Overview of Colored Coins

Meni Rosenfeld

December 4, 2012

Abstract

Bitcoin ([3]) is the world's first decentralized digital currency, allowing the easy storage and transfer of cryptographic tokens. It uses a peer-to-peer network to carry information, hashing as a synchronization signal to prevent double-spending, and a powerful scripting system to determine ownership of the tokens. There is a growing technology and business infrastructure supporting it.

By the original design bitcoins are fungible, acting as a neutral medium of exchange. However, by carefully tracking the origin of a given bitcoin, it is possible to color a set of coins to distinguish it from the rest. These coins can then have special properties supported by either an issuing agent or a Schelling point, and have value independent of the face value of the underlying bitcoins. Such colored bitcoins can be used for alternative currencies, commodity certificates, smart property, and other financial instruments such as stocks and bonds.

Because colored bitcoins make use of the existing Bitcoin infrastructure and can be stored and transferred without the need for a third party, and even be exchanged for one another in an atomic transaction, they can open the way for the decentralized exchange of things that are not possible by traditional methods. In this paper we will discuss the implementation details of colored bitcoins and some of their use cases.

Contents

Chapter 1

Introduction

Bitcoin has revolutionized currency by creating a medium of exchange that can stored and transferred digitally without reliance on any single third party, with overreaching implications for efficiency, security and counterparty risk. The colored coins project aims to extend these abilities to other assets; it would allow handling arbitrary digital tokens in much the same way that bitcoins are handled, and in particular easily trading them for digital currencies. Some potential uses are:

1. **Smart property:** Ownership of physical assets such as cars and cellphones can be represented as a token, and the device will only respond to the owner of the token. ([1])

2. **Company stock:** A company could issue tokens representing shares in the company. The platform would easily allow sending Bitcoin dividends to shareholders, and allow shareholders to cryptographically vote.

3. **Deterministic contracts:** A person or company can issue contracts specifying a particular future payment, such as a mining bond or a commodity option.

4. **Bonds:** A special case of the above, bonds can be issued with a particular face value and repayment schedule, denominated in bitcoins or some other currency or commodity.

5. **Demand deposits:** Similar to bonds, except the issuer guarantees to redeem the token for its face value at any time. This can be used as either an interest bearing instrument, or as a way to handle physical assets more efficiently.

6. **Emergent currencies:** A community may want to use a local currency which is similar technically to Bitcoin but detached from it monetarily. They can issue tokens for this purpose and distribute them among themselves in some fashion, and have them gain value organically through use rather than through some concrete backing.

7. **Decentralized digital representation of physical assets:** This is a hypothetical use case that is not proven to be viable, but is eagerly anticipated by some groups. Over

time, a consensus could arise that a token is commensurable in value to some traditional currency or commodity, without a specific backer apart from a bootstrapping period. This will allow digitally holding value tied to physical assets.

What characterizes colored bitcoins in comparison with other methods to achieve the same goals is that it is entirely built on top of the infrastructure of Bitcoin (or some other blockchain-based currency) – the tokens are any bitcoins that can be traced back to a particular output, and the transactions in which tokens are moved are Bitcoin transactions, recognized as normal transactions by oblivious Bitcoin nodes but must satisfy additional requirements to be considered legitimate by color-aware nodes.

The structure of this work is as follows: In chapter 2 we examine the advantages and disadvantages of this system over alternatives. In chapter 3 we explain some of the details of tracking the color of coins.

Chapter 2

Merits of colored coins

2.1 List of benefits

There are many use cases for colored coins, and many alternative methods to satisfy them; it will be useful to first list the potentially beneficial features of the colored coins method.

1. Colored coins are very general. Virtually any kind of asset or contract can be represented using them.

2. They can be stored digitally without needing a third party. In particular, the full force of the Bitcoin scripting language can be mustered for their safe storage, such as multi-signature transactions.

3. They can be transferred digitally to a new owner with no need for central authorization, which has implications for ease of use, efficiency and availability.

4. They can be exchanged for other colored coins or uncolored bitcoins in a single atomic transaction – meaning there is no counterparty risk, even without blockchain confirmations. And once again the entire range of scripting options is available to allow more complex trades, such as exchanging for coins of a different blockchain with a similar security guarantee, or automated escrow.

5. Properly used, ownership of colored coins can be made anonymous, while still enjoying the benefits of ownership.

6. The infrastructure of technology, software, hardware and services which powers Bitcoin carries naturally to benefiting colored coins. Technical challenges that are overcome with Bitcoin translate to the colored coins platform; software for handling Bitcoin can be used, with or without patching, to handle colored coins; mining hardware which synchronizes Bitcoin transactions automatically also synchronizes colored coins transactions; and various Bitcoin-related services can be used in the context of colored coins, sometimes while remaining color-unaware.

7. The intuitions behind dealing with Bitcoin translate to understanding the colored coin platform, and together they form the "common language", on both discussion and software levels, to tie up the various applications.

2.2 Comparison with alternative methods

Many of the use cases could be accomplished, to some extent, using methods other than colored coins. We will list some such methods and emphasize the advantages that colored coins may have over them.

