Personal Blockchains:
Proof of Integrity in a Centralized System

DRAFT (2018.01.29)

Abstract. A published consensus of rules governing interactions between a centralized system and each of its users would allow for proof of integrity between the two parties and to any concerned observer. Decentralized blockchains allow for the easy and secure transfer of funds to and from a centralized system, but cannot offer accounting for what happens within the system. We propose a solution to the problem of accountability using personal blockchains to bridge the gap between decentralized blockchains. The centralized system publishes a set of rules for interactions with services provided and each party signs their requests or service receipts, verifying the validity of each as they are received. Mining is not necessary. Privacy is maintained by default unless a party chooses to make public a part of the personal blockchain. A disagreement can be fairly judged by any impartial observer.

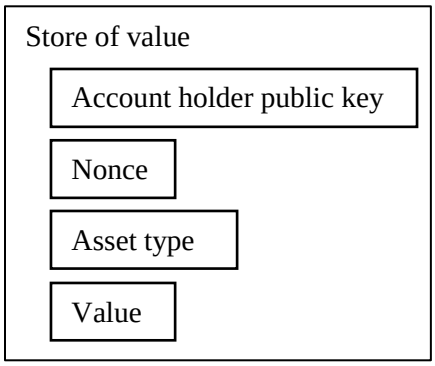
1. Introduction

Services available on the Internet are almost exclusively provided by centralized systems, mirroring the centuries-old model used by all businesses, large and small. The trend is familiar and unlikely to vanish. Bitcoin introduced a peer-to-peer electronic cash system[1] to solve the problem of the inherent weaknesses of a trust based model. While a payment system using cryptographic proof instead of trust is essential, the solution is incomplete if the service being paid for relies on trust. The Internet is replete with confusion and complaints by customers facing challenges in their dealings with centralized systems. Both customer and service provider may state a position on the facts of a matter, but neither has proof, and disputed facts often can never be decided with certainty. A business will often take up the burden of a marketing and public relations effort to establish trust and sway opinion, but the efforts consume valuable resources and have limited effect. Cryptographic proof of integrity would enhance the efficacy of such efforts.

The system of cryptographic proof used by decentralized payment systems could be applied to a service provider. Ideally, the request for service and the service itself can be defined and verified by a published set of rules and secured by cryptographic proofs. If accomplished, an unbroken chain can be created, providing proof of integrity. In the case that a service, by its nature, cannot be proven by a computer algorithm, there may still be strong benefits to implementing the system to the maximum degree possible.

2. Store of Value

We propose that assets held on account are defined at minimum by an immutable data structure.



The store of value can represent any type of asset or liability, whether digital, like Bitcoin or game tokens, or tangible, such as gold, dollars or real estate.

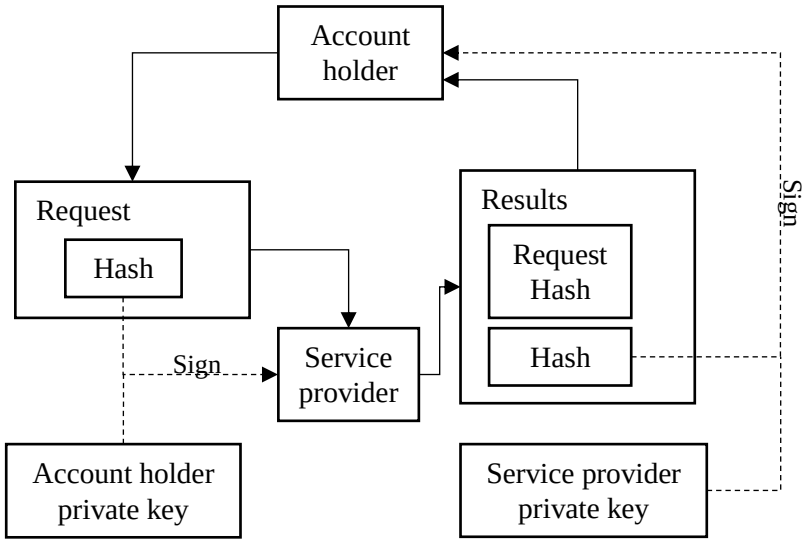
3. Contracts

Contracts can exist in any form, the parameters of which must be represented in a data structure. The rules governing each contract must be published and available to any potential third party judging the fairness of execution. There are no limitations as to the function of the contract.

