗号資産の取引構造を概観し，暗号資産に関する用語の定義を明確にすることにしたい。

(1) 円滑な暗号資産取引の条件

暗号資産（crypto assets）は，ウェブ上の P2P と呼ばれるネットワークにおいて取引されるデジタル通貨である。**P2P**（peer to peer）とは，中央集権的なサーバを介さず

に，不特定多数の情報端末が対等の立場でデータを送受信する分散型の通信ネットワークであり，P2P の不特定多数の情報端末は**ノード**（node）と呼ばれる。P2P の主たる特徴は，次の通りである。

- 分散型の通信ネットワークであるため，特定のノードに負荷がかかりにくく，システム障害のリスクが小さい。
- 各ノードが通信情報を保有しているため，特定のノードに障害が発生しても，システム全体に対する影響が小さい。
- 各ノードが対等の立場で参加する通信ネットワークであるため，各ノードの匿名性が高い。

これらの P2P の特徴が，そのまま暗号資産取引の特徴となっている。

図 1　P2P のイメージ

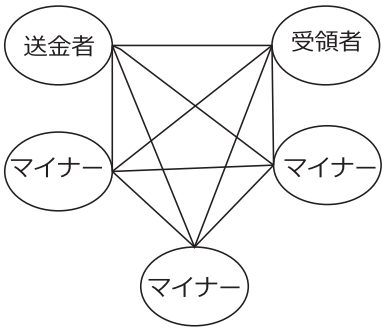


図 1 は，暗号資産取引にかかわるノードの関係を簡略化して示している。P2P 上には，暗号資産の送金者と受領者がいる。そして，送金取引の承認競争に参加している複数のマイナーがいる[3]。P2P 上では各ノードの匿名性が高い。つまり，P2P は世界中の面識のない人々によって構成されている。従って，暗号資産取引を円滑に進めるためには，次の条件が必要である[4]。

〈条件〉

①　P2P 上の送信者のメッセージについて，受信者が送信者の本人確認をできること[5]

3　マイナーについては，以下の「第Ⅱ節（3）ブロックチェーンとマイニング」で定義を明確にする。
4　Nakamoto（2009）は，P2P 上において匿名性が高いノード間で安全に送金取引を行う方法を提唱した最初の論文であり，ビットコインのブロックチェーンについての理論的基礎を示している。
5　「送信者」，「受信者」は，それぞれ P2P 上でのメッセージの送信者，受信者という意味である。マイナーが送信者または受信者となることもあるので，必ずしも送金取引の「送金者」，「受領者」と一致しない。

② P2P 上の送信者のメッセージが改ざんされていないことを，受信者が確認できること

条件①は，「メッセージに記載されている送信者名が，そのメッセージの作成者のものであること」を，受信者が確認できることである。条件②は，「メッセージが他のノードによって改ざんされていないこと」，ならびに「送信者自身の事後的な改ざんが行われていないこと」を，受信者が確認できることである。条件①は公開鍵暗号とハッシュ値の利用によって，条件②はそれに加えてブロックチェーンの利用によって解決されている。以下では，このメカニズムを概観する。

（2）公開鍵暗号とハッシュ値の利用

公開鍵暗号とは，一般に公開する**公開鍵**と秘密情報である**秘密鍵**の併用によって，メッセージの暗号化・復号を行う暗号技術である。公開鍵と秘密鍵について，次の関係が成り立っている。

- ある人の公開鍵で暗号化したメッセージは，その人の秘密鍵で復号できる。
- ある人の秘密鍵で暗号化したメッセージは，その人の公開鍵で復号できる。

つまり，メッセージ m の送信者（sender）の公開鍵と秘密鍵をそれぞれ $S(\cdot), S^{-1}(\cdot)$ とすると，$S^{-1}(S(m)) = m$ と $S(S^{-1}(m)) = m$ が成り立ち，受信者（receiver）の公開鍵と秘密鍵をそれぞれ $R(\cdot), R^{-1}(\cdot)$ とすると，$R^{-1}(R(m)) = m$ と $R(R^{-1}(m)) = m$ が成り立つ。ここで重要なことは，送信者の公開鍵 $S(\cdot)$ から送信者の秘密鍵 $S^{-1}(\cdot)$ を，受信者の公開鍵 $R(\cdot)$ から受信者の秘密鍵 $R^{-1}(\cdot)$ を特定できないことである[6]。以下では，公開鍵，秘密鍵を用いて，上記の条件①②が満たされることを確認する。

（a）受信者の公開鍵・秘密鍵の利用

最もシンプルな公開鍵暗号の利用方式は，「送信者が受信者の公開鍵を使って暗号 $R(m)$ を作成・送信し，受信者は自分の秘密鍵を使って $R^{-1}(R(m)) = m$ と復号する」ことである。この方式を用いれば，メッセージ m の盗聴は防止できる。なぜなら，盗聴者は暗号 $R(m)$ を入手できたとしても，受信者の秘密鍵 $R^{-1}(\cdot)$ をもっていないため，暗号 $R(m)$ を復号できないからである。しかしこの方式では，誰でも暗号 $R(m)$ を作れるので，受信者は送信者の本人確認をできない。つまり，条件①が満たされない。

