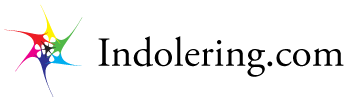
[**Indolering**](http://www.indolering.com/)



ユーザビリティとデザインの開発

|  |  |
| --- | --- |
| [Home](http://www.indolering.com/) [Contact](http://www.indolering.com/rates) [Portfolio](http://www.indolering.com/portfolio) [Calendar](http://www.indolering.com/calendar) | |
| [偽造不能なビットコイン硬貨](http://www.indolering.com/puf-bitcoin) |  |
| in [Namecoin](http://www.indolering.com/category/namecoin), [Research](http://www.indolering.com/category/research)  現時点の「実体を持つ」ビットコインのシステムに潜む問題は、発行コストは O(1+v\*m\*n) (*初期投資* + *ビットコイン価格* x *材料費* x *n)* に従って増えていくのに、偽造攻撃にかかるコストはたったの O(1+m\*n)で済む点です。Namecoinの個々の硬貨内に、単方向のハッシュを物理的に内蔵すれば、硬貨を「偽造不能」にして、攻撃にかかるコストも、製造コストに比例させることができます。これは、ビットコインのみならず、硬貨一般についても革命的な発明です。 | |
| 以下、文法に誤りがある場合が多いので、コメント欄にて修正を受け付けます。) | |
| どんな通貨であれ、偽造する場合は、調査と設備の準備のために初期費用が必要となり、後は発行数に応じて維持費がかかります。例えば、1ドル札を偽造する場合、印刷機を購入して、紙幣の構造を解析するのに多大な時間をかけなければなりません。しかし、その初期投資さえ済んでしまえば、各ドル札を印刷するのにわずか[$0.10](http://www.federalreserve.gov/faqs/currency_12771.htm) しかかかりません。ゆえに、通貨の保護は*主に*警察の努力と国際政治上の提携に委ねられています。それでもなお、ドル札を偽造するのは多大な利益を伴うため、[大規模な偽造行為](https://en.wikipedia.org/wiki/Superdollar)は今でも存在します。  通貨の偽造コストは、コンピューター工学にて複雑性を計算する方法と同じやり方で割り出せます。既存の通貨に対する攻撃は、初回時にかかる費用 *c* と発行数に応じてかかる材料費 *n* にわけて計算できます。O(1 x *c + m x n*) または *初回費用 + 材料費 x 硬貨数*  コンピューター処理上の問題の難易度を計算する場合、問題となる箇所は一般的に n なので、コンピューター工学の研究者は通常、c を無視します。硬貨数が増えれば、初回費用の影響は少なくなっていきます。やがては、材料費 x n（硬貨数）が初回費用 c を大幅に上回るようになります。  もっと実体に即した例で考えてみましょう。[ビットコイン硬貨](https://en.bitcoin.it/wiki/Casascius_physical_bitcoins)の偽造コストを例にとります。 | |

硬貨はホログラムシールで守られているとします。実体のある硬貨を発行しようと思うと、金型を作り、硬貨のデザインを彫りこむ必要があります。



2013年度の25セント硬貨にかかる金型です。

金型ごとに ~$500、あるいは硬貨ごとに ~$1,000 かかります。本物の金属を用いると、硬貨の原材料費は ~$1 であり、ホログラムシールは ~$0.10です。つまり、概算で費用を計算すると、 O(*c+n*) = O($1000 +

$1.10 x *n*)となります。硬貨を一枚だけ発行すると、 ~$1001.10かかります。しかし、1000枚発行すると、硬貨一枚あたりの値段は$2.10に下がります。10000枚発行すると、一枚あたり$1.20です。つまり、初回費用の c は、ホログラムシール一枚分の値段まで下がったことになります。

法定通貨の利点は、政府が硬貨の製造コストよりはるかに高い値段を任意に定められる点です。ビットコインを用いると、各硬貨は、それ自体が財布の役割を果たします。つまり、各硬貨の価格は、原材料費に硬貨自体の金額を加えたものになります。

法定通貨：*初回費用 + (原材料費 x 発行数)*

暗号化通貨：*初回費用 + (原材料費 x 額面価格 x 発行数)*

硬貨の額面価格を守るための手法として、暗号化シールの外面に公開されている口座番号を印刷し、シール内部に口座の秘密鍵を埋め込むことが行われてきました。しかし、暗号化シールの製造コストはたったの$0.10程度です。保護の役割はあまり果たせません。これでは、焼け石に水です。

