http://financialcryptography.com/mt/archives/001469.html

[**金融システムにおける暗号化**](https://financialcryptography.com/)

暗号化が金融制度に進出した場合…

[« Digital Currencies get their mojo back: the Ripple protocol](https://financialcryptography.com/mt/archives/001467.html) | [Main](https://financialcryptography.com/) | [Hard Truths about the Hard Business of finding Hard Random Numbers »](https://financialcryptography.com/mt/archives/001471.html)

**2014年1月22日**

**共用レポジトリの発明者：ビットコイン、Boyle、経緯**

[[](http://en.wikipedia.org/wiki/Luca_Pacioli)](http://en.wikipedia.org/wiki/Luca_Pacioli)共用取引レポジトリ（STR）を考案したのはTodd Boyleだ、と以前書きました。

*「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*](http://financialcryptography.com/mt/archives/001325.html)。*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。」*

これについては私達の間で意見の相違があり、学術的炎上の寸前まで行きましたが、ビットコインの発展と、ブロックチェーンと呼ばれる台帳の公開制度により、Toddのアイデアが再度注目されています。

過去のいきさつが気になる点であり、この経緯を追っている学生であるLuukから問いただされたこともあり、私はようやく調査に乗り出しました。残念ながら、Toddはネットを離れ、他の分野にて活躍しています。しかしwayback machine（インターネットアーカイブ）には彼の記述が残されており([GLT-GLR](https://web.archive.org/web/20070920010046/http://ledgerism.net/GLT-GLR.htm)、[STR](https://web.archive.org/web/20070312235353/http://ledgerism.net/STR.htm)、[CDEAの死](https://web.archive.org/web/20071001201740/http://www.ledgerism.net/GLSchema1.txt))、私はGLT（標準取引台帳）や世界中の取引を扱うウェブサーバーに関する以下の彼の考察を発見しました。

[*三式簿記は次のように定義されます*](https://web.archive.org/web/20070920010046/http://ledgerism.net/GLT-GLR.htm)：*自分の「標準取引台帳（GLT）」内にて取引を作成します。GLTは全て、外部の人間に名称を与えなければなりません。...例えば、顧客の実名や、公開されている納入業者IDなどです。ドメイン名やメールアドレスが公共の名前空間を成しているのと同様です。*

*投稿すると、取引はいつもと同じように、（GLT）内部に保存されます。しかし、同時に、あらかじめ選択しておいた「共有取引保管庫」内にある三式簿記にも入力されます。多分、その保管庫は自分のSTRサーバー（GL内のSTRモジュールなど）になるでしょう。あるいは、ExodusやISP、あるいはBSP内にある巨大なSTRサーバーかもしれません。GLTに入力したのと全く同じ情報を、STRと自分のStubに対する共用入力に用いることができます。*

*...  
3. GLTはコミュニティ資産の様相を呈しています。取引の一部を共有場所へ移そう、と参加者の間で真の合意が得られない限り、私達が目指している統合型経済は達成できません。私は「公開」とは言っていません。「共有」と言いたいのです。取引の金額、日時、説明は、原則的に2者間で共有されており、この2者だけが見られるように保管されるべきです。つまり、システム上で個人許可を得るか、2者のみが閲覧できるように暗号化するか、が必要となります。*

私には、2003年まで溯るこのアイデアが、原典の一部と見なせます。私はこのアイデアには関与しません。ビットコインで実装されている公開台帳はプライバシー侵害の点でとんでもないしろものだ、と私は考えているからです。ただし、市場は大して問題にならない、と判断したようです。興味深いことに、最近の記事では珍しく、Marc Andreesenが自らこう発言しています：

*...*[*ビットコインはその根本において、*](http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/?_php=true&_type=blogs&_r=0)*コンピューター工学の革命であり、世界中の数壱千もの研究者による、20年に及ぶ暗号化通貨の開発と、40年に及ぶ暗号化の研究の成果です。*

1995年から暗号化通貨に取り組んできた者として、この経緯がどう推移していったか、私はよく理解しています。サトシ・ナカモトは先人達が既に築いた財産の上に立っています。彼の設計したものは、既に実証され、様々な理由から必要だ、と判断された要素をうまく組み合わせることで成り立っています。

公開台帳、あるいは共有台帳はビットコインで実装された要素の一つであり、その意味において、Toddは歴史的に認識されるべきだと私は考えています。

Todd Boyleへ！デジタル通貨に起業の活路を見出そうとしてきた私達は、あなたに感謝します。

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=1469)