6　現在，ビットコインなどで使われている楕円曲線暗号では，このことが証明されている。小島（2019）では，RSA 暗号の簡単な数値例を用いて，このことが証明されている（pp.182-184）。

（b）デジタル署名の利用

（a）で述べた欠点を解決する方法として，「送信者が送信者の秘密鍵を使って暗号 $S^{-1}(m)$ を受信者に送信し，受信者が送信者の公開鍵を使って $S(S^{-1}(m)) = m$ と復号する」方式が考えられる。これは，**デジタル署名**と呼ばれる。デジタル署名を用いれば，送信者が送信者自身の秘密鍵を使って暗号 $S^{-1}(m)$ を作成しているので，条件①は満たされる。しかし，デジタル署名には次のような欠点がある。

- 誰でも送信者の公開鍵を使って $S(S^{-1}(m)) = m$ と復号できるので，盗聴を防止できない。
- メッセージが改ざんされたとしても（$\widetilde{m}$），復号されたメッセージの $S(S^{-1}(\widetilde{m})) = \widetilde{m}$ が正しいメッセージ m ではないことを，受信者が確認できない（条件②が満たされない）。

（c）デジタル署名とハッシュ値の併用

（a）（b）で述べた欠点を解決する手段が，デジタル署名とハッシュ値の併用である。**ハッシュ値**（hash）とは，メッセージ m をハッシュ関数 $h(\cdot)$ によって変換した値 $h(m)$ であり[7]，ハッシュ値 $h(m)$ は固定長のデータである[8]。重要なことは，ハッシュ値 $h(m)$ から元のメッセージ m を復元できないことである。これは，暗号とは異なる特徴である。

デジタル署名とハッシュ値を併用すれば，次のようにして条件①②を満たすことが可能である。

- 送信者はデジタル署名 $S^{-1}(m)$ を受信者に送る。それと同時に，送信者はメッセージ m のハッシュ値 $h(m)$ を送信者の秘密鍵で $S^{-1}(h(m))$ と暗号化して受信者に送る。（条件①が満たされる）
- 受信者は送信者の公開鍵を使って，デジタル署名を $S(S^{-1}(m)) = m$ と復号し，その上でメッセージの m のハッシュ値 $h(m)$ を求める。それと同時に，送信者から送られてきた $S^{-1}(h(m))$ を送信者の公開鍵を使って，ハッシュ値 $S(S^{-1}(h(m))) = h(m)$ を求める。そして両者のハッシュ値 $h(m)$ の一致をもって，受信者はこのメッセージが改ざんされていないことを確認できる。（条件②が満たされる）

7　ハッシュ関数には，元のメッセージ m を少しでも改ざんすると，出力されるハッシュ値 $h(m)$ が大きく変わるという特徴がある。

8　ハッシュ関数である SHA-256 は，256 ビット（固定長）のハッシュ値を出力する。

（3）ブロックチェーンとマイニング

ブロック（block）とは，暗号資産に関する（1つまたは複数個の）取引の記録であり，各ブロックには次のことが記録されている。[9]

- 1つ前のブロックのハッシュ値
- 取引内容[10]
  - 送金者のアドレス
  - 受領者のアドレス
  - 送金金額

ブロックチェーン（blockchain）とは，このようなブロックが連なったチェーン状の記録である。

マイナー（miner）とは，暗号資産取引の記録であるブロックを承認・形成することによって，報酬を得ようとするP2P上のノードである（図1）。マイナーがブロックの承認・形成を試みることは，**マイニング**（mining）と呼ばれる。マイナーはマイニングを行うにあたって，まず，以前に形成されたブロックが正しく形成されていること（**真正性**）を確認する。上述のように，ブロックの中には「1つ前のブロックのハッシュ値」が含まれ，これには1つ前のブロック以前におけるすべての取引情報が反映されている。そのため，マイナーは自分がマイニングを行おうとしているブロックの「1つ前のブロックのハッシュ値」と，他のマイナーがマイニングを行おうとしているブロックの「1つ前のブロックのハッシュ値」とを比較することにより，自分のブロックの真正性を確認することができる。[11]真正性が確認されないブロックには，その後のブロックが続かないので，長く続いているブロックチェーンに真正性が付与される。

マイナーは承認・形成しようとしているブロックに，あるデータを追加したら，ブロック全体のハッシュ値の先頭z桁（$z = 1, 2, \cdots$）がすべて0となるようなデータ（**ナンス**（nonce）と呼ばれる）を発見しようとする。[12]そして，最初にナンスを発見したマイナーはP2Pにナンスを伝え，P2P上の他のマイナーはナンスが正しいことを確認する。P2P上の過半数のマイナーに正しいナンスであることが認められれば，発見者であるマイナーにブロックの承認・形成の権利が与えられ，暗号資産のシステムからマイニング

9 実際のブロックではもっと記録事項が多いが，ここでは簡略化して記している。

10 各ブロックには送金者のアドレス，受領者のアドレス記録されている。これらは，送金者，受領者，それぞれの公開鍵から作成された暗号である。これらのアドレスから，送金者，受領者の公開鍵を特定することはできない。