暗号化通貨の偽造費用：*初回費用 + (原材料費 x 発行数)*

正式な暗号化通貨の費用：*初回費用 + (原材料費 x 額面価格 x 発行数)*

必要なのは、偽造しようとするとコストが硬貨の額面価格を上回るようにし、その一方で、正式な硬貨を発行する場合はコストが額面費用を下回るようにすることです。*偽造コスト　＞　額面価格　＞　発行コスト*硬貨の発行コストが額面価格より低ければいいわけですね。

そうするためには、各コインを完全に個別化する必要があります。各硬貨の属性をデータベースに入れれば、各硬貨の偽造費用は次の通りになります：

暗号化硬貨の偽造費用: *初回費用 + (原材料費 x 偽造費用 x 発行数)*

暗号化硬貨の正式発行費用: *初回費用 + (原材料費 x 額面金額 x 発行数)*

印刷された紙幣はシリアルナンバーを用いて各紙幣を区別しますが、それはただの数字です。数列にすぎないので、紙幣固有の属性は何も表しません。T偽造コストを上げるために、発行プロセス内にランダム性を取り入れます。これは、[物理的に偽造不能にする技術（PUF）](https://en.wikipedia.org/wiki/Physical_unclonable_function)と呼ばれています。

PUFはランダム性を含む物理特性を、もっともらしく表現したものです（1）。実質的に無料で、製造工程にランダム性を*追加*できます。ランダム特性がどう実装されるかは関係ないからです。床に、トランプのカードを撒き散らすようなものだと考えてください。しかし、ランダム性を*複製*するのは無料ではできません。

無造作にばら撒かれたトランプのカードの山を再現するには、カードを一枚一枚、それぞれの正確な場所に配置しなければなりません。

実際の例では、[ラメ入りのマニキュア](http://www.wired.com/threatlevel/2013/12/better-data-security-nail-polish/)を使用して電子機器の監視を検出できます。ジャーナリストがコンピューターや周辺機器をNSAや政府の監視から保護しようとすれば、すべてにマニキュアを塗り、写真を撮れば良いのです。NSAですら、マニキュアの塗り模様を再現するには苦労するでしょう。

より実用的なやり方は、クレジットカードの磁気部分です。数百万もの磁気を帯びた極小の棒が「ランダムに」配置されており、非常に低コストでそれを行えます。クレジットカードには質問／回答機能を内蔵したチップを組み込むことも可能であり、ビットコインの秘密鍵にそうしたチップを組合せ、秘密鍵が常に取り出せるようにできます。しかし、質問／回答チップだけでは、秘密鍵を盗み出して、別の硬貨に入れ込むことを防げません。（2）。そうした「物理的な二重使用」を防ぐために、PUFを硬貨の物理的な構造に結びつける必要があります。誰かが秘密鍵を盗み出そうとすれば、硬貨を破壊しなければならない、ということです。

私が提案するのは、NFCで読み出せる空洞の硬貨を発行することです。硬貨の内部に秘密鍵を印刷して保管し、公開鍵とNFC番号は[Namecoinデータベース](http://namecoin.info/)(任意のデータを安全に、監視不能な形で保管できる暗号化通貨)に入れれば、NFC機能を持つ携帯電話であれば誰でも、硬貨が偽造されたものかどうかを判定できます（3）。質問／回答チップ（NFCや他の手法を用いて）を利用すれば、コインの秘密鍵／公開鍵の組合せが正式であり、すぐに取り出せることを確認できます。

さて、私は硬貨が「偽造不能」と言いましたが、抜け目のないハッカーなら、不可能なのではなくとてつもなく困難なだけなのだから、括弧でくくれ、と言うでしょう。困難さを増すために、複数のPUF機能をレイヤーに重ねることができます。NFC読み取り用署名、磁気テープ読み取り用署名、オプションの署名などです。PUFが一つ破られても、他にまだ2つ、根本的に異なるPUFが保護を続けられます。

この方式の長所は、偽造のコストを調べ上げ、どの方式が劣っているかを判断できることです。全てのPUFを解読してビットコイン硬貨を偽造し始めた人物がいるとしても、*既存硬貨*の所有者は損を被りません。