1. **Traditional stock exchanges.** The traditional ecosystem of stock exchanges and brokers serves today for the issue and trade of financial instruments, and was proven in the test of time to be viable for this purpose. However, old established businesses tend to suffer from lack of innovation; these platforms pose a significant barrier of entry to smaller issuers; and the lack of a truly digital representation for the assets has all the usual disadvantages with regards to transaction fees, availability, self-sufficiency and so on.

2. **Modern central services.** Start-ups such as GLBSE ([2]) attempted to use the power of Bitcoin to provide a modern, international, low-cost alternative to traditional markets. Such a lean platform could mitigate some of the disadvantages of centralization. However, it is by far more exposed to others: As was widely suspected in the case of GLBSE and eventually turned out correct, the lack of track record and regulatory compliance exacerbate the risk of unclean shutdown, throwing asset issuers and holders to limbo.

3. **Dedicated blockchain per asset.** The Bitcoin technology allows the creation of new blockchains with relative ease, each representing its own alternative currency. An issuer could create a new blockchain where the units of currency are tokens of his asset. If the different blockchains conform to some standard, a single software could handle several of them with a convenient interface.

   However, this greatly increases the barrier to entry and misses an opportunity for economies of scale in the security of cryptocurrencies. Different cryptocurrencies work best if they pool their hashrate, as each of them enjoys the security of the combined hashrate. This can be achieved with merged mining; however, this still requires some amount of hashing native to the currency, as well as support of some miners from the host blockchain (such as Bitcoin). Smaller issues with few users will find it difficult to enjoy protection from hashrate-based attacks. Also, the host blockchain will not benefit from the native hashing of the guest blockchains.

   Furthermore, for such smaller issues, there will be few nodes storing, verifying and serving blockchain data, posing a risk to network integrity and availability. Even if enough nodes can be found, a software client handling several asset types will need to connect to several nodes of each, increasing the networking overhead.

It also makes it more difficult to send dividend and coupon payments (in bitcoins or other currency or asset) to the owners of assets.

By having the assets embedded in the Bitcoin blockchain, the entire existing infrastructure of Bitcoin network nodes and miners can be utilized to benefit each and every one of the assets. This allows creating a secure asset with no barrier to entry. The extra burden on the host network can be paid for with a proper transaction fee system. The inclusion of arbitrary assets in the Bitcoin network will increase its total economic value, attracting more nodes and miners to strengthen it even further. Payments to asset holders can be done directly to the holding address in either the host or any guest currency.

4. **Separate asset-aware blockchain.** This is similar to the above, except a single blockchain (unrelated to existing blockchain currencies) will be used for all assets. This is in fact a variant of, not an alternative to, the concept of colored coins, as coloring will still need to be used to track specific assets within this blockchain. Its advantages are that it can spare the host blockchain from any real or perceived ill effects, and that additional features can be developed for it to make it more friendly for its intended purpose.

   However, this variant is slower to bring to market, as the infrastructure needs to be built from scratch rather than leveraging the Bitcoin infrastructure.

5. **Open Transactions.** Open Transactions ([4]) is a powerful platform that can satisfy most, if not all, of the desired use cases. However, its intuitions are different than those of Bitcoin, which means it will likely be more slowly adopted by the Bitcoin community (who is the primary target market for the features we are espousing) than a Bitcoin-based system. It can still exist as a viable alternative, with its own pros and cons, to a colored coin system.

2.3 Demerits of colored coins

We should also consider (and in some cases, refute) the suggested disadvantages of the colored coin system, specifically when embedded in an existing blockchain.

1. **Blockchain bloat.** The inclusion of the extra burden of colored coin transactions can supposedly bloat the blockchain, increasing the cost of running a node. However, scalability is an issue for any blockchain even with only native transaction, and is an issue which should be solved rather than worked around. Every transaction carries the marginal cost of being received, verified and stored by every node on the network. These are all commodities, an transaction fees exist in part to pay for them. With a properly chosen system for the distribution of fees to nodes, any additional transaction makes it that much more lucrative to run a node, maintaining the balance of the number of nodes and their profitability. In fact, since new economic activity can bear

above-cost fees, it can serve to actually strengthen the network. The overall level of fees is a protocol-level decision to balance the number of nodes with the reduction of friction; whatever level is chosen, additional layers can be used to accommodate transactions with a lower value than the threshold (for both the native currency and colored coins).

2. **Insufficient hashing fees.** More difficult than the problem of funding network resources, is the problem of funding hashing. Since the cost of hashing is amortized over all transactions, it is essentially a bargaining game between miners and users, which unconstrained would lead to a race to the bottom. As such it will be useful to have protocol-enforced methods (such as a limit on the total value of transfers per block) to make sure fees are paid by those who can afford them (typically senders of high-value transactions). With colored coins, the network is unable to determine the value of the transactions and charge accordingly. This means what this economic activity contributes to the hashing network is not proportional to, and typically lower than, the value it obtains from it. However, no actual harm will be done by colored coins; and while a system which does contribute fairly would be preferable, unless such a system can be come up with, this objection is moot.