11 これの詳しいメカニズムについては，【附録】「ブロックチェーンによる改ざん防止のメカニズム」を参照してほしい。

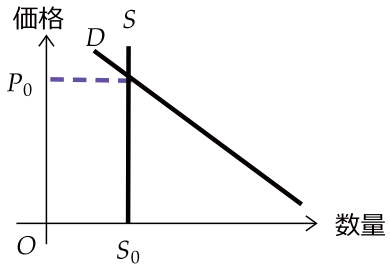
12 桁数zが大きいほど，ブロック承認・形成の難度が上がる。

報酬が支払われる[13]。このように，「マイニングに成功したマイナーがブロックを承認・形成する」という工程が繰り返されることによって，P2P 上において暗号資産の取引記録であるブロックチェーンが継続する。

Ⅲ　暗号資産に対する信念の形成：長期的課題

暗号資産による企業の資金調達を可能にするためには，投資家が安心して暗号資産を取引できる環境の整備が必要である。図 2 は，ある暗号資産について，ある時点（0 時点とする）の需要曲線 D と供給曲線 S を表している。ここでは，多数の投資家が暗号資産に対して異なる選好をもつと仮定している。そのため，需要曲線は右下がりとなっている[14]。一方，0 時点における暗号資産の供給量は，暗号資産価格にかかわらず一定（S_0 とする）であるので，供給曲線は垂直な直線となる。需給が均衡する点は（S_0, P_0）である。

図 2　暗号資産の価格決定メカニズム



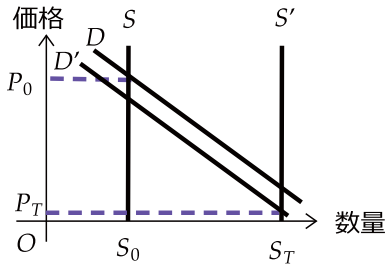
P2P 上の暗号資産の量は，マイニング報酬によってのみ増加するが，インフレ抑制のために暗号資産の供給限度は事前に決められている。そのためマイニング報酬は，時間の経過とともに減少するように設定されている。例えば，ビットコインでは供給限度は約 2,100 万 BTC であり，21 万ブロックが形成されるごとに，マイニング報酬が半減するように設定されている[15]。

図 3 は，暗号資産が供給限度に達した時点（T 時点とする）における暗号資産の需給関係を表している。T 時点の供給曲線 S' は，0 時点の供給曲線 S より大きく右にシフトしている（このときの供給量を S_T とする）。一方，暗号資産は決済手段であるので，暗号資産が供給限度に達した時点 T では，マイニング報酬がゼロであり，暗号資産の

13　この一連の過程は，**プルーフ・オブ・ワーク**（proof of work）と呼ばれ，ブロックチェーンの信頼性を保証している。
14　すべての投資家が暗号資産に対して同じ選好をもつと仮定すれば，水平な需要曲線となる。
15　ビットコイン開始時（2009 年 1 月 4 日）のマイニング報酬は，1 ブロックあたり 50BTC であった。既に 3 回半減し，現在のマイニング報酬は 1 ブロックあたり 6.25BTC である。

決済手段としての需要は非常に小さくなっている[16]。そのため T 時点の需要曲線 D' は，0 時点の需要曲線 D より下にシフトしている。需給が均衡する点を（S_T, P_T）とすると $P_T << P_0$ であり，これは暗号資産価格の暴落を意味する。

図 3　暗号資産価格の暴落



暗号資産は兌換通貨でないので，そもそも換金能力がない。そして，暗号資産にもともとの原資はないから[17]，巨額の暗号資産を返済する資金もない。この状態を放置すると，遠い将来に暗号資産価格が暴落する可能性がある。第 1 節でも述べたように，現代において暗号資産の流通額は膨大であるので，その経済的影響は計りしれない。そのため，暗号資産の暴落を防止することが，長期的かつグローバルな根本的課題である。

しかし，暗号資産に中央銀行は存在しないので，既存の金融政策は使えない。考えられる 1 つの方策は，暗号資産の決済手段としての機能が失われても，兌換通貨でない暗号資産に「価値がある」という信念を人々に共有させることである。マンキュー（2017）には，次のような例が紹介されている[18]。

> かつてヤップ島（太平洋の島）では，フェイと呼ばれる巨大な石貨が用いられていた。石貨の運搬は大変だから，島民はしだいに石貨を運搬せずに，石貨の所有権のみを貨幣として使うようになった。あるとき，嵐によって非常に高価な石貨が海に流された。このとき，島民は石貨の流出が所有者の過失ではないという理由により，海中の石貨の所有権を所有者に認めた。数世代が経過して流出前の石貨を見た人がいなくなっても，島民はこの石貨の所有権を交換手段として認めていた。

16　暗号資産の送金者は早期の取引承認を促進するために，ナンスを発見したマイナーに対して手数料を支払う。この手数料がマイナーのインセンティブとしてはたらくので，マイニング報酬がなくなっても，暗号資産の決済手段としての需要がゼロになることはない。

17　例えば，ビットコインの最初の取引（**GENESIS** と呼ばれる）においては，‘No inputs’と記録され原資はない。マイニング競争の勝者に対して，50BTC のマイニング報酬が支払われているだけである。この取引は，下記から閲覧可能である。
https://chainflyer.bitflyer.jp/Transaction/4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