硬貨を割って開け、別の財布に入れるだけです。同時に、新型のPUFが発明されていくでしょう。

PUF対応ビットコインの偽造防止は非常に優れており、ビットコインにとって大きなチャンスです。「法定」通貨でも、[ビットコインの主要機能を取り入れようとする](http://mintchipchallenge.challengepost.com/)ものが出現しています。[カナダ造幣局は、マイクロ国家に類似した位置づけのChannel Islandsというデジタル通貨の発行を](http://mintchipchallenge.challengepost.com/) [試み、その過程でビットコインをベースにした硬貨を目指しています。しかし、暗号化通貨のデジタル世界と物理的な世界をまたごうとするこうした風変わりな試みはどちらも、](http://www.ft.com/intl/cms/s/0/4903fc9a-591f-11e3-a7cb-00144feabdc0.html#axzz2sm4crTkl) ビットコイン自体以外の場所に価値を保存しようとしているため、失敗に終わります（4）。

最後に、そして最も重要なことに、PUFビットコインは、自国の通貨が不安定な国々にとって*完璧な*選択肢でしょう。例えば、[ミャンマー、](http://www.npr.org/blogs/money/2013/05/10/182309623/why-almost-no-one-in-myanmar-wanted-my-money) [ベネズエラ、](http://www.tradingeconomics.com/venezuela/inflation-cpi)そして[北朝鮮や](http://www.businessinsider.com/south-korean-leaflets-north-korea-2014-1)その他 [国々](https://en.wikipedia.org/wiki/Dollar#Countries_unofficially_accepting_a_dollar)は、非公式に米ドルを受け付けています（5）。紙幣に対する信頼が極端に低下しており、あの米ドルですら、苦労している状況にあります。

# ミャンマーに降り立つと、いかに現地の人が取引熱心なのかがわかります。現地の携帯電話レンタルサービスへ行くとします。

すると、受付の男性は米ドルをほしがるのです。しかし、私が札を取り出すと、彼は首を横に振ります。

「駄目だね」彼は言います。

彼は20ドル札の中央にある折り目を指差します。折り目は駄目だ、ということです。

そこで別の札を出すと、今度はかすれているから駄目だ、と言われます。三枚目は少し破れているので駄目、

四枚目はインクの染みがあるので「あまり受け取りたくないね」となります。

-[Planet Money](http://www.npr.org/blogs/money/2013/05/10/182309623/why-almost-no-one-in-myanmar-wanted-my-money)

ビットコインが多くの市場にまだ広まっていない理由はただ一つ、物理的な形状を持たないからです。ビットコインを用いようとすると、根本的なところでつまづきます。私の自宅から半ブロック離れたところにあるシアトル大学通りにある農産物直売所では、クレジットカードを扱える店は半数だけです。お高いシアトルの住民に高級有機野菜を売る農家ですらクレジットカードを考慮していないのであれば、後進国の田舎にいる農家が500ドルの携帯電話や毎月100ドルのネットアクセス費用を払って、ビットコインを受け付けるなんてことが起こるでしょうか？たとえPUFがなかったとしても、ビットコイン硬貨があれば、そうした市場において既存の通貨と同じ土俵で競合できるようになります。

PUFは既存の硬貨と同程度に偽造が困難なはずだ、という点に注目してください。検証が可能になるのです。誰かがビットコイン硬貨の取引を検証したければ、ずっと安く行え（6） 、クレジットカード機械よりも安全です（7）。PUFスキャン用機械を20ドル以下の価格帯で（8） 購入することも可能であり、携帯電話に付属したNFC読み取り機よりも正確でしょう。インターネットに常時接続する必要もありません。数ヶ月硬貨と取引を保留することができ、オフラインのデバイスを更新して新しい硬貨を入手するとともに、偽造を報告することもできます。後進国のユーザーは、そうした機械を太陽光発電や手動発電で稼動することもできます。更新に必要な費用は数人でシェアすることもできます。（9）。

こうした課題に取り組むだけの専門技術を私は持ち合わせていませんし、今は非常に忙しい状態です。しかし、Namecoinについてpuf/ namespaceの項目を（一時的に）[wiki](https://github.com/namecoin/wiki/wiki/puf)へ申請しました。Namecoinの「中核」開発者として、私はNamecoinを贔屓にしていますが、それはNamecoinがデータ保管に最高の場所だからです。だいたい、ブロックチェーンに余計なデータを付け足すのが賢明でしょうか？

