http://financialcryptography.com/mt/archives/001325.html

[**Financial Cryptography**](https://financialcryptography.com/)

暗号化と金融制度の狭間にて

[« Bitcoin and tulip bulbs](https://financialcryptography.com/mt/archives/001324.html) | [Main](https://financialcryptography.com/) | [BitCoin - the bad news »](https://financialcryptography.com/mt/archives/001327.html)

**2011年6月13日**

**ビットコインは三式簿記システム足りえるのか？**

*最近、James Donaldが*[*この興味深い疑問を考察する上で*](http://lists.randombit.net/pipermail/cryptography/2011-June/000789.html)*挑戦を投げかけてきました。肝心な部分を抽出するのに*[*時間がかかりましたが*](http://financialcryptography.com/mt/archives/001324.html)*、全体の骨格が見えてきた感じがします。*

*13/06/11 12:56 PM、James A. Donald より：  
> 2011-06-12 8:57 AM, Ian G より：  
> > John Levineが提唱した2000年に提唱した、学習不足についての文書、「*[*金融システムにおける暗号化の7段階*](http://iang.org/papers/fc7.html)*」について、*[*考察を加えました*](http://lists.randombit.net/pipermail/cryptography/2011-June/000754.html)。*> > 明確に主張されていませんが、元の文献の骨子は次の通りです：金融システムにおける暗号化について理解するには、多方面の専門知識を有する必要があり、最高7つの分野においてそれを行う必要がある。デジタル通貨関連スタートアップのほとんどは、そうした専門知識を有していないため、非常に困難な課題でした。*[*あなたが言及した分野の一つに、会計があります。*](http://lists.randombit.net/pipermail/cryptography/2011-June/000767.html)

そうです。暗号化、少なくとも金融制度における暗号化、に話を戻しましょう。

金融システム内の暗号化部分において実装されている通貨システムの会計レイヤーは、ある事例に関する全体のバランスシートを作成するために、全ての取引記録を保有して報告（１）できるように作成されています。

ビットコインが最も大きな影響力を駆使できるのは恐らくこの分野であり、世界初の大規模な[三式簿記](http://iang.org/papers/triple_entry.html) （2）の実証を行ったと見なせるかもしれません。

三式簿記は会計における革命ですが、思想は簡単です。三式簿記には当事者が3者存在し、そこではアリスがボブに支払い、イワンが調停を行います。イワンは取引を一旦保留し、写しを3通作成します。

取引を完了させるために、アリスは彼女の公開鍵を元にして行った署名（３）と共に、支払手順指示をボブに送ります。発行人であるイワンは、アリスの支払要求を領収書に変換します。そして、この領収書が取引の本体となります。

この取引は複数の当事者からデジタルで署名されます。当事者には、中立な立場の者が少なくとも一名必要です（４）。それが、強力な取引証拠（５）となります。

最終的な領収書が「入力」となります。次に、「署名済みの領収書の束」が、会計用語で言う勘定になります。この「束」が複式記入の会計方法にとって替わります。デジタル署名された領収書が一つあれば取引の入力内容が2つあるよりも強力な証拠となるからです。署名済み領収書の束は、会計チャートよりも優れた記録として機能します（５）。

[[](http://en.wikipedia.org/wiki/Luca_Pacioli)](http://en.wikipedia.org/wiki/Luca_Pacioli)複式簿記にとって替わるというのは革新的な考えであるため、古典的な会計からは少し逸脱します。[Luca Pacioli](http://en.wikipedia.org/wiki/Luca_Pacioli)というベネチアの修道士が始めて以来、複式簿記は500年にわたり企業会計の根本を成して来ました。複式簿記がここまで続いた理由はとても重要であり、暗号化に携わる人々にとっても肝心なので、少し脱線しましょう。

複式簿記は、詐欺によるエラーを検出できるという驚異的な特性を持ちます。単式簿記（数字を並べて足し合わせる行為です）の問題は、入力者が数字を操作できるので、誰も信用できない点です。（７）ある人物が、単に間違いを犯したのか、故意に詐欺を行っているのか、判別がつきません。単純な会計にはこういう弱点があるので、会計を実行可能な業務の規模は、正直な会計士を雇えるかどうか、に左右されていました。

正直な会計士とは、家族の一員を指します。他の全ての人は、たいていは雇い主の金を盗むでしょう。（家族の一員だって盗みますが、少なくとも家族の利益であることには変わりありません）ですので、1400年頃まで、ほとんどの企業は王室に所属するか（疑いのある会計士は首をはねられました）、家族経営でした。