18　この部分は，マンキュー（2017），p.118 の要約である。

この例と同様に，「目に見えない資産に価値がある」という信念を人々に共有させることが，将来における暗号資産価格の暴落を回避する 1 つの有力な手段であると考えられる。これは，グローバルな長期的課題である。これを解決するにはには，次節で示す短期的課題を 1 つ 1 つ，解決することが必要であると考えられる。

Ⅳ　暗号資産価格の安定と会計数値への信頼性付与：短期的課題

(1) 投資家のセンチメントの解明

長期的に「暗号資産には価値がある」という信念を人々に共有させるためには，暗号資産市場を継続的に発展させなければならない。そのためには，短期的に暗号資産価格のボラティリティを小さくすることが重要である。一般に，暗号資産価格は通貨危機，発行主体による暗号資産の買戻し（バーン（burn））などによって変動する。そして，暗号資産価格のボラティリティを増大させる原因として，次の 3 つが考えられる[19]。

① 暗号資産市場では，洗練された（sophisticated）投資家に比べて，ナイーブな（naive）投資家の比率が大きい。
② 暗号資産市場では，1 日あたりの取引額が比較的小さい。
③ 暗号資産市場には，ストップ安・ストップ高の規制がない。

この中で最も根本的な原因は，①であろう。なぜなら②③は，ナイーブな投資家の取引によって生じた価格ボラティリティを，さらに大きくする要因であると考えられるからである。

ここでナイーブな投資家は，伝統的経済学が想定する合理的経済人ではない。合理的経済人は，あらゆる情報を用いて瞬時に経済合理的な行動ができる。しかし，ナイーブな投資家はすべての情報を有しているわけではなく，それを瞬時に判断して取引を行う能力もない。そして，ナイーブな投資家の意思決定は時として，感情的・心理的影響を受けることがある[20]。暗号資産市場では，ナイーブな投資家の比率が大きいので，ナイーブな投資家のセンチメントが市場に与える影響は大きくなると考えられる。

従って，暗号資産価格のボラティリティを小さくするためには，ナイーブな投資家のセンチメントの発生メカニズムを解明し，それをコントロールすることが重要である。そのために理論的研究では，合理的経済人仮説を前提としない行動経済学・行動ファイ

19　例えば，Coincheck の以下のウェブサイトを参照してほしい。https://coincheck.com/ja/article/271
20　現実の人間は合理的経済人ではない。これは，洗練された投資家も同様である。しかし，ナイーブな投資家は洗練された投資家より，その性質が合理的経済人からの乖離が大きいと考えらえる。

ナンスの知見が有用である[21]。実証研究では，ナイーブな投資家のセンチメントデータの蓄積と分析が重要である。筆者らの研究グループは，2002 年から 2007 年にわたって 3 か月ごとに，世界中の財務担当役員（Chief Financial Officer: CFO）を対象に，自国経済に対する楽観度と自社に対する楽観度について，サーベイ調査を行った[22]。暗号資産市場についても，ナイーブな投資家のセンチメントの解明のために，同様の国際的なサーベイ研究が有用であると考えられる。

（2）会計規制・監査制度の革新

暗号資産による企業の資金調達を促進するためには，企業が開示する会計数値に信頼性を付与しなければならない。これはローカルな短期的課題であり，各国において会計規制と監査制度の充実が必要である。従来の会計規制・監査制度は，企業の会計帳簿を会計証憑によって確認することにより，会計数値の信頼性を保証しようとしてきた。しかし，第Ⅱ節でも述べたように，暗号資産の取引情報は，暗号化されたデジタル情報である。そのため，従来の会計処理・監査手続の実行が非常に困難である[23]。ここで発想の転換が必要である。すなわち，会計帳簿を会計証憑によって確認するのではなく，経営者に会計不正を行わせないように動機づけすることが，会計数値の信頼性を確保する上で重要であると考えられる。

経営者は正しい会計数値を公表しない傾向がある。例えば業績不振のとき，株主や債権者に企業業績を知られなくないため，粉飾を行う傾向がある。一方，業績好調のとき，租税回避のために逆粉飾を行う傾向がある。そもそも人は嘘をつく傾向があり，会計不正はその 1 つの例である。それなら，「嘘をつくインセンティブそのものを削減する」という発想への転換が重要である。人が嘘をつくメカニズムについては，経済学や心理学において多くの知見が蓄積されており[24]，その利用が有用であると考えられる。

しかし，これだけでは十分でない。第Ⅱ節で述べたように，暗号資産のブロックチェーンの改ざんは現実的に不可能である。そのため，経営者が会計不正を行う方法は，企業内部での会計操作に限定される。これを防止するには，企業の内部統制制度の充実

21　加藤・岡田（2010）は行動経済学を基盤として，投資家のセンチメントをわかりやすく検討している（pp.88-97）。

22　その調査結果の一部は，井上・山﨑・山本（2013）にまとめられており，以下のサイトにもある。http://www.iee.e.titech.ac.jp/~inouelab/cfo/index.htm

23　現時点で暗号資産の会計処理規定は，企業会計基準委員会・実務対応報告第 38 号「資金決済法における暗号資産の会計処理等に関する当面の取扱い」（2018 年）だけである。一方，常に発展を続ける暗号通貨技術に対して，確立された監査手続は存在しない。

