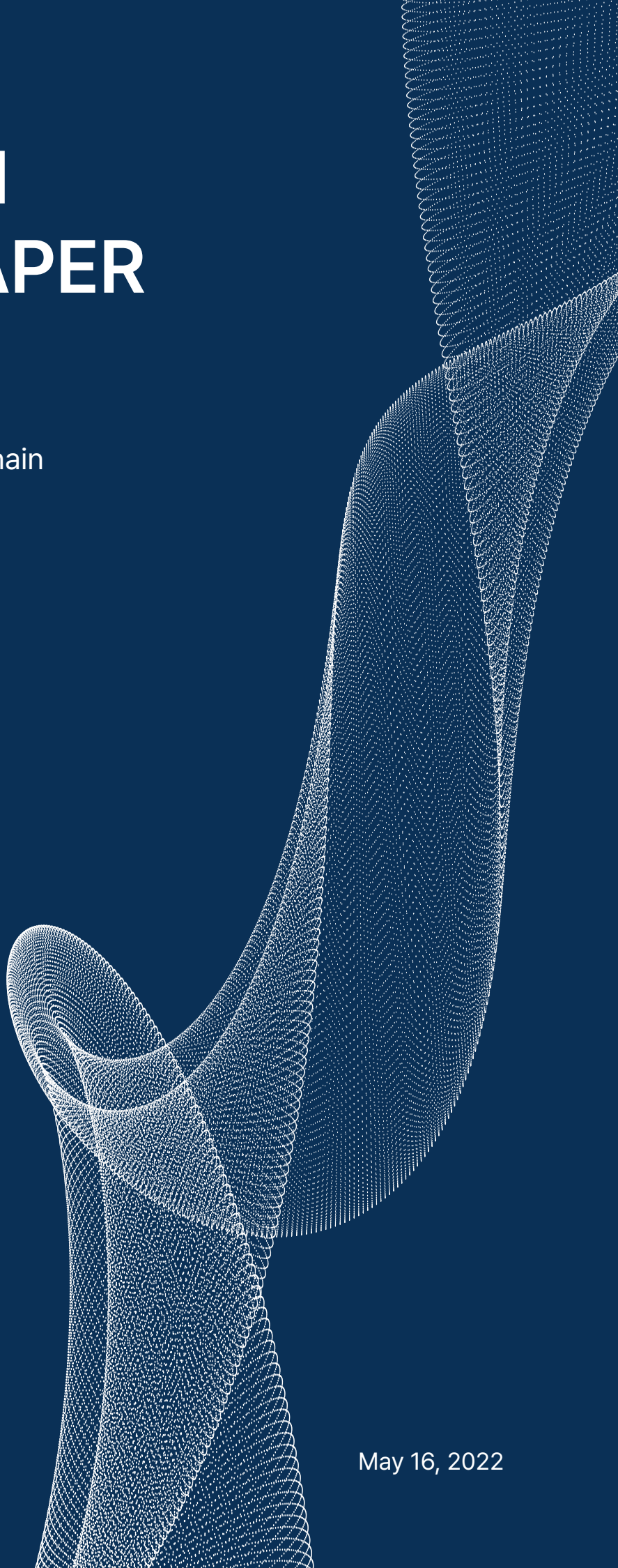
PROTOCON YELLOW PAPER

PART 2: FACT HASH

Fact, Fact Hash, and Cross-chain



Choi, Yoon-il
Bae, Min-hyo

May 16, 2022

Table of Contents

1. Overview

This document discusses Fact and Fact Hash, technical elements critical for data processing by the Mitum blockchain- the core technology of the Protocon network. It introduces and defines the concepts, features and benefits of Fact and Fact Hash, which was never proposed in the history of the blockchain industry.

In addition, this document describes the cases in which Fact Hashes can be utilized; particularly focusing on how it can be used to enable interoperations between heterogeneous blockchains.[1]

When heterogeneous blockchains are linked with each other-so called 'cross-chained'- what matters is the issue of trust accompanied as to whether the bridge [2] service linking two blockchain based off-chains can be trusted or not. If the bridge contains certain vulnerabilities or attack vectors, it may be exposed to security breaches such as hacking. Fact Hash provides a highly effective solution to address certain issues.

Following Section 1, Section 2 hereof describes the background and the necessity of introducing Fact and Fact Hash, while Section 3 defines and explains how Fact and Fact Hash can be used in any business. Section 4 explains the generic structure of cross-chain, its operating mechanism along with the common security issues, which Fact Hash can effectively handle. Section 5 addresses the conclusion of this paper.

2. Background & Necessity

2.1 Background

Blockchain is a shared, immutable ledger for recording transactions[3], tracking digital assets and building trust. In order to find the record of a specific transaction, an ID which can uniquely identify the transaction is required. This is referred to as Transaction Hash or Transaction ID.

[Fig.1] illustrates the structure of an Ethereum transaction. In general, most blockchain transactions have similar structures to the transaction structure presented below.

---

[1] Heterogeneous blockchains may refer to not only public blockchains including Bitcoin, Ethereum, Solana, etc. but also private blockchains such as Hyperledger Fabric.
[2] A blockchain bridge refers to a system that allows users to transfer assets and data between heterogeneous blockchain networks.
[3] Setting aside digital asset transfers, blockchains supporting smart contracts record the execution of each and every instruction constituting a smart contract also as a transaction.