イタリアの貿易港を通じて複式簿記が広まったことで、家族経営以外にも企業が栄えることになりました。ゆえに複式簿記は企業の根幹を成しており、現在のイタリアにある都市国家の貿易力が爆発的に発展した原因です（８）。

三式簿記に戻りましょう。デジタル署名された領収書は、簡単に移動でき、第三者による検証が可能で、コンピューターで作業しやすいために、複式簿記よりも優れています。複式簿記においては、簿記記録を一箇所に、安全に保存する必要がありますが、三式簿記には必要ありません。

署名済み領収書が完全な証拠とはならない可能性が一つだけあり、それは証拠となるデジタル情報が失われた場合です。だからこそ、アリス、ボブ、イワンが全員写しを保持するわけです。3者全員に、写しを保持しようとする動機があります：お互いを監視できるわけです。

ビットコインに戻りましょう。ビットコインは取引記録を安全に記録するために、顧客に対して分散型の公開データベースを作成することで、発行人の役割を果たしています。保管庫を公開することで偽造を防ぐアイデアは、[Todd Boyleのネット台帳設計にて初めて発表されました](http://financialcryptography.com/mt/archives/001469.html)。

私達はそれぞれ個別に、三式簿記の考えに行き着きました。それが起こったのは、三式簿記がデジタル価値をネット上で機能させる最適な方法だからでしょう。ナカモトは中央発行人を払拭するために厳しい制約を課しましたが、彼ですら同じ結論にたどり着いたように見えます。アリス、ボブ、イワン（あるいはイワン的な仕組み）が、暗号化を用いて署名された取引の同一コピーをそれぞれ保有しているわけです。

この基礎が出来上がれば、取引を行えます。

*> 2005年11月に、不良債権が本当に不良なことが、誰の目にも明らかになったことを思い出してみてください。*

2005年に、SEC（証券取引委員会）が私の三式簿記実装に着目した際・・・

*> 2005年後半から2007年後半にかけて、大手の金融機関がすでに死に体であったにも関わらず活動を続けていたのが広く知られるようになりました。それが可能だったのは、非常に狡猾な方法でルールを書き換えていたからです。*

実際に、金融業界が大混乱しているのを肌で感じることができました。SECは不安そうに三式簿記を調査していました。

私達（Todd Boyle、私、サトシ）がそれぞれ考案した三式簿記設計が2007年の金融危機に影響を及ぼすことができたかどうか、という疑問がわきます。私の考えは、手遅れだっただろう、です。しかし、別に状況を悪化させることはなかっただろうし、他の要素（９）も考慮すると、もし三式簿記が広く普及していれば、全体としては影響を及ぼせた可能性があります。

しかし、（a）必要なイノベーションの量は少なくなく、金融機関は、当たり前ですが、その全てに反対しています。

また、（b）[金融危機の根本には証券化があり](http://financialcryptography.com/mt/archives/001297.html)、それは金融に関する一切の要素を変えてしまいます（１０）。本当に、全てです。証券化がもたらす役割を理解せずに、三式簿記や不良債権や格付け機関や悪習慣や貧乏人やその他もろもろを語っても意味がありません。

でも、それこそが金融機関が望んでいることなのですが。

*> 2011年の今、不良債権が本当に不良だったことを確認するための監査は未だに行われていません。*

これは（１１）まで遡ります・・・

*> 健康的な金融制度はこうした専門知識を全てうまく活用するでしょうが、既存の金融制度はそうではありません。*

*修正：Luca Pacioliと複式簿記の年が間違っていたので直しました。*

*後記：*  
  
（１）ここで言う信頼性とは、詐欺行為などを防ぐ総合能力を指します。  
（２）この主張は、以下の内容を凝縮したものと言えるでしょう：  
http://iang.org/papers/triple\_entry.html  
（３）預金指示の中にボブが支払を署名して受領を確認するという中間作業もあります。しかし、これは最適化の過程で無くすこともできます。署名済みの取引領収書については、[Gary HowlandがSOXについて記した](http://www.systemics.com/docs/sox/overview.html)白書で詳細が得られます。  
（４）両者にとって調停の責任を負うヨーロッパの公証人を思い浮かべてください。  
（５）暗号化に携わる人々は、「拒否不能」という言葉を使いたがりますが、もはや廃れています。「拒否不能」は、拒否されました。ビットコイン白書では、「非可逆」という用語を用いています。金融機関は、「最終合意」という言葉を好んで用います。法律関係者は、「証拠」を求めます。私が法律関係者の方を採用するのは、揉め事が発生した場合は、彼らの意見の方が重要視されるからです。  
（６）文書内では明確にされていません。プログラムとその実装（事例とも呼ばれます）にてのみ、明確にされています。  
（７）こうした理屈は、会計士がコンピューターなら、適用可能であり、類似であり、一貫しているのですが・・・  
（８）会計学の歴史においては、この点は実証されたと認められていません。複式簿記と三式簿記の違いを会計システム上で確認した私にとっては、明確に実証されています。しかし、歴史家には会計システムを詳細に見る余裕はありません。彼らは古文書を解析するしか手立てがないのです。  
（９）その他必要不可欠な要素は、[投資信託スキャンダル](http://iang.org/papers/mutual_funds.html)と比べて、多くのデジタル通貨に存在する最終処理、非可逆性、拒否不能などです。  
（１０）金融危機について肝心な点全ては、ここから始まる4つの短いエッセイにまとめられています。<http://financialcryptography.com/mt/archives/001297.html>  
（１１） <http://financialcryptography.com/mt/archives/001126.html>

