Introduction

The Bitcoin blockchain, by being entirely public, protected by a proof of work and redundant in every Bitcoin clients\footnote{Soon the Bitcoin clients might not be using the entire blockchain history, but by then multiple specialized miners should have arisen, guaranteeing a large number of redundant database.}, is perhaps the most secure database in the world. By tying a meaning to a specific Bitcoin, it is possible to use the power of the blockchain with precise purposes, such as a proof of ownership.

Understanding

Before we continue, the reader should have a basic understanding of how Bitcoin works. Suggested readings include the Satoshi Nakamoto’s paper Bitcoin: A Peer-to-Peer Electronic Cash System and the Bitcoin’s wiki. A particularly
Figure 1: The Master Bitcoin is a specified transaction in a given block.

Important notion is that there is no Bitcoins per se, but rather a double-entry bookkeeping system, meaning that only transactions exist. It is, however, easier to understand and speak of Bitcoins as if they existed as an entity.

Current problems and weaknesses

When an individual acquires something of great value, it usually comes with a proof of ownership; some kind of paper stating he is the owner, or the equivalent in a database. One usually trusts many things:

1. There is only (and will ever be) a single object associated with this claim;
2. The delivering authority of this proof of ownership can’t deny it;
3. No one can forge the proof of ownership.

Yet, none of these points are guaranteed. In addition, these documents are often of little redundancy, hard to obtain and use on a short notice, and dependent on a central bookkeeping.

How can the Bitcoin blockchain help?

Let’s take a car as an example. When the vehicle is produced, the serial number engraved on it is the number of a Bitcoin transaction in a given block, which we call a Master Bitcoin (as seen on figure 1). In this transaction, a single Bitcoin is transferred. From now on, we can associate the ownership of the car with this Master Bitcoin. When an individual buys the car, the seller transfers

---

2 For example, 2 cars from the same manufacturer shouldn’t have the same serial number.
3 The amount can vary, 1 is used here for simplicity.
the Bitcoin to the new owner’s address. The property can be transferred easily by sending the Bitcoin. This method remains reliable for the entire life of the object, even with multiple second hand owners. By using the blockchain, an almost unbreakable chain of title is formed, protected by the same computing power used to protect normal Bitcoins. This information is available anytime, everywhere on the planet (where Bitcoins aren’t blocked) and is upgraded automatically by each property transfer, without need of a witness or notary.

It is easy to check if the owner is genuine: he simply has to make a transaction from the current Master Bitcoin’s address. If a manufacturer wants to offer special services to current owner of his products, he can ask for a proof of ownership. This method automatically prevent access from previous owners and enables a market for some (previously) single-use product, such as software keys.

Here is how, by using the Bitcoin’s blockchain, the 3 preceding trust issues are answered:

1. A unique serial number: otherwise the purchaser would see the item as already purchased (spent) when looking at the blockchain.

2. An engraved Master Bitcoin prevent any kind of deniability from the delivering authority: They can’t deny it is the serial number, and the blockchain proves who is the owner.

3. The proof of ownership, which is the private key currently holding the Master Bitcoin, can’t be forged.

A step further: divisible ownership

Not every ownership in this world is atomic. For example, a share in a company is only a portion of the property. A Master Bitcoin can be used in this case too.

Because Bitcoins are divisible, so is the Master Bitcoin. This offers the possibility to subdivide a share. This is a clear advantage over classical stocks, which can only be sold as a whole. In addition, the market never closes. One could buy or sell whenever he wants, without depending on business hours. The ownership and exchanges can also be anonymous, to the same extent that Bitcoins can be. In case of shares in a company, the owners could still vote while remaining anonymous, by making transactions from the same address.

---

4 A chain of title is the sequence of historical transfers of title to a property and is required in many fields, such as real estate, to prove ownership.

5 For immaterial property, the association of the Master Bitcoin and the property must be public (easily verifiable from the future and for everyone).

6 In order to change the blockchain history, an attacker would have to fork it at a block where the last property transfer occurred, and outpace all of the honest workers continually until his fork is longer. In addition to being exponentially harder for each additionnal block to rewrite, it is also noticeable by every Bitcoin user.
as their Master Bitcoin’s. Dividends can also easily be sent to every current owner, to the proportion of their share.

**Proposed implementation**

Here is the author’s humble proposition for rules of implementation. The conditions for a valid proof of ownership are:

**For indivisible property**

- Can be traced back to the original transaction;
- For every transaction in its history, it is always the biggest recipient (in case the Master Bitcoin is divided in a transaction);
- If the Master Bitcoin is divided exactly in half, the destination address first in an alphanumeric sorting has precedence. For example, 3102d83e9... would have precedence over 8d67f4476..., because 3 comes before 8.

A Master Bitcoin numeric value can change without consequence (provided the previous rules are respected), which enables fees to be paid directly from the Master Bitcoin, as seen on figure 2.
Figure 2: The Master Bitcoin (indivisible property) through multiple transactions

**For divisible property**

- Can be traced back to the original transaction;
- Any non-Master Bitcoin in the input **must** be used as a fee. This is to avoid mixing Master Bitcoin with regular Bitcoin.

A Master Bitcoin share can be destroyed if the numeric value is tampered with. In this case, the proportion of every other share will grow. See figure 3 for an example.
Conclusion

The Bitcoin blockchain has everything it takes to be used as a proof of ownership. The decentralized aspect of Bitcoin guarantees an undeniable chain of title, available everywhere and anytime. The property titles can be held anonymously and cross borders without approbation from a third party. All property transfers are handled by the network and do not require any witness or notary. A truly worldwide stock market can now emerge, available to everyone.

The most important argument in favor of the Master Bitcoin concept is that it doesn’t require any modification to the current Bitcoin networks, or any of
its derivative currency. The entire hashing power used to secure transactions can be used immediately. Only those who cares about a Master Bitcoin need some modification to the client, leaving the others unencumbered.