24　例えば，Cao, Li, and Niu（2022），Erat and Gneezy（2012），Geraldes, Heinicke, and Kim（2021），Gibson, Tanner, and Wagner（2013），Gneezy（2005），Gneezy, Imas, and Madarász（2014），Gneezy, Kajackaite, and Sobel（2018），Kandul and Kirchkamp（2018），Shalvi, Eldar, and Bereby-Meyer（2012）などがある。

とそれに対する監査が不可欠である。但し，内部統制制度の監査には限界がある。なぜなら，常時，企業を監督する経営者と，一定の時期にのみ往査を行う監査人との間において，情報の非対称性は非常に大きい。これを解決する 1 つの方法として，内部通報制度が考えられる。

人は嘘をついている時は，罪悪感を感じる。従業員が経営者の指示により自分の意思に反して嘘をついているとしたら，罪悪感はいっそう大きい[25]。そこで，通報者の本人情報の秘匿を保証して内部通報を受信する機関を企業外部に確立することは，新しい時代において，会計数値の信頼性を高める 1 つの有力な方法であると考えられる。これについては，ビジネス倫理学において多くの知見の蓄積があるので[26]，その利用が有用である。

V　む　す　び

本研究では，「暗号資産によって革新的な技術をもつベンチャー企業の資金調達が容易になれば，社会全体が幸せになる」という前提で，この実現に向けての研究アプローチを検討した。

もっとも重要な課題は，人々が安心して暗号資産取引を行う環境を整備することである。暗号資産は決済手段であり，基本的にマイニング報酬のみによって供給量が増加するが，供給限度が決められている。そのため，供給限度に達した暗号資産には，もはやマイニング報酬が支払われることはなく，決済手段としての機能が大きく低下する。このとき考えられる 1 つのシナリオは，暗号資産価格の暴落である。これを回避する政策を提示することが，グルーバルな長期的課題である。1 つの解決方法は，兌換通貨ではない暗号資産について，「価値がある」という信念を人々に共有させることである。そのためには，次の 2 つの短期的課題の解決により，暗号資産市場を継続的に発展させることが必要である。

第一の短期的課題は，暗号資産価格のボラティリティの削減である。そのためには，暗号資産市場においてマジョリティを占めるナイーブな投資家のセンチメントを解明することが重要である。理論的研究としては行動経済学・行動ファイナンスの知見が有用であり，実証研究としては国際的なサーベイ調査によって，投資家センチメントのデータを蓄積・分析することが有用であると考えられる。

第二の短期的課題は，会計規制・監査制度の革新である。暗号資産の取引記録は暗号化されたデジタル情報であるため，「証憑による会計記録の確認」という従来の会計手

25　Gneezy *et al*.（2018），Shalvi *et al*.（2012）より。
26　内部通報制度についてのサーベイ論文として，Lee and Xiao（2018）がある。

続は困難である。ここで，発想の転換が必要である。すなわち，「証憑によって会計記録を確認する」のではなく，「経営者の会計不正のインセンティブそのものを削減する」ことが重要である。これについては，経済学・心理学の知見が有用である。しかし，それだけでは十分でない。暗号資産による資金調達を促進するためには，企業のディスクロージャーに信頼性を付与することが重要である。そのためには，会計不正を告発する内部通報制度の確立が不可欠である。

暗号資産の技術は日々進歩し，そのスピードは非常に速いので，技術発展の後追いの改革は有効でない。むしろ，暗号資産取引の基本的な構造を前提とし，暗号資産取引という大きな枠組に対して緩やかな方針を示すことが重要である。そして，その方針のもとで暗号資産取引の技術発展に応じて，それぞれの課題の解決方法を具体化することが適切であると考えられる。

参考文献

［1］Cao, Q., J. Li, and X. Niu（2022）, White lies in tournaments, *Journal of Behavioral and Experimental Economics* 96, pp.1-11.

［2］Erat, S., and U. Gneezy（2012）, White lies, *Management Science* 58（4）, pp.723-733.

［3］Geraldes, D., F. Heinicke, and D. G. Kim（2021）, Big and small lies, *Journal of Behavioral and Experimental Economics* 91, pp.1-12.

［4］Gibson. R., C. Tanner, and A. F. Wagner（2013）, Preferences for truthfulness: Heterogeneity among and within individuals, *American Economic Review* 103（1）, pp.532-548.

［5］Gneezy, U.（2005）, Deception: The role of consequences, *American Economic Review* 95（1）, pp.384-394.

［6］Gneezy, U., A. Imas, and K. Madarász（2014）, Conscience accounting: Emotion dynamics and social behavior, *Management Science* 60（11）, pp.2645-2658.

［7］Gneezy, U., A. Kajackaite, and J. Sobel（2018）, Lying aversion and the size of the lie, *American Economic Review* 108（2）, pp.419-453.

［8］Kandul, S., and O. Kirchkamp（2018）, Do I care if others lie?: Current and future effects when lies can be delegated, *Journal of Behavioral and Experimental Economics* 74, pp.70-78.

［9］Lee, G. and X, Xiao（2018）, Whistleblowing on accounting-related misconduct: A synthesis of the literature, *Journal of Accounting Literature* 41, pp.22-46.

［10］Nakamoto, S.（2009）Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org.

［11］Shalvi, S., O. Eldar, and Y. Bereby-Meyer（2012）, Honesty requires time（and lack of justifications）, *Psychological Science* 23（10）, pp.1264-1270.