最近のビットコイン話題：

1. [ビットコインとチューリップバブル](http://financialcryptography.com/mt/archives/001324.html)
2. ビットコインは三式簿記システム足りえるのか？
3. [ビットコイン：悪いニュース](http://financialcryptography.com/mt/archives/001327.html)

著者： iang、2014年1月22日、02:34 PM | [トラックバック](https://financialcryptography.com/cgi-bin/mt/mt-tb.cgi?__mode=view&entry_id=1325)

18 Comments

Securitization is in theory, really great.But who is it that is to actually manage the loans, and make sure that they actually exist, that the payments are made, and so forth?

The lowest tranch on a bundle of debt has to be shares, not debt, and the people owning the lowest tranch have to be responsible for managing the bundle of debts.

Our recent securitization crashed because the people managing the debts had no interest in managing them, or whether they had any value.

The debts in the bundle, and the people managing them, all have to be in one geographical area, so that those managing the debts can look at the assets on the ground, and check out the people who are supposed to be paying the debts, and look those people in the eye.

Securitized debt should be bonds issued to a company whose major asset is a pile of loans, and whose major skill is managing loans - which is a very old form of finance.

Posted by:[James A Donald](http://blog.jim.com/) at June 13, 2011 06:25 PM

unregulated loan originators found they could access an unlimited amount of funds by paying the rating agencies for triple-A rated.As a result they no longer needed to worry about loan quality and/or borrower's qualifications ... immediately unloading the loans as triple-A rated toxic CDOs as fast as possible.There has been estimate that there was $27T in triple-A rated toxic CDO transactions during the bubble ... which would have been possibly $3T-$5T in profit, fees, and commissions between the original real-estate transaction and far backend warehousing of the CDOs (there were statements that the financial industry tripled in size as percent of GDP during the bubble off those toxic CDO transactions).I had also heard references to musical chair analogy during the height of the bubble and who would be left standing when the music stops.Zakara's "Post American World" uses a Cinderella analogy, the major players all knew they had to leave before the stroke of midnight, but most wanted to stay until the last possible minute.For the most part the individuals all walk away with what they wanted ... it was some of the institutions that were left holding the toxic CDOs.

Posted by:[Lynn Wheeler](http://www.garlic.com/~lynn/) at June 13, 2011 08:11 PM

Note that securitized instruments had been used during the S&L failure with fraudulent documents.In the late 90s we had been asked to look at processes that might be used to significantly improve the trust & integrity of the supporting documents (the magnitude of the problem in the S&L failure was much smaller not having the triple-A ratings).

Being able to pay for triple-A ratings on the CDOs, much of the supporting documentation became superfluous and the unregulated loan originators could make no-documentation loans.No-documentation, no-down, 1% interest only ARMs became very attractive to speculators ... during the bubble some sectors of the country had 20-30% real-estate inflation & speculators could make 2000% ROI.

Posted by:[Lynn Wheeler](http://www.garlic.com/~lynn/) at June 14, 2011 09:06 AM

one of the items pointed out in the "wall street money machine" was the frequent enormous disconnect between the compensation for individuals packaging and dealing the triple-A rated toxic CDOs and their institutions ... individuals motivated to repeatedly engage in activities that could easily take down the institution (if it weren't for gov. bailouts); there has been periodic references that the environment represents enormous "moral hazard".

Posted by:[Lynn Wheeler](http://www.garlic.com/~lynn/) at June 14, 2011 01:45 PM

Linking triple accounting to a public database of expenditures is interesting... the network becomes the third party.

Incidentally, are you aware this post is completely unreadable in the RSS feed?All the formatting is gone and the whitespace removed.

Posted by:[gwern](http://www.gwern.net/Bitcoin%20is%20Worse%20is%20Better) at June 28, 2011 11:23 AM