BlockFate

Andrew Barisser

September 5, 2014

Abstract

A protocol governing the ownership and management of physical devices, layered on the Bitcoin Blockchain. By representing ownership as a digital token abstracted on Bitcoin, devices can verify the identity of their owners through cryptographically signed messages solely by observing the Blockchain. Access rights and administrative privileges can be trustlessly exchanged between parties with ownership following the tokenholder. The problem of proving the loss of keys, and of double-spending, are obviated by rendering keys fungible on a universal consensus ledger. Devices need not consult a central database to respond appropriately to changes in ownership, even as they comply with sophisticated contractual arrangements, such as rental agreements. Provable digitized ownership opens up the potential for advanced machine-machine transactions, management of intellectual property, and more.

1 Introduction

The Bitcoin Blockchain makes ownership of bitcoin the currency mathematically self-evident. As bearer items, possession is equivalent to ownership. The divorce between Bitcoin and centralized, human-verified systems has made the former orders of magnitude faster, more efficient, and more transparent. It is an obvious goal to seek to apply the advantages inherent in Bitcoin to other systems.

Many groups are currently working on 'Bitcoin 2.0' technologies to expand the latent capabilities exposed by Satoshi Nakamoto. These include such enticing areas as Colored Coins, CounterParty, Ethereum, and a whole host of altcoins. But they all suffer from a common weakness. They are all separated from the physical world. Whereas ongoings within a Blockchain may be mathematically consistent, interacting with the outside world, such as feeding in trusted data, is as error prone and trust-dependent as ever. As a result, many potential use cases of 'Bitcoin 2.0' technologies, while internally perfect, fatally rely on imperfect external interactions.

Meanwhile, the dominant mindset of Bitcoin innovators has been Bitcoin's role as a financial instrument. This has shaped developments in the Bitcoin ecosystem and in various offshoots. The relative ease of internal consistency within the blockchain has obscured the broader use cases for a trustless, consensus ledger as it interacts outside the system. Financial instruments are convenient mathematical constructs, but broadening the impact of the blockchain entails expanding its scope into the physical world.

2 Trustless Machines Aware of Ownership

Just as bitcoins are self-evidently owned by public addresses, other forms of ownership may be equally well-represented on the Blockchain. The right to issue commands to a physical device may be represented as a digital token that may be moved. Ownership of that token is provable; the public Bitcoin address holding it may sign a message with its private key. A car whose ownership is represented by a digital token may only respond to commands signed by what it, and everyone, recognizes as the car's owner. "Open the door" could be a message signed by the owner's private key. The car would see this, be able to verify everything trustlessly, and comply. Other messages, signed with other private keys, would be disregarded.

Ownership may also be transferred. An owner, after selling his car-ownership token to someone else, may no longer issue commands to the car, which has recognized the change in ownership and responds accordingly to its new owner. The transfer of rights occurs entirely without a trusted third party arbiter. Passwords may not be copied nor keys replicated. There is no trust necessary on the part of the device or owners. Ownership becomes transparent, mathematically secure, and highly fluid. Access rights themselves become algorithmically transferrable between machines.

3 Abstracting Tokens above Bitcoin

Digital tokens may be represented on top of the Bitcoin Blockchain with additional metdata encoded in Bitcoin OPRETURN transactions. An agreed upon protocol can interpret specially crafted Bitcoin transactions to represent transfers of digital tokens. Relying upon the Bitcoin Blockchain confers several important advantages, not the least of which are security and longevity. Numerous protocols already exist to this effect, including CounterParty, MasterCoin, and Open Assets Colored Coins. While existing protocols work as intended, they lack SPV, or simple payment verification, introducing scalability problems. While the encoded information is secure and transferrable on the Bitcoin Blockchain, verifying the validity of metadata-inscribed transactions is a computationally laborious process. Either a database must be maintained monitoring the entire Blockchain, or, to verify a single transaction, an exponentially scaling back-trace must be performed through the transaction history. Because numerous inputs often map to a single output, going backwards in time involves exploring a tree of transactions that grows exponentially. Bitcoin itself avoids this problem because it has SPV built into the protocol. But meta-protocols built on top of Bitcoin do not have SPV, hence they, so far, scale poorly.

