AZZOTTObit

Cryptocurrency

-: White Paper :-

Table of Contents

Preamble

In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest. Our core development principles and strategies are based on: security in depth, simple and modular code, clarity driven naming convention, comprehensive unit testing, pre-and-post-condition sanity checks, code consistency, and regular audits.

AZZOTTObit operates as a custom decentralized system for our News, Entertainment, Social Interaction, Streaming and Research platform, governed and built on Ethereum. The platform is powered by its core token, AZZOTTObit. AZZOTTObit tokens are essentially membership certificates in the AZZOTTO Platform, which give the following rights and privileges to their owners provided compliance policies of AZZOTTO and proof of member activity confirmed by running an AZZOTTO node on the member's computer:

The AZZOTTO platform aims to be the world's first fully diversified integrated digital News, Entertainment, Advertising and Social Interaction honest trading platform for .promoting creativity and widening the current talent pool.

Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services.

With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof through computing instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers.

Abstract

Blockchain is fundamentally a new type of database technology that is optimized to tackle a unique set of challenges. Historically, databases have been used as central data repositories by organizations to support transaction processing and computation. However, databases are rarely shared between organizations due to a variety of technology and security concerns. Blockchain is a shared, distributed database of transactions among parties that is designed to increase http://atlant.io 10 transparency, security, and efficiency.

Blockchain is a database (with copies of the database replicated across multiple locations or nodes) of transactions (between two or more parties) split into blocks (with each block containing details of the transaction such as the seller, the buyer, the price, the contract terms, and other relevant details) which are validated by the entire network via encryption by combining the common transaction details with the unique signatures of two or more parties. The transaction is valid if the result of the encoding is the same for all nodes and added to the chain of prior transactions (as long as the block is validated). If the block is invalid, a “consensus” of nodes will correct the result in the non-conforming node. The blockchain ledger is replicated across multiple locations (we show just six in Figure 7 for simplicity), and each maintains its own copy, which is separately updated based on new transaction data. We show a sequence of three transactions. In the first two transactions, data and signature information are properly validated by all six nodes with matching “hash” values. However, for Transaction #3 at Location #5, the hash does not match the others, and will be corrected by the others via “consensus.”

Security:
Blockchain relies on encryption to validate transactions by verifying the identities of parties involved in a transaction. This ensures that a "false" transaction cannot be added to the blockchain without the consent of the parties involved. A complex mathematical calculation known as a "hash" is performed each time a transaction is added to the blockchain, which depends on the transaction data, the identities of the parties involved in the transaction, and the result of previous transactions. The fact that the current state of the blockchain depends on previous transactions ensures that a malicious actor cannot alter past transactions. This is because if previous transaction data is changed, it will impact the current value of the hash and not match other copies of the ledger. ?

Transparency:
By its very nature, blockchain is a distributed database that is maintained and synchronized among multiple nodes – for example, by multiple counterparties who transact with each other frequently. In addition, transaction data must be consistent between parties in order to be added to the blockchain in the first place. This means that by design, multiple parties can access the same data (in some cases locally within their organizations) – thus significantly increasing the level of transparency relative to conventional systems that might depend on multiple "siloed" databases behind firewalls that are not visible outside a single organization.

Efficiency:
Conceptually, maintaining multiple copies of a database with blockchain would not appear to be more efficient than a single, centralized database. However, in most real-world examples (including several of the case studies we examined in capital markets), multiple parties already maintain duplicate databases containing information about the same transactions. In many cases, the data pertaining to the same transaction is in conflict – resulting in the need for costly, time-consuming reconciliation procedures between organizations. Employing a distributed database system such as blockchain across organizations can substantially reduce the need for manual reconciliation, thus driving considerable savings. In addition, in some cases blockchain offers the potential for