VitaBridge: A Generic Decentralized Cross-Chain Transfer Protocol

Author: Vitalik Buterin
Contributors: Jeff Coleman, Jon Lee, Ben Fisch, Dan Boneh, Mustafa Al-Bassam, Alexander Chepurnoy, Ethan Buchman, Jae Kwon, Zarko Milosevic, Ivan Homoliak, Aggelos Kiayias, Ioannis Kaklamanis, Oliver Zhang, Kostis Karantias

Background

Single Chain

Blockchains are a technology that can be understood as being a decentralized version of a single-threaded computer. Ethereum, for instance, can be understood as being a decentralized version of the Intel x86 instruction set, with the ability to run any program, but with the property that every computational step that any program makes must be processed by every node in the network. Because of this property, blockchains are highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition. However, blockchains are also highly inefficient, because every node in the network must perform every computational step that any program on the blockchain makes, and because of this inefficiency, blockchains are limited in the amount of computation that they can perform, and they are also vulnerable to denial of service attacks, because an attacker can easily create a program that requires a very large amount of computation, and the network will be forced to process that program, and the network will be slowed down or even stopped by the attacker's program.

Multi-Chain

One way to address the inefficiency of blockchains is to create a multi-chain system, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient. However, multi-chain systems are also highly complex, because the blockchains must be able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, multi-chain systems are also vulnerable to denial of service attacks, because an attacker can easily create a program that requires a very large amount of communication, and the network will be forced to process that program, and the network will be slowed down or even stopped by the attacker's program.

Sharding

One way to address the complexity of multi-chain systems is to create a sharded system, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, sharded systems are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, sharded systems are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Cross-Chain Transfer Protocol

One way to address the complexity of multi-chain systems is to create a cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer protocols are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer protocols are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Cross-Chain Transfer Operations

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Cross-Chain Transfer Operations

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Contribution

Goals

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Assumptions

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Notation

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Definitions

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Blockchain

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Transaction

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Block

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Header

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Problem Statement

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Cross-Chain Transfer

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Cross-Chain Transfer Operations

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Cross-Chain Transfer Operations

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Asynchronous Transfer Model

Cross-chain transfer operations are a type of cross-chain transfer protocol, in which there are many blockchains, and each blockchain is responsible for a different part of the system, and each blockchain is only responsible for processing the transactions that are relevant to its part of the system, and the blockchains are connected to each other by a protocol that allows them to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this complexity, cross-chain transfer operations are also highly efficient, because the blockchains are able to communicate with each other and to exchange information about the state of the system, and to coordinate their actions with each other, and to ensure that the system as a whole is secure and efficient, and because of this efficiency, cross-chain transfer operations are also highly secure, because the network can easily reach consensus about the correct state of the system, and it can easily detect if any attacker attempts to make an invalid state transition.

Cross-Chain Transfer