This protocol directly addresses the scalability problem of metacoins built on top of the Bitcoin Blockchain. Unlike previous Colored Coin implementations, which have sought to be as general as possible, involving the potential mixing of large numbers and kinds of colored coins, BlockFate transactions are more constrained. In a given digital token transaction, each output must map uniquely, based on order, to a single input. Different tokens can therefore be moved en masse, but are not mixable on the level of outputs. Because one colored input directly maps to one colored output, the backscanning process reverts from exponential scaling to linear scaling. This dramatically improves the feasibility of this technique at scale.

4 The Mechanics of Ownership

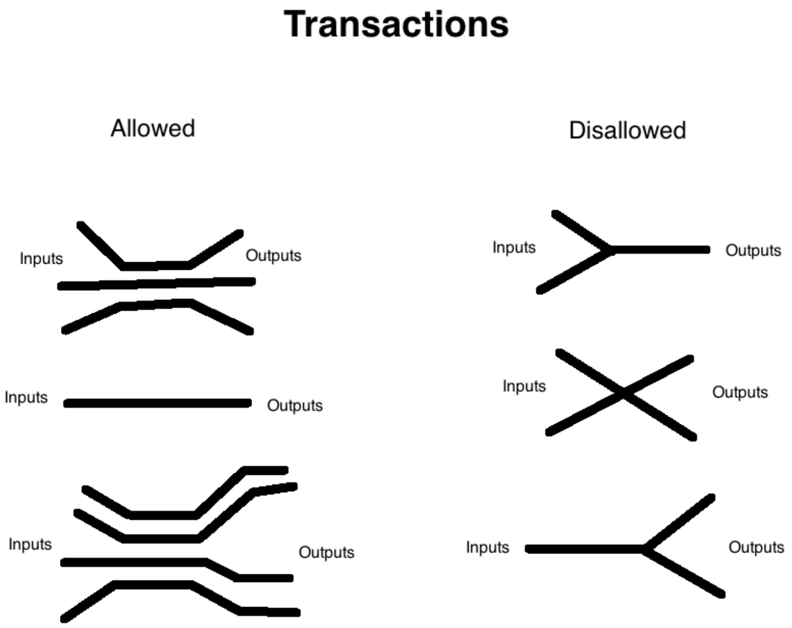
4.1 Transferring Tokens

As stated above, to simplify authentication of metadata written on the Bitcoin Blockchain, the format for the transfer of digital tokens has been constrained to one token input for each token output. Hence tokens move indivisibly and thus, in practice, one at a time. Since they represent control over physical devices, different tokens always represent fundamentally different asset classes. Thus the lack of divisibility should not be an impediment.

The transfer of a token occurs as follows. Taking cues from previous incarnations of Colored Coin protocols, a transaction consists of inputs, some of whom are colored, some of whom are not colored. Output colors are order-based vis-a-vis inputs. The first output maps to the first input, etc. An OPRETURN output separates colored outputs from regular Bitcoin outputs. Different colored outputs may consist of separate colors (indeed they always will). It is assumed that the corresponding input is of the same color. If it is not, the transaction is not legitimate.

Metadata is stored in the OPRETURN Statement. This metadata indicates

- That this is a BlockFate protocol transaction of version 1.0
- The type of operation performed. In this case, a transfer of ownership requires no identifier. But other types of operations do.



4.2 Issuing Commands

Commands are cryptographically signed messages instructing devices what to do, as signed by owners and licencees. Devices must be aware internally of the correctness of the messages they have received. By monitoring the Blockchain, devices will be aware of the public addresses that have access rights, what those specific rights are, under what terms they exist, and for how long. Besides querying the Blockchain, there should be no need for external data to ascertain these rights. Devices receive commands and decide whether they are legitimate. This involves checking the signing of messages as compared against the known public addresses of its controllers. The contents of commands may differ between devices based on their particular specifications. These can be agreed upon in advance and are specific to each device. Various methods may exist for devices to receive commands. They may be sent directly via a physical connection. They may be sent as HTTP requests. They may be publically posted on a common website, encrypted with a timestamp for the recipient device, which also has a public key. Because messages can be encrypted only for their recipients, they may be publically posted without loss of anonymity.

4.3 Monitoring the Blockchain

Devices must monitor the Blockchain to stay current on who has access rights at any given time. Since Bitcoin blocks come out every 10 minutes on average, the bandwidth requirements should not be too serious. Low-trust solutions may require even an even more trivial amount bandwidth.