多くの（全てではないにしろ）代替通貨は、表面的な変更を施しただけの、模造商品です。投機目的以外の何者でもありません。PUFはNamecoinの素晴らしい応用方法であるだけでなく、どうしてNamecoinに普遍的な価値／解が存在するのか、をも実証しています。Namecoinはビットコインとは競合しません。交換媒体としてはビットコインに及ばず、Namecoin硬貨を発行する理由は見えません。

|  |
| --- |
| 趣味だけでやるのなら、話は別ですが。しかし、IDや、[電子機器](https://twitter.com/indolering/status/426961058587107329)、その他私がまだ考え付いていない、通貨以外のものを扱うためには、ブロックチェーンに備わっているセキュリティや監視防止機能に対応するPUFデータベースが必要になります。各利用方法について、暗号化通貨をいちいち設立しなければいけないのでしょうか？ |
| [Corvus and Columba](http://corvusandcolumba.com/)にて、天才級の数学者たちとこのアイデアを話し合いました。彼らも、この問題について考えたことがあります。なので、あなたが（ジャーナリストであれ何であれ）実際のプロセスについて質問があるのであれば、彼らに聞いてください。この領域における研究を援助したいのであれば、彼らはオープンソースに身も心も捧げているので、小額であっても初期研究や試作には十分でしょう。 |
| 1. PUFは単方向ハッシュ機能のように機能します。秘密鍵ではありません。秘密鍵は簡易型PUF読み取り機をバイパスするために用いることができます。PUF読み取り機が十分に詳細情報を読取れない場合は、メーカーの秘密鍵に頼ることができます。しかし、PUFを用いると、メーカーは単一の公開鍵／秘密鍵を用いて複数の硬貨を製造することができなくなります。↩ 2. あるいは、新規発行の硬貨に質問／回答チップを埋め込む誰かに頼るか、同じ公開鍵／秘密鍵の組合せで複数の硬貨を発行するメーカーに頼るか、となります。↩ 3. もしNFC対応電話を既に所有していれば、検証デバイスを購入するコストはゼロです。大量生産効率と、中古機器の市場を考慮に入れてみましょう。そうすれば、後進国の貧民層ですら、数年経てば「無料で」検証デバイスが入手できるでしょう。ブロックチェーン（特にUXTOバージョン）が携帯電話同士で共有できることを考慮に入れれば、なおのことです。↩ 4. コメント欄で指摘があったように、法定通貨でもPUFは設定できます。しかし、PUFを用いているだけなら、防げるのは詐欺行為だけです。ビットコイン硬貨は、ビットコインがニッチ市場で発揮している有用性を、物理的な取引へ持ち込む作用を果たします。例えば、PUFビットコイン硬貨は、銀行へ行かずともデジタルバージョンに変換できたりするでしょう。↩ 5. Slashdotのコメントに対する返答です。こうした不安定な地域では、硬貨が社会規模の問題を解決すると私は考えていません。*助け*にはなるでしょう。通貨操作は長期的な影響があるため、触れられなくなるはずです。ハイパーインフレの可能性のある通貨にしがみつくことが、住民にとっては益であるならば、政府は短期的な利益を享受し続けるでしょう。現時点では、米ドル紙幣／硬貨を用いるか、直接取引を行うかしか、他の手段がありません。この2つのどちらも、PUFビットコイン硬貨を用いてデジタルで価値を保存する利点には遠く及びません。しかし、住民はそれでも、政府の目を逃れ、隠れて行動しなければならないでしょう。そうした代替硬貨は現状をより*安全に*することはできませんが、より*手軽に*、より*安定に*することはできます。↩ 6. クレジットカードの手数料を考慮に入れれば、です。↩ 7. 詐欺的な支払拒否はありません。↩ 8. 私にはATMが見つけられませんでしたが、ブロックチェーン用のメモリとプロセッサを考慮しても、価格は100ドル以下に収まるでしょう。 ↩ 9. コメントに返答すると、ブロックチェーンを用いればオフラインデバイスを安全に、確実に更新できます。オフラインの読取り機において認証コードを解読でき、別のデータを機械に与えることに成功したとしても、持ち主がどの硬貨を扱えるのか、についても管理しなければなりません。その結果、被害者は非常に偏狭なコミュニティに追いやられ、攻撃者はコミュニティを掌握して技術的にも高度な人々とつながることになります。もっとよく概要を理解したい場合は、 |

|  |  |
| --- | --- |
| UXTO拡張を持ちいて、ブロックチェーンを全て持たなくとも取引の正当性を検証できる方法について読んでみてください。↩  2014年2月8日  18 Comments | |
| **About indolering**  [View all posts by indolering →](http://www.indolering.com/author/indolering) |  |
|  |
| **Contact Me** | |