［12］EY 新日本有限責任監査法人（2018）『図解でスッキリ　仮想通貨の会計とブロックチェーンのしくみ』中央経済社.

［13］PwC あらた有限責任監査法人（2018）『仮想通貨の会計・税務・監査』中央経済社.

［14］井上光太郎・山﨑尚志・山本達司（2013）「グローバル CFO サーベイ開始 1 年の報告」『CFO FORUM』第 47 巻，pp.7-11.

［15］大垣昌夫・田中沙織（2018）『行動経済学〔新版〕　－伝統的経済学との統合による新

しい経済学を目指して－』有斐閣.
［16］岡嶋裕史（2019）『ブロックチェーン　－相互不信が実現する新しいセキュリティ－』講談社.
［17］加嵜長門・篠原航（2018）『ブロックチェーンアプリケーション開発の教科書』マイナビ出版.
［18］加藤英明・岡田克彦（2010）『人生に失敗する 18 の錯覚　－行動経済学から学ぶ想像力の正しい使い方－』講談社.
［19］木村史彦・山本達司（2013）「倒産企業の資金調達と会計操作」『現代ディスクロージャー研究』第 13 号，pp.49-63.
［20］木村史彦・山本達司・辻川尚起（2004）「倒産企業の会計操作」『會計』第 166 巻第 1 号，pp.112-126.
［21］小島寛之（2019）『暗号通貨の経済学　－21 世紀の貨幣論－』講談社.
［22］須田一幸・山本達司・乙政正太（2007）『会計操作　－その実態と識別法，株価への影響－』ダイヤモンド社.
［23］長沼伸一郎（2020）『現代経済学の直観的方法』講談社.
［24］野口悠紀雄（2014）『仮想通貨革命　－ビットコインは始まりにすぎない－』ダイヤモンド社.
［25］野口悠紀雄（2017）『ブロックチェーン革命　－分散自律型社会の出現－』日本経済新聞出版社.
［26］マンキュー，N. G.（2017）（足立英之・地主敏樹・中谷武・柳川隆訳）『マンキューマクロ経済学 I　入門篇（第 4 版）』東洋経済新報社.
［27］山崎重一郎・安土茂亨・田中俊太郎（2017）『ブロックチェーン・プログラミング　－仮想通貨入門－』講談社.
［28］山本達司（2009）「株式所有構造と利益マネジメント」『管理会計学』第 17 巻第 2 号，pp.3-21.
［29］山本達司（2020）「ビットコインの潜在的リスク」『同志社商学』第 71 巻第 5 号，pp.115-128.
［30］山本達司（2023）『財務会計のファンダメンタルズ』中央経済社.
［31］山本達司・田口聡志・三輪一統（2021）「粗雑なシグナルか，精緻なシグナルか？　－逆淘汰防止のための経営管理ツールの構築に向けて－」『メルコ管理会計研究』第 12 号－Ⅱ，pp.47-62.

【附録】

ブロックチェーンによる改ざん防止のメカニズム

ここでは，簡単な数値例を用いて，ブロックチェーンによる改ざん防止のメカニズムを概観する。具体的には，次のような送金データの改ざんを防止する方法を検討する。

送金データ（*message*）

	day	*time*	*id*	*yen*
取引 1	1	1200	1	5,000
取引 2	1	1201	1	10,000

（*day*：取引日，*time*：取引時刻，*id*：取引記録者の番号，*yen*：送金額）

ここにおいて，取引のハッシュ値 h を生成するハッシュ関数を次のように定義する。[27]

$$h = [\underbrace{(day \text{ と } time \text{ を並べた数字} + id) \times yen}_{\text{取引の情報 } m} \text{を 999 で割った余り}]$$

（1）ハッシュ値による改ざん防止の効果

取引 1 の情報 m_1，取引 2 の情報 m_2 から得られるそれぞれの正しいハッシュ値 h_1, h_2 は，次のように求められる。

$m_1 = (11200 + 1) \times \underline{5{,}000} = 56{,}005{,}000 = 999 \times 56{,}061 + 61$ だから，$h_1 = 61$

$m_2 = (11201 + 1) \times 10{,}000 = 112{,}020{,}000 = 999 \times 112{,}132 + 132$ だから，$h_2 = 132$

ここで，取引 1 と取引 2 の正しい記録が P2P 上のすべてのノードで完了し，その上で，あるノードが取引 1 のデータを $\underline{yen = 5{,}001}$ に改ざんするとしよう。このとき，取引 1 の情報 $\widetilde{m_1}$，取引 2 の情報 $\widetilde{m_2}$ から得られるそれぞれのハッシュ値 $\widetilde{h_1}$，$\widetilde{h_2}$ は，次のようになる。

$\widetilde{m_1} = (11200 + 1) \times \underline{5{,}001} = 56{,}016{,}201 = 999 \times 56{,}072 + 273$ だから，$\widetilde{h_1}$ =273

$\widetilde{m_2} = (11201 + 1) \times 10{,}000 = 112{,}020{,}000 = 999 \times 112{,}132 + 132$ だから，$\widetilde{h_2} = 132$