Potential Attacks and Solutions

- Race Attacks, in which ownership is transferred, but in the intermediary time between blocks, the previous owner issues malicious commands. For many devices, malicious commands may not really exist. For others, a Blockchain-based contractual-command could be issued, ordering the device to HALT instructions for a given amount of time. This order, encoded on the Blockchain and in force for the device for a certain amount of time, would supercede any malicious commands later performed by the seller. This halted status would also be provable to buyers as it would be on the Blockchain. The halted status would be designed to encompass only the next few blocks.
- Disconnecting the device from the Internet while simultaneously selling access rights. If the device is not updated, it is not aware of the change in ownership. Devices should be able to write their own cryptographically signed messages with private keys unavailable even to owners. They should be able to respond to queries about what block they have reached in a cryptographically provable way. Thus buyers could verify the up-to-dateness of devices.

4.4 A Lightweight Wallet

A central goal of BlockFate is to create lightweight clients that monitor the movement of a particular class of digital token in a secure, trustless fashion. Storing the entire Bitcoin Blockchain clientside is too onerous for small devices.

Instead, a thin-client approach will be applied. Blocks may be inspected one at a time from a device's internal 'moment of creation', checking merkle roots and block headers. Only limited metadata pertinent to that individual device need be stored locally. While each device will require an internet connection, at least sporadically, the computational and storage burden client-side should be sharply reduced.

4.5 Monitoring from a Device's Perspective

Devices must perform the following actions regularly to keep up-to-date with the Blockchain.

- Search for Bitcoin Nodes that can supply Block Data and maintain an adequate list of neighbors.
- Download blocks and confirm Block Headers.
- Verify the merkle root of each Block.
- Iterate through the list of transactions for block, looking for an instance in which the Last-Known-Owner's public address has been involved.
- In any cases where the Last-Known-Owner's public address has been involved, try to parse metadata.

Parsing Metadata involves the following

- Decide whether this is an ownership transfer transaction. If the unspent output representing ownership from the device's last transfer transaction is an input in the transaction, then ownership is being transferred again. Unspent Outputs are used from one transaction to the last to harness Bitcoin's implicit double-spending defenses. As long as the device knows which unspent output represents its own ownership, there can be no double-spend attack.
- If there is no transfer transaction this block, then look for OPRETURN transactions involving the Last-Known-Owner.
- Of the OPRETURN transactions found, check for any explicitly labelled as BlockFate Protocol transactions. They will be so marked in the OPRETURN 40 byte field.
- Specific instructions as to the device's status may be included in these OPRETURNs. These instructions are temporary, contractual commands, such as rental agreements, or guest access rights. Devices acknowledge these contractual commands in order of occurrence, with certain kinds of commands invalidating others under certain circumstances. Contractual Commands are device specific. They are generally not superceded by transfers in root ownership. They are also publically visible on the Blockchain, so the state of a device cannot be hidden from potential buyers.
- At all times each device must be aware of the public address of its Last-Known-Owner, the unspent output transaction hash with index of its last ownership transfer, and the current state of any active or pending contractual commands, purely from queries to the Bitcoin Blockchain.

4.6 Rules Governing the Parsing of Contractual Commands

Contractual commands are published on the Bitcoin Blockchain as OPRETURN messages sent by the recognized device owner. They do not involve transfers of ownership, but instead represent binding declarations of intent by the owner. Different kinds of devices may have different permissible contractual commands. The validity of contractual commands depends on numerous factors. Whereas device ownership is always represented on the Blockchain, the validity of contractual commands depends on their order, timing, internal logic, and compatibility with pre-existing rules. While the legitimacy of contractual commands must be calculated by devices, all of the inputs necessary for an unambiguous, predictable decision should be drawn from the Bitcoin Blockchain. In general they shall follow the following rules:

- Order matters. Contractual commands issued first, as measured by block, receive precedence first. If occuring on the same block, commands listed first on the block take precedence.
- Every contractual command has an explicit or implicit duration of effect. No contract may last forever, though it may be endlessly renewed.
- Given commands issued in quick succession, the first will be valid. If successive commands are issued before the expiration of the first valid command, the subsequent commands are illegitimate and ignored.
- Contractual commands may never be reneged once issued.
- Transfers of ownership may be performed before the fulfillment of issued Contractual commands. However the new ownership will not be recognized until the expiration of previous contracts. This is to prevent fraud against counter-parties in contractual agreements. Buyers of devices should be aware, via the Blockchain, of the locked state of any devices.

