Ziotta - (ZTTA)

ZIOTTA

Whitepaper

TECHINVENTOR

Table of contents

History

The concept of decentralized digital currency, as well as alternative applications like property registries, has been around for decades. The anonymous e-cash protocols of the 1980s and the 1990s, mostly reliant on a cryptographic primitive known as Chaumian blinding, provided a currency with a high degree of privacy, but the protocols largely failed to gain traction because of their reliance on a centralized intermediary. In 1998, Wei Dai's b-money became the first proposal to introduce the idea of creating money through solving computational puzzles as well as decentralized consensus, but the proposal was scant on details as to how decentralized consensus could actually be implemented. In 2005, Hal Finney introduced a concept of "reusable proofs of work", a system which uses ideas from b-money together with Adam Back's computationally difficult Hashcash puzzles to create a concept for a cryptocurrency, but once again fell short of the ideal by relying on trusted computing as a backend.

Because currency is a first-to-file application, where the order of transactions is often of critical importance, decentralized currencies require a solution to decentralized consensus. The main roadblock that all pre-Bitcoin currency protocols faced is the fact that, while there had been plenty of research on creating secure Byzantine-fault-tolerant multiparty consensus systems for many years, all of the protocols described were solving only half of the problem. The protocols assumed that all participants in the system were known, and produced security margins of the form "if N parties participate, then the system can tolerate up to N/4 malicious actors". The problem is, however, that in an anonymous setting such security margins are vulnerable to sybil attacks, where a single attacker creates thousands of simulated nodes on a server or botnet and uses these nodes to unilaterally secure a majority share.

The innovation provided by Satoshi is the idea of combining a very simple decentralized consensus protocol, based on nodes combining transactions into a "block" every ten minutes creating an ever-growing blockchain, with proof of work as a mechanism through which nodes gain the right to participate in the system. While nodes with a large amount of computational power do have proportionately greater influence, coming up with more computational power than the entire network combined is much harder than simulating a million nodes. Despite the Bitcoin blockchain model's crudeness and simplicity, it has proven to be good enough, and would over the next five years become the bedrock of over two hundred currencies and protocols around the world.

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 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. 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 nodes collectively control more CPU power than any cooperating group of attacker nodes.

Ziotta: Peer-To-Peer Electronic Cash System

Mergas Satwa
mergassatwa@ziotta.com
www.ziotta.com

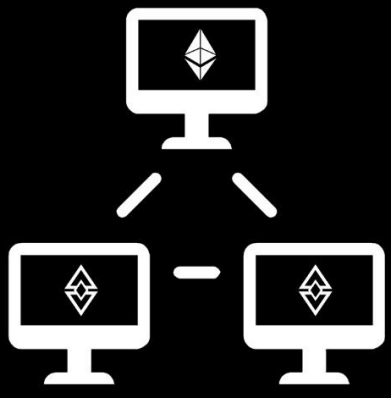
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they wil generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

ERC20 Blockchain Based Ethereum

An ERC20 token is a blockchain-based asset with similar functionality to Bitcoin, Ether, and Bitcoin Cash: it can hold value and be sent and received.

The major difference between ERC20 tokens and other cryptocurrencies is that ERC20 tokens are created and hosted on the Ethereum blockchain, whereas Bitcoin and Bitcoin Cash are the native currencies of their respective blockchains.

ERC20 tokens are stored and sent using Ethereum addresses and transactions, and use gas to cover transaction fees.



Ziotta - (Ethereum protocol)
using ERC20

Smart Contract

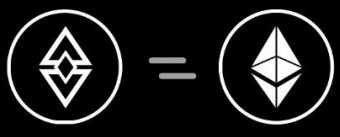
Smart contracts are applications that run on the Ethereum Virtual Machine. This is a decentralized "world computer" where the computing power is provided by all those Ethereum nodes. Any nodes providing computing power are paid for that resource in Ether tokens.

They are named smart contracts because you can write "contracts" that are automatically executed when the requirements are met.

For example, imagine building a Kickstarter-like crowdfunding service on top of Ethereum. Someone could set up an Ethereum smart contract that would pool money to be sent to someone else. The smart contract could be written to say that when $100,000 of currency is added to the pool, it will all be sent to the recipient. Or, if the $100,000 threshold hasn't been met within a month, all the currency will be sent back to the original holders of the currency. Of course, this would use Ether tokens instead of US dollars.

This all would happen according to the smart contract code, which automatically executes the transactions without the need for a trusted third party to hold the money and sign off on the transaction. For example, Kickstarter takes a 5% fee on top of a 3% to 5% payment processing fee, which would mean $8000 to $10000 in fees on a $100,000 crowdfunding project. A smart contract wouldn not require paying fees to a third-party like Kickstarter.

Smart contracts can be used for many different things. Developers can create smart contracts that provide features to other smart contracts, similar to how software libraries work. Or smart contracts could simply be used as an application to store information on the Ethereum blockchain.



Ethereum smart contract

Utilities - cryptoasset

Using digital currency you can complete payments much faster than current means, like ACH or wire transfers, which can take days for financial institutions to confirm a transaction. Less expensive international transfers.