[← Safeplug is not Safe](http://www.indolering.com/safeplug-is-not-safe) [Last Mile →](http://www.indolering.com/last-mile)

### 18 Responses to “Counterfeit­Proof Physical Bitcoins”

1.



[SW](http://stephan.sugarmotor.org/) February 9, 2014 at 7:31 am #

Two questions.

1. So someone receives one of your coins.How do they know the matching private key is actually inside?
2. What is the difference of your proposal to having a mint simply publish a list of PUF signatures for verification?Then coins can be verified against this list.All data in the coin is only added for verifiability.What is lost from your proposal, except that no bitcoins are used?

Stephan

[Reply](http://www.indolering.com/puf-bitcoin?replytocom=2771&respond)



[indolering](http://indolering.com/) February 9, 2014 at 10:38 am #

* 1. So someone receives one of your coins.How do they know the matching private key is actually inside?

The simplest way is to just embed a challenge­response chip like they have on credit cards.

* 1. What is the difference of your proposal to having a mint simply publish a list of PUF signatures for verification?Then coins can be verified against this list.All data in the coin is only added for verifiability.What is lost from your proposal, except that no bitcoins are used?

Uhh, all of the benefits that come with using Bitcoins?:P

[Reply](http://www.indolering.com/puf-bitcoin?replytocom=2773&respond)

[indolering](http://indolering.com/) February 9, 2014 at 12:56 pm #



Which is to say that a physical Bitcoin bridges all of things that make Bitcoin great for 3rd world markets to physical transactions.Most of these countries are shut out of the legitimate banking system due to fraud.Even if, for example, a farmer is paid in physical currency the farmers

\*suppliers\* can seamlessly exchange the physical currency for a digital one, much like we can deposit cash in a bank.Except they don’t have to go to a physical bank.

|  |  |  |
| --- | --- | --- |
| [Reply](http://www.indolering.com/puf-bitcoin?replytocom=2774&respond) |  |  |
|  | |  |

[SW](http://stephan.sugarmotor.org/) February 10, 2014 at 9:28 am #

Thanks for your answer.

About “… embed a challenge­response chip like they have on credit cards.”

I don’t see how a challenge­response system can help here.The methods are about “providing a valid answer”, but how can the owner of a bitcoin get to verify the private key without learning about it?

So I think such a mint could cheat, issue coins that are not backed by actual bitcoins.

On top of that it might be accused of cheating without being able to defend itself.A bunch of people open their coins, extract the private key, transfer funds, and months later (so as to pretend they had nothing to do with it) complain that “the bitcoins were stolen.”

[Reply](http://www.indolering.com/puf-bitcoin?replytocom=2780&respond)



[indolering](http://indolering.com/) February 11, 2014 at 4:10 pm #

You validate that the private key exists by challenging it to encrypt something….Think about PGP email signing or signed binaries.

To prevent nefarious users, we could setup a WOT that would track the last time a coin had been scanned.If the users funds were stolen AFTER such a scan took place, we could verify whether that hash function had been broken.

[Reply](http://www.indolering.com/puf-bitcoin?replytocom=2782&respond)



[SW](http://stephan.sugarmotor.org/) February 11, 2014 at 7:53 pm #

Just because a device can encrypt something doesn’t mean that the key itself is recoverable.I fear this coin design may get quite complicated.



[Stuart Gathman](http://gathman.org/vitae) April 1, 2014 at 8:22 pm #

“Challenge response” refers to “zero knowledge proofs” – one of the many mathematical ways to prove you know a secret without revealing that secret.Digital signatures prove that you know the private key, without revealing that private key.

A simple C/R with a 1 way hash may be simpler to understand.Server wants to know if user knows the password without the user having to transmit said password.