このとき，$h_1 = 61 \neq \widetilde{h_1} = 273$ により，改ざんは発覚しそうであるが，もし改ざん者がすべてのノードについて取引 1 の記録を改ざんすれば，改ざんに成功する。そ

27　任意の整数を 999 で割った余りは，0 から 998 までの整数であり，これを 000 から 998 までとみなすと，この関数は送金データから 3 桁のデータ（固定長）を出力する関数であり，ハッシュ関数の要件を満たしている。

して，$h_2 = \widetilde{h_2} = 132$ だから，取引 2 については改ざんの必要はない。そのため，より強力な改ざん防止手段が求められ，その 1 つがブロックチェーンである。

（2）記録のブロックチェーン化による改ざん防止の強化

記録をブロックチェーン化するためには，ハッシュ関数を次のように変更すればよい。

$$H = [\underbrace{(day \text{ と } time \text{ を並べた数字} + id) \times (yen + 1 \text{ つ前のブロックのハッシュ値})}_{\text{取引の情報 } M} \text{を 999 で割った余り}]$$

取引 1 の 1 つ前のブロックのハッシュ値を $h_0 = 0$ とし，取引 1 の情報を M_1，取引 2 の情報を M_2 とすると，取引 1，取引 2，それぞれの正しいハッシュ値 H_1, H_2 は，次のように求められる。

$M_1 = (11200 + 1) \times (5{,}000 + 0) = 56{,}005{,}000 = 999 \times 56{,}061 + 61$ だから，$H_1 = 61$

$M_2 = (11201 + 1) \times (10{,}000 + \underline{61}) = 112{,}703{,}322 = 999 \times 112{,}816 + 138$ だから，$H_2 = 138$

ここで，取引 1 と取引 2 の正しい記録が P2P 上のすべてのノードで完了し，その上で，あるノードが取引 1 のデータを $\underline{yen = 5{,}001 \text{ に改ざん}}$するとしよう。このとき，取引 1 の情報 $\widetilde{M}_1$ と取引 2 の情報 $\widetilde{M}_2$ から得られるそれぞれのハッシュ値 $\widetilde{H}_1$，$\widetilde{H}_2$ は，次のようになる。

$\widetilde{M}_1 = (11200 + 1) \times (\underline{5{,}001} + 0) = 56{,}016{,}201 = 999 \times 56{,}072 + 273$ だから，$\widetilde{H}_1 = 273$

$\widetilde{M}_2 = (11201 + 1) \times (10{,}000 + \underline{273}) = 115{,}078{,}146 = 999 \times 115{,}193 + 339$ だから，$\widetilde{H}_2 = 339$

このとき，$H_1 = 61 \neq \widetilde{H}_1 = 273$ により，改ざんは発覚しそうである。そして，たとえ改ざん者がすべてのノードについて取引 1 の記録を改ざんしたとしても，$H_2 = 138 \neq \widetilde{H}_2 = 339$ により，取引 2 より以前のどこかで改ざんが行われたことが発覚し，結果的に取引 1 の改ざんが発覚する。つまり，記録のブロックチェーン化により，改ざん者は取引 2 の正しい記録を有効利用できず，すべてのノードについて取引 2 の記録を書き換える必要がある。

このことを一般化すると，過去の取引記録を改ざんするためには，P2P 上のすべてのノードについて，改ざん時点から最新時点まで，すべての記録を書き換えなければならなくなり，現実的に改ざんは不可能となる。これが，記録のブロックチェーン化による改ざん防止強化の効果である。

（3）マイニングの仕組み

記録のブロックチェーン化によって，改ざんの防止が強化されたことは確認されたが，問題は「**誰がブロックの承認・形成を行うか**」である。つまり，P2P 上の

ノード（具体的には，マイナー）にインセンティブを与えなければならない。そこで次のようなゲームを行い，ゲームの勝者にブロックの承認・形成権とマイニング報酬を与えることにする。

「送金データ *message* にあるデータ n を書込み，送金記録全体のハッシュ値が一定の条件を満たす $n = \hat{n}$（ナンス）を最初に見つけたノードにブロックの承認・形成権を与える。」

先の数値例を用いて，次のようなゲームを設定することにしよう。

〈ゲーム〉

「取引のハッシュ値 η を生成するハッシュ関数を

$\eta =$［(*day* と *time* を並べた数字+*id*)×(*yen*+前の取引の *hash*)×n を 999 で割った余り］（*）

として，ハッシュ値 η の先頭の 2 桁が 00 となるナンス $n = \hat{n}$ を見つけなさい[28]。」

この問題を解く，数学的アルゴリズムは開発されていない。そこで，マイナーはナンスの候補 n に適当な値を代入して，しらみつぶしにナンス $n = \hat{n}$ を見つけなければならない。一方，それが正解であることを確認する作業は容易である。なぜなら，（*）式に $n = \hat{n}$ を代入して，ハッシュ値 η の先頭の 2 桁が 00 となることを確かめればよいからである。

取引 1，取引 2，それぞれのナンス n_1, n_2 とハッシュ値 η_1, η_2 は，次のように求められる。

- $\eta_1 = (11200 + 1) \times (5{,}000 + 0) \times n_1$ を 999 で割った余りが 1 桁の整数となる n_1 の一例は $n_1 = 82$ であり，このとき $\eta_1 = 7$（1 桁の整数）である。