3. **Legal concerns.** With colored coins embedded in a host blockchain, any legal issue with the guest assets, such as uncertainty about security trade regulations or specific unsavory assets, might project into the host blockchain. This issue deserves more exploration, but it is the author's belief that the inclusion of multiple heterogeneous entities within the same blockchain will only reinforce its position as defying traditional legal approaches.

Chapter 3

Implementation overview

The foundation of colored coins is the ability of an issuer to set aside some of his bitcoins and declare that they have a specific color, and state his obligations to owners of coins of this color. "Color" is used metaphorically, of course - in practice a color will be identified by a ticker symbol and a unique hash.

The crux, then, is the method to determine whether bitcoins held at some future time are of this color or not. The issuer should be able to send these coins to another party while maintaining their color identity. That party should be able to send them to yet another party, and so on. It should be impossible to have coins recognized to be of the color in any other way to receive coins which were already of this color, following a chain of transactions that can be traced back to the color's genesis.

The fundamental unit of account in Bitcoin is an output – the issuer will declare one or several of his outputs as belonging to the color, and then every output which can be traced back to them will also belong to this color. By default, bitcoins are fungible at the intra-transaction level; when a transaction has multiple inputs and multiple outputs, the protocol does not dictate a correspondence between particular inputs and outputs. Even if a transaction has an input recognized to be of a certain color, there is no way, in general, to identify specific outputs as successors which inherit this color.

This is possible, however, by requiring a certain structure for color-aware transactions, and having a specification for how to parse such transactions – that is, how to determine that given outputs have given colors. For such a specification to be valid, it will need to satisfy the conversation laws, that it is possible to move coins but impossible to create them out of nothing (by anyone but the issuer). With this in place, verifying that an output is of a certain color is simply a matter of examining the transaction it is part of, determining which inputs need to be of this color, and recursively verifying that indeed they are, all the way to the genesis outputs (there may be more computationally efficient methods to achieve the same result).

A naive solution would be to require that all inputs must be of the same color, and that in this case all outputs are of this color too. However, with this system transaction fees need to be paid out of colored coins, which are much more valuable than their underlying Bitcoin value as recognized by the network. This also misses out on some important applications,

such as atomic transactions with coins of multiple colors.

The standard of choice for the structure of color-aware transactions is order-based coloring. It has several extensions to deal with various use cases, but in its simplest form, it requires that:

- Inputs and outputs are sorted by color, with uncolored coins at the end.
- The same order of colors is used for both inputs and outputs.
- For each color, the total value of all inputs is equal to the total value of outputs; only uncolored coins can have a greater input value than output.

To parse such a transaction, we go over the different colors in order. For each color we sum up the input values of this color. Then we go over each output in order and assign it to this color, until the total output value is equal to the input value. By requirement, all outputs of the first color appear first, and their total value is equal to the total input value; hence, we will eventually reach an output which brings the total to match exactly.

Then we move on to the next output in the list and the next color, assigning outputs to it until the total output value of this 2nd color is equal to the total input value; and so on. After all colors have been exhausted, the remaining outputs will be uncolored; if the total uncolored outputs value is less than the input, the rest will be transaction fees. (The uncolored outputs will be no more than the uncolored inputs because this is a valid Bitcoin transaction.)

Note that colored transactions are a special case of Bitcoin transactions. A valid Bitcoin transaction which does not follow the special colored format, will be recognized by the Bitcoin network, but not as a legitimate color-preserving transaction by the colored coin network. The color of these coins will be lost, and hence users and software clients need to be careful to avoid doing this and losing their value.

Example: Suppose we are given a transaction with the following inputs and outputs: The computation will proceed as follows:

Index	Inputs	Outputs
#0	13 Red	3
#1	6 Green	6
#2	4 Green	4
#3	9 Blue	10
#4	2 Blue	3
#5	8 Uncolored	8
#6		5
#7		2

```
First color: Red. Total Red input value: 13.
Output #0 is Red. Total Red output value: 3.
```

```
Output #1 is Red. Total Red output value: 9.
Output #2 is Red. Total Red output value: 13. Red is complete.
Next color: Green. Total Green input value: 10.
Output #3 is Green. Total Green output value: 10. Green is complete.
Next color: Blue. Total Blue input value: 11.
Output #4 is Blue. Total Blue output value: 3.
Output #5 is Blue. Total Blue output value: 11. Blue is complete.
Total uncolored input value: 8.
Output #6 is uncolored. Total uncolored output value: 5.
Output #7 is uncolored. Total uncolored output value: 7.
No more outputs. Total uncolored output value is less than input value.
Difference of 1 BTC is transaction fee.
```

Bibliography

[1] Mike Hearn. Smart property. https://en.bitcoin.it/wiki/Smart_Property. Retrieved on Oct 30th 2012.

[2] James McCarthy. Glbse. https://glbse.com.

[3] Satoshi Nakamoto. Bitcoin p2p virtual currency. http://www.bitcoin.org/.

[4] Fellow Traveler. Open transactions. https://github.com/FellowTraveler/Open-Transactions.