1. Server sends a random number to user
2. User (his computer rather) computes a hash of the password with the random number, and sends back the result.
3. Server hashes the password with the random number, and checks that the result matches what the user (his computer rather) sent.

[Reply](http://www.indolering.com/puf-bitcoin?replytocom=2847&respond)



2.

proofreaderonimous February 9, 2014 at 11:43 pm #

“The with these systems is no different” => “The problem with these systems is no different” or similar?

[Reply](http://www.indolering.com/puf-bitcoin?replytocom=2776&respond)



[indolering](http://indolering.com/) February 11, 2014 at 4:27 pm #

ありがとうございました！

[Reply](http://www.indolering.com/puf-bitcoin?replytocom=2783&respond)



3.

[SDLerner](http://firmcoin.com/) February 10, 2014 at 5:09 am #

It’s unclear in this article how PUFs can be used to create digital signatures (a privkey/pubkey pair).PUFs can be verified as long as the verifier has already performed several challenge/response interactions and have the corresponding responses.And if these responses cannot be public: they should be stored secretly by a verification entity (such as a central bank).So people won’t be able to verify their physical coins without running an online protocol with a central authority.

The right way to do this (completely offline) is using the Firmcoin (Firmcoin.com)

[Reply](http://www.indolering.com/puf-bitcoin?replytocom=2779&respond)



[indolering](http://indolering.com/) February 11, 2014 at 4:03 pm #

PUF’s are not pub/private signatures, they are physical one­way hash functions.

Although a public/private key could be useful for dealing with low­fidelity PUF readers: if the PUF reader couldn’t get enough detail, it could rely on the manufacturers private key.しかし、PUFを用いると、メーカーは単一の公開鍵／秘密鍵を用いて複数の硬貨を製造することができなくなります。

[Reply](http://www.indolering.com/puf-bitcoin?replytocom=2781&respond)

[SW](http://stephan.sugarmotor.org/) February 11, 2014 at 8:00 pm #



Thanks for the link.Yes, firmcoin sounds more plausible and complete.It also shows how complicated this gets when one tries to cover all angles.

[Reply](http://www.indolering.com/puf-bitcoin?replytocom=2785&respond)



4.

[Ron Helwig](https://shiresilver.com/) February 16, 2014 at 6:35 am #

None of this addresses the primary issue with physical bitcoins, which is that the person receiving it has absolutely no way to ensure that the issuer hasn’t kept the private key.It might have enough tamper­resistant and tamper­evident features to make you believe that no one has retrieved the private key since it was issued, but you still have to have absolute trust in the issuer for it to be worth anything.This is a problem with every physical bitcoin proposal I have seen, and IMHO is the primary issue – counterfeiting of the physical token is much less of a problem.

[Reply](http://www.indolering.com/puf-bitcoin?replytocom=2793&respond)



[indolering](http://indolering.com/) February 27, 2014 at 2:31 pm #

Ahh, this is true!However, we can combat this in a few different ways.One is to just establish the issuer in a country with a strong rule­of­law.If said company or any of it’s employees tried to wholesale defraud their customers, they would be put in prison.

However, we must protect against internal attacks as well.One can imagine a radically open system in which everything is cryptographically secure and formally proven, from the computers generating the wallets and transferring the money to the machines printing the physical coins.The entire production process could be streamed online it could be staffed with rotating academics and others so the system is regularly audited and the internals of the system are trustless.

|  |  |  |
| --- | --- | --- |
| [Reply](http://www.indolering.com/puf-bitcoin?replytocom=2818&respond) |  |  |
|  | |  |

[indolering](http://indolering.com/) February 27, 2014 at 2:32 pm #

Ahh, this is true!We must trust *someone*, that cannot be removed entirely.However, we can combat bad actors in a few different ways.

One is to just establish the issuer in a country with a strong rule­of­law.If said company or any of it’s employees tried to wholesale defraud their customers, they would be put in prison.

However, we must protect against internal attacks as well.One can imagine a radically open system in which everything is cryptographically secure and formally proven, from the computers generating the wallets and transferring the money to the machines printing the physical coins.The entire production process could be streamed online it could be staffed with rotating academics and others so the system is regularly audited and the internals of the system are trustless.