- Payment Gateway
- Sport
- Art Industry
- Digital Finance
- Digital Asset
- Tech Innovation

Ziotta - digital currency functionality

Ziotta ecosystem

Go-Cashless

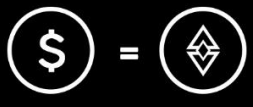
Bullish Movement After the Pandemic

Transparency Transaction

More Businesses to Accept Ziotta Payments

Experts Opinion

Decentralized Finance



DeFi and NFT

DeFi is a collective term for financial products and services that are accessible to anyone who can use Ethereum – anyone with an internet connection. With DeFi, the markets are always open and there are no centralized authorities who can block payments or deny you access to anything. Services that were previously slow and at risk of human error are automatic and safer now tha t they are handled by code that anyone can inspect and scrutinize.

A non-fungible token (NFT) is a unit of data stored on a digital ledger, called a blockchain, that certifies a digital asset to be unique and therefore not interchangeable. NFTs can be used to represent items such as photos, videos, audio, and other types of digital files. Access to any copy of the original file, however, is not restricted to the buyer of the NFT. While copies of these digital items are available for anyone to obtain, NFTs are tracked on blockchains to provide the owner with a proof of ownership that is separate from copyright.

In 2021, there has been increased interest in using NFTs. Blockchains like Ethereum, Flow, and Tezos have their own standards when it comes to supporting NFTs, but each works to ensure that the digital item represented is authentically one-of-a-kind. NFTs are now being used to commodify digital assets in art, music, sports, and other popular entertainment. Most NFTs are part of the Ethereum blockchain; however, other blockchains can implement their own versions of NFTs. The NFT market value tripled in 2020, reaching more than $250 million.

Decentralized Applications - dApps

Decentralized applications are a piece of software that communicates with the blockchain, which manages the state of all network actors. The interface of the decentralized applications does not look any different than any website or mobile app today. The smart contract represents the core logic of a decentralized application. Smart contracts are integral building blocks of blockchains, that process information from external sensors or events and help the blockchain manage the state of all network actors.

The frontend of a decentralized application represents what you see, and the backend represents the entire business logic. This business logic is represented by one or several smart contracts interacting with the underlying blockchain. The frontend, as well as files like a photo, a video, or audio, could be hosted on decentralized storage networks such as Swarm or IPFS. Traditional Web applications use HTML, CSS, and Javascript or the like to render a webpage. This page interacts with a centralized database, where all the data is stored. When you use a service like Twitter, Facebook, Amazon, or Airbnb, for example, the webpage will call an API to process your personal data and other necessary information stored on their servers, to display them on the page. User ID and passwords are used for identification and authentication, with low levels of security, since personalized data is stored on the server of the service provider.

Decentralized applications are similar to a traditional Web application. The frontend uses the exact same technology to render the page. It contains a "wallet" that communicates with the blockchain. The wallet manages cryptographic keys and the blockchain address. Public-key infrastructure is used for user identification and authentication. Instead of an API connecting to a database, a wallet software triggers activities of a smart contract, which interacts with a blockchain: Web3 compatible website: Front End (including wallet) → Smart Contract → Blockchain.

ZIOTTA - ZPocket for Ziotta Wallet and ZiottaX for Exchanger

Conclusion

Ziotta is more than its code sources, protocols and utilities. Ziotta is something that puts trust into cryptocurrency again and enable people to embrace it and uniting people and technology. As the time changes, so does the society. Ziotta provides 'smart contracts', cryptoassets for accesible online transactions, decentralized finance; Ziotta aims to go far beyond just currency. Ziotta will increase the efficiency of computational industry and provide better peer-to-peer(P2P) protocol from time to time. Ziotta believe that being united in both financial and non-financial protocols will be a greater good for the now and the future.

- ZIOTTA core developer

Ahmad Nasrun
Azril Salleh
Mergas Satwa
Judith Alushzka
Rauf Hamzah
Azli Shah
Tiffany Elynn
Najib Zacary
Alex Pang
Danial Pang
and
Community Board Members

Reference and further reading

Cryptography - Science and Technology
Blockchain Revolution, *Don Tapscott*
Financial Technology Era, *Op Zukurov*
Algebraic Aaspects of Cryptography, *Neil Koblitz*
Military Cryptanalysis (NSA-USA), *William F. Friedman*
Security Engineering, *Ross J. Anderson*
Network Security, *Charlie Kaufman - Radia*
Cryptography and Network Security: Principles and Practice, *William Stallings*
Codes and Cryptography, *Dominic Welsh*
Encyclopedia Of Cryptography And Security, *Unknown*
Cracking Codes with Python, *Al Sweigart*
Discrete Algebraic Methods, *Volker Diekert*
Security of Block Ciphers, *Kazuo Sakiyama, Yu Sasaki, Yang Li*
Algorithmic Number Theory, *J.P. Buhler, P. Stevenhagen*
Applied Algebra, *Darel W. Hardy, Fred Richman, Carol L. Walker*
Applied Network Security Monitoring, *Chris Sanders*
Defensive Security Handbook, *Lee Brotherston*
Complex Social Networks, *Fernando Vega-Redondo*
Writing Secure Code, *Michael Howard*
Bitcoin Organization
Ethereum Organization
USA
Russia
China
Turkey
2012 - 2021
>