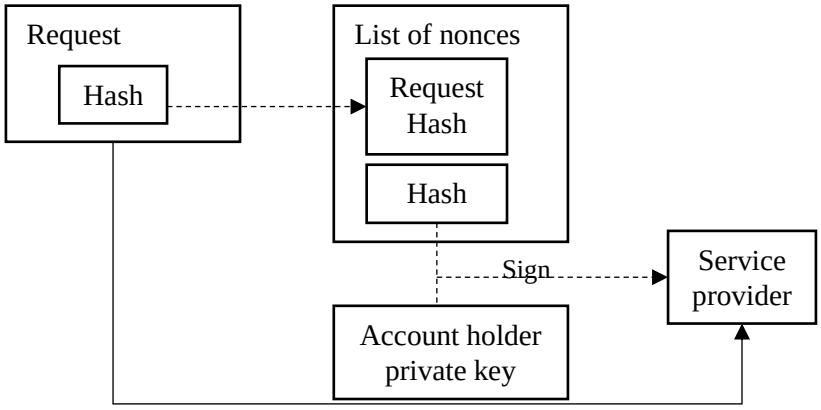
Assets or liabilities held in stores of value are created and consumed only through the fulfillment of contracts.

4. Transactions

Requests for service by way of contract are digitally signed by the account holder. The results of contract execution are digitally signed by the service provider and must include the request itself.



Stores of value will be consumed as required by the contract. Authorization is indicated by including the nonce of each store of value as part of the digital signature.



The service provider can prove that service was requested, and the details of the request, by way of the account holder's digital signature. The account holder can prove the results of the service, as well as the details of the request, by way of the service provider's digital signature.

Consumption of a store of value can be proven while maintaining privacy as to how it was consumed. Only the request hash and a list of nonces must be provided along with a digital signature as proof of consumption.

5. Resources

Maintenance of personal blockchains requires minimal resources. Implementation of the system is not expected to pose a significant burden on any typical or future consumer grade computer system.

Mining is not required. There is no double-spending problem in a centralized system, so each transaction itself forms a link in the personal blockchain. The only computational overhead is a single digital signature and verification, requiring only a fraction of a second.

The system does not require broadcasting of transactions, since by default, transactions are private between account holder and service provider. The digital signature required during communications typically adds only a few bytes of data and represents a negligible bandwidth overhead.

Storage requirements differ between account holders and service providers. The account holder typically only needs to store a record of unspent stores of value and contracts which have not yet finished execution. The actual storage requirements depend on the implementation details of the personal blockchain, however it is expected to require orders of magnitude less data storage than a decentralized blockchain. The service provider typically should maintain a record of all transactions, although requirements depend on the needs of the service provider. In particular, requests consuming stores of value should be retained. Most centralized services already retain a transaction history, so it is expected that storage requirements of personal blockchains would not be significantly different.

6. Incentive

There is a strong incentive for a centralized service to act fairly. Acting in discordance with a published contract has reputational implications, as the offended party can publicly publish cryptographic proof of the facts. Presumably, this would tarnish the reputation of a business or threaten their existence altogether. As the popularity of a business increases, so does the incentive to continue to act with integrity.

There is also a disincentive for users to falsely make public complaints about a business. The business can defend against inaccurate complaints by demanding a digital signature or providing one themselves, depending on the circumstance.

In some cases, users unintentionally make false complaints, whether publicly or via support channels. Having a record proven by digital signatures can create clarity. The unfortunate circumstances of a user's computer being hacked and assets stolen, and that of a business simply stealing the assets themselves, are distinguishable only by the production of digital signatures from the personal blockchain.

7. Conclusion

We have proposed a system providing for accountability in a centralized system. We borrowed the concept of decentralized blockchains for payments and adapted it for use in centralized systems. The use of stores of value in conjunction with an open ended system of contracts was proposed. Together with the use of digital signatures, a centralized system can provide improved, or even perfect proof of integrity.

References

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf, 2008.