Finally, we can also purchase insurance.An external organization can provide financial coverage to

compensate those who stand to lose money from a systemic collapse.The insurance providers would watchdog the entire process and enable us to spread the risk of inevitable problems.

I think these counter­measures can ameliorate the dangers to an acceptable level.Thank you for pointing this out!

[Reply](http://www.indolering.com/puf-bitcoin?replytocom=2819&respond)

### Trackbacks/Pingbacks

1. [Counterfeit­proof Physical Bitcoins | Social Media Marketing 24/7](http://smm24.dk/counterfeit-proof-physical-bitcoins/) ­ February 8, 2014 […] I haven’t seen this discussed here yet:[http://www.indolering.com/puf­bitcoin](http://www.indolering.com/puf-bitcoin) […]
2. [bitcoins físicos, ¿posible?| Virgilio Leonardo Ruilova Castillo](http://virgilioruilovacastillo.wordpress.com/2014/02/09/bitcoins-fisicos-posible/) ­ February 9, 2014 […] bitcoins físicos, ¿posible?[…]
3. [Counterfeit­proof Physical Bitcoins | NewsBitcoin.com](http://newsbitcoin.com/?p=43221) ­ February 9, 2014

[…] I haven't seen this discussed here yet:[http://www.indolering.com/puf­bitcoin](http://www.indolering.com/puf-bitcoin) […]

### Leave a Reply

Name (Required)

Email (Required)

Website

Comment



Submit Comment

**CONNECT**

**PGP KEY ID 04A324C9AD568825**

[971E 691A 5356 5F57 57EA 2542 04A3 24C9 AD56 8825](https://mega.co.nz/#!VgwzFYID!D8a3UQn9FUhMIQYxNWj_j2U8GRV6dCERR-SFVWdeGWI)

Search

Popular Latest

Tags

|  |  |
| --- | --- |
|  | [Counterfeit­Proof Physical Bitcoins](http://www.indolering.com/puf-bitcoin) February 8, 2014 |
| [Movie Player Mockup \*Updated\*](http://www.indolering.com/ff-player) July 15, 2011 |
| [15 Torrent Freak approved proxies/VPNs by cost, speed, access to iPlayer/London Olympics and more!](http://www.indolering.com/15-torrent-freak-vpn)July 28,  2012 |
| [Escaping Callback Hell](http://www.indolering.com/escaping-callback-hell) April 4, 2014 |
| [Spook Trolls](http://www.indolering.com/spook-trolls) March 22, 2014 |
| [coop.js](http://www.indolering.com/coop-js) March 3, 2014 |
| [bitcoin](http://www.indolering.com/tag/bitcoin) [btc](http://www.indolering.com/tag/btc) [design](http://www.indolering.com/tag/design) [educational psychology](http://www.indolering.com/tag/educational-psychology) [health-care](http://www.indolering.com/tag/health-care) [ira glass](http://www.indolering.com/tag/ira-glass) [minimalist documentation](http://www.indolering.com/tag/minimalist-documentation) | |
| [page load](http://www.indolering.com/tag/page-load) [page speed](http://www.indolering.com/tag/page-speed) [political](http://www.indolering.com/tag/political) [proxy](http://www.indolering.com/tag/proxy) [psychology](http://www.indolering.com/tag/psychology) [rant](http://www.indolering.com/tag/rant) [review](http://www.indolering.com/tag/review) [social](http://www.indolering.com/tag/social) [tor](http://www.indolering.com/tag/tor)[vpn](http://www.indolering.com/tag/vpn) [yslow](http://www.indolering.com/tag/yslow) | |
|  | |

## CATEGORIES

[Activism](http://www.indolering.com/category/design-2/activism) [Design](http://www.indolering.com/category/design-2) [Framing](http://www.indolering.com/category/framing) [JavaScript](http://www.indolering.com/category/web-development/javascript) [Mozilla](http://www.indolering.com/category/mozilla) [Namecoin](http://www.indolering.com/category/namecoin) [Personal](http://www.indolering.com/category/personal)[Random](http://www.indolering.com/category/random)

[Research](http://www.indolering.com/category/research)[Speech.is](http://www.indolering.com/category/speech-is) [Ubiquity](http://www.indolering.com/category/mozilla/ubiquity) [Usability](http://www.indolering.com/category/design-2/usability)[Web Development](http://www.indolering.com/category/web-development)