4.7 Example Contractual Commands

These would be encoded as sets of OPRETURNS on the Blockchain. Their purpose is not to encompass all possible commands to devices, but to provably write temporary access privileges (so further commands can be issued off-blockchain). I have shown the general format only.

- LOAN X to A - Give access rights to address A for the next X Bitcoin Blocks.
- LOAN X IF Y at Z to A - Give access rights to A for the next X blocks if Y Bitcoin paid to Z.
- GUEST RIGHTS to A - Give guest access only to A.
- HALT X - Halt further Contractual Commands for this device for X Blocks.
- DO X IF Y ELSE Z - Perform a specific device-specific command if criteria Y is met. Otherwise do command Z.
- WHILE X, Y - While X criteria is true, the device should perform command Y.

5 A Changed Paradigm of Physical Ownership

The BlockFate protocol seeks to introduce fundamentally new capabilities in handling access rights vis-a-vis the physical world. Current definitions of ownership are especially backwards. They refer either to nebulous, informal physical possession, or centrally documented rights stewarded by lawyers, accountants, and regulators. Nowhere is ownership truly absolute. Instead there lie several invisible layers, whole industries, deadening owners' control over their assets. We live in a world where one must constantly ask permission, to wait three business days, and to surrender personal information, just to exercise ownership over private goods. Because in the past we could never be true executors over our own possessions, the Intermedaries that Be have commanded great value at our expense. No longer.

With a private key, your ownership of your car, or your digital book, or your rented billboard, or even your house, are self-evident and self-enforcing. You shall have no need for recourse to external arbitration, the interpretation of contracts by expensive lawyers, the processing fees, the delays, and the mediocrity. Your private key will be your word. Math will do what laws strive to do.

Inscribing real-world access in Satoshi's Blockchain is more than just an improvement on existing methods. It opens up fundamentally new possibilities. You may send someone the keys to your house in seconds from across the world. You may even sell your house completely. The new owner need not worry that you still have access or have attempted to double-spend. Devices may monitor the Blockchain for contractual agreements of dizzying complexity. There will be no space for interpretation. Rental agreements, safety deposits, contingencies, and more may be programmed irrevocably and unforgeably on the Blockchain. The ease, the fluidity, and the sophistication of such transactions will be unprecedented.

If a private key can control physical devices, digital content, and access rights to devices, then so can machines themselves own other machines. If ownership is digital, then may not digital entities also be owners? BlockFate makes this possible.

6 Programmable Physical Ownership: Access Rights, Rental Agreements, and More

If a machine can be an owner, then ownership itself can be programmed. Used cars could be algorithmically traded between automated, self-regulating car dealerships. Equipment could be rented with a safety deposit, paid directly to the device, which returns the deposit minus rental fees when it detects it has been returned. Perhaps then it forwards the profits to its owner, man or machine.

With ownership subject to digital rules, a panoply of possible variations unfold. Personal assets that would otherwise be too tedious to rent out, or to resell, may be trivially monetized. Objects for which the legal transactions fees are too high, or the exchange friction too great, may suddenly become tradeable when enforcement is automatic and the incentive for theft exactly nil. Consider the phone aware of its owner's public address, who would ever bother stealing it? Such a phone could be sold and resold, until utter obsolescence, because no party would ever be subject to exchange risk.

Vastly more complicated contingencies could be developed. Because devices monitor the Blockchain, they may track money transfers in addition to ownership and contractual commands. Consider the parking space aware of whether it has been paid for recently. It need only check the Blockchain. Or perhaps the rental car, sensing that it has been driven past the mileage limit, which withholds an additional fee. Monitoring payments in real-time, as well as responding to precise, publicly visible messages from owners, mean that ownership and lesser rights, guest rights, leasing, rental, etc, may all be programmed to virtually any contingency.

7 Conclusion

The existing paradigm of Blockchain-as-currency is only one of many uses of a universal-consensus-ledger. Giving devices algorithmic awareness of their own ownership, and securing access rights with cryptographic tools, could dramatically multiply the number of ways to monetize devices, data streams, and distributed sensor networks.

While some applications may seem far-fetched, others surely lie closer to home, such as monetizing street cameras, rental cars with safety deposits, and home security. The coexistence of device access rights on the same network as a payment mechanism, Bitcoin, is an elegant and secure symbiosis.