  $\eta_1 = (11200 + 1) \times (5{,}000 + 0) \times \underline{82} = 4{,}592{,}410{,}000 = 999 \times 4{,}597{,}007 + \underline{7}$
- $\eta_2 = (11201 + 1) \times (10{,}000 + 7) \times n_2$ を 999 で割った余りが 1 桁の整数となる n_2 の一例は $n_2 = 309$ であり，このとき $\eta_2 = 9$（1 桁の整数）である。

  $\eta_2 = (11201 + 1) \times (10{,}000 + 7) \times \underline{309} = 34{,}638{,}409{,}926 = 999 \times 34{,}673{,}083 + \underline{9}$

ここで，取引 1 と取引 2 の正しい記録が P2P 上のすべてのノードで完了し，その上で，あるノードが取引 1 のデータを $\underline{yen = 5{,}001 \text{ に改ざん}}$するとしよう。このと

28　任意の整数を 999 で割った余りは，0 から 998 までの整数であり，これを 000 から 998 までとみなすと，そのうち先頭の 2 桁が 00 である余りは 1 桁の整数である。従って，ハッシュ値 η は 1 桁の整数である。

き，取引 1，取引 2，それぞれのナンス $\widetilde{n_1}$，$\widetilde{n_2}$ とハッシュ値 $\widetilde{\eta_1}$，$\widetilde{\eta_2}$ は，次のようになる。

- $\widetilde{\eta_1} = (11200+1) \times (\underline{5{,}001}+0) \times \widetilde{n_1}$ を 999 で割った余りが 1 桁の整数となる $\widetilde{n_1}$ の一例は $\widetilde{n_1} = 11$ であり，このとき $\widetilde{\eta_1} = 6$（1 桁の整数）である。
  $\widetilde{\eta_1} = (11200+1) \times (\underline{5{,}001}+0) \times \underline{11} = 616{,}178{,}211 = 999 \times 616{,}795 + \underline{6}$
- $\widetilde{\eta_2} = (11201+1) \times (10{,}000+6) \times \widetilde{n_2}$ を 999 で割った余りが 1 桁の整数となる $\widetilde{n_2}$ の一例は $\widetilde{n_2} = 158$ であり，このとき $\widetilde{\eta_2} = 3$（1 桁の整数）である。
  $\widetilde{\eta_2} = (11201+1) \times (10{,}000+6) \times \underline{158} = 17{,}709{,}779{,}496 = 999 \times 17{,}727{,}507 + \underline{3}$

このとき，$\eta_1 = 7 \neq \widetilde{\eta_1} = 6$ により，改ざんは発覚しそうである。そして，たとえ改ざん者がすべてのノードについて取引 1 の記録を改ざんしたとしても，$\eta_2 = 9 \neq \widetilde{\eta_2} = 3$ により，取引 2 より以前のどこかで改ざんが行われたことが発覚し，結果的に取引 1 の改ざんが発覚する。つまり，ブロックチェーンにマイニングの仕組みを取り入れても，ブロックチェーンによる改ざんの防止の強化は有効である。

但し，一般に 1 つの取引に対して複数個のナンス $\hat{n}$ が存在する。マイナーの誰かが $\widetilde{n_2} = 141$ を発見すると，$\widetilde{\eta_2} = 9$ となり，$\eta_2 = 9$ と一致してしまい，取引 1 の改ざんが発覚しにくくなる。

$$\widetilde{\eta_2} = (11201+1) \times (10{,}000+6) \times \underline{141} = 15{,}804{,}296{,}892 = 999 \times 15{,}820{,}117 + \underline{9}$$

このような状態を避けるために，ゲームのルールを，

「取引のハッシュ値 η を生成するハッシュ関数を
η=[（*day* と *time* を並べた数字+*id*）×（*yen*+前の取引の *hash*）×*n* を 99999 で割った余り]
として，η の先頭の 2 桁が 00 となるナンス $n = \hat{n}$ を見つけなさい。」

などとすると，ハッシュ値が 3 桁となるので，ハッシュ値の衝突が起こりにくくなる[29]。

まとめると，次のようになる。

29　任意の整数を 99999 で割った余りは 0 から 99998 までの整数だから，ハッシュ値は 00000 から 99998 までの整数である。そのため，先頭の 2 桁が 00 であるハッシュ値は 3 桁の整数となる。

	正しい／改ざん	取引 1	取引 2
(1) ハッシュ値のみ	正しい	$h_1 = 61$	$h_2 = 132$
	改ざん	$\widetilde{h_1} = \underline{273}$	$\widetilde{h_2} = 132$
(2) ブロックチェーン化	正しい	$H_1 = 61$	$H_2 = 138$
	改ざん	$\widetilde{H_1} = \underline{273}$	$\widetilde{H_2} = \underline{339}$
(3) マイニングの導入	正しい	$\eta_1 = 7$	$\eta_2 = 9$
		$n_1 = 82$	$n_2 = 309$
	改ざん	$\widetilde{\eta_1} = \underline{6}$	$\widetilde{\eta_2} = \underline{3}$
		$\widetilde{n_1} = 11$	$\widetilde{n_2} = 158$
	改ざん（ハッシュ値の衝突）		$\widetilde{\eta_2} = 9$ (!)
			$\widetilde{n_2} = 141$