Field	Description
Nonce	Account Nonce
From	Sender address
To	Recipient address
Value	Amount of cryptocurrency sending to the recipient
Payload	Transaction data
Gas Limit	The gas limit for the transaction
Gas Price	The price of the gas determined by the transaction initiator
V, R, S	The signature output values

[Figure 1] Ethereum Transaction Structure

The transaction hash (or transaction ID) that serves as the separator of each transaction is calculated as a hash value of the transaction contents-illustrated in the above figure-and Ethereum uses the following calculation formula.

Ethereum Transaction Hash
= Keccak-256(RLP(nonce,gasPrice,gasLimit,to,value,data,v,r,s))

[Figure 2] Ethereum Transaction Hash Calculation Formula

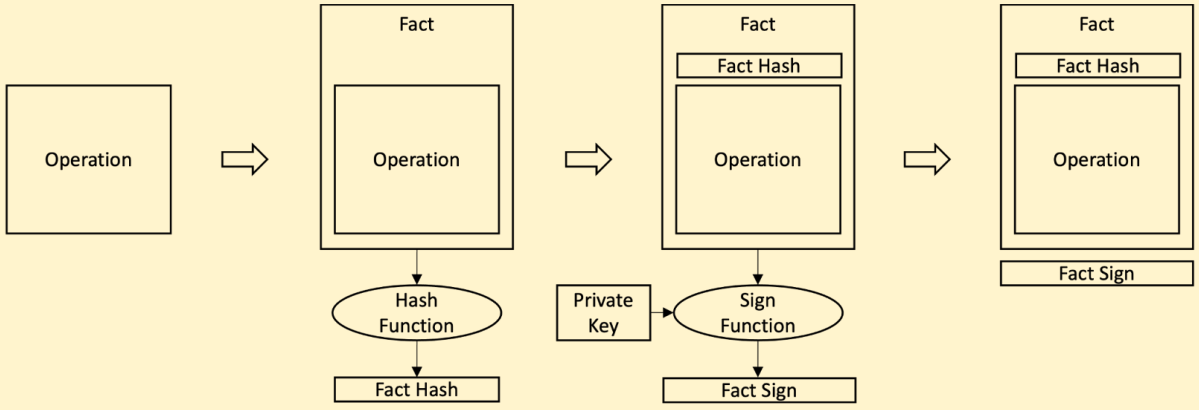
An Ethereum transaction hash is constructed by RLP encoding and Keccak-256 hash calculation with the value of each transaction field such as Nonce, Gas Price, and parameters(v, r, s, etc.) used in digital signatures.

In order to find the value of a transaction hash with calculation, the value of each field in a transaction must be recognized. Yet, when it comes to a digital signature, a private key is necessary, which means no-one other than the owner of the account who generated the transaction can calculate. This means, the calculation is possible in effect only by the owner of the account. Therefore, in the case of Ethereum, transaction hashes must be recorded separately and be utilized as keys when necessary in order to search and confirm transactions, such as cryptocurrency transfer records. In other words, verifying or confirming the processing results of transactions cannot be automated nor systemized; this poses a security vulnerability to the configuration of a bridge between heterogeneous blockchains.

2.2 Necessity

Protocon's Mitum blockchain allows hashes to be calculated only with the main transaction contents. In other words, by using the Mitum blockchain, anyone can search for specific transactions and verify whether the transaction is well processed or not.

[Fig. 3] illustrates the generating process of a certain transaction based on the Mitum blockchain. The terms used in the figure below is defined in Section 3, but it is fair to say that a fact can be understood as a transaction, a Fact Hash as a transaction hash, and a fact sign as a transaction signature.



[Figure 3] Mitum Blockchain Transaction Generation Process

When a transaction (such as cryptocurrency transfer) occurs, the Mitum blockchain recognizes it as an operation and abstracts it into a 'fact'. The fact is calculated with a hash function to generate a 'Fact Hash', and then it includes the fact as an element.

Since the process does not include any private key, anyone can calculate a fact and a Fact Hash as long as the contents are recognized.

In the case of a transaction related to the cryptocurrency transfers, a Fact Hash corresponding to a transaction hash can be calculated along with the sender address, the receiver address, and the transaction amount. The transaction can be retrieved, and its status can also be confirmed by calculation even if one does not recognize the Fact Hash.

Subsequently, transaction ID can be created by using the digital signature of the account owner-who generated the transaction. As the transaction ID is made through a separate process subsequent to the generation of the transaction and the transaction hash, the transaction hash itself can be calculated without the account owner's digital signature,

namely, the private key. Normally, transaction IDs are not disclosed and it contains sign values of private keys, making it difficult to search and to specify transactions. However in Protocon network, the Fact Hash consists of only disclosed information, so it can be used as a transaction key value. Therefore, it has the advantage of being secure and tracking transactions in a much easier way.

This hash calculation approach enables transactions in need of verification to be tracked easily even in a random moment; and it can happen without synchronizing all Protocon blocks in cryptocurrency wallet, off-chain, and at bridge, etc.

This method can ensure reliability of interoperations between blockchains, not only drastically stepping up off-chain data reliability but also enabling De-Fi services utilizing heterogeneous blockchains and cryptocurrencies.

3. Definitions

Section 3 defines ‘Fact’ and ‘Fact Hash’ and explains their benefits.

3.1 Fact

In the Mitum blockchain, all operations in a blockchain[4] are defined as a ‘Fact’.

The Mitum blockchain abstracts all kinds of operations in a blockchain into facts and includes various contents and hash values.


```
{
  "_hint": "mitum-currency-create-accounts-operation-fact-v0.0.1",
  "hash": "3Zdg5ZVdNFRbwX5WU7Nada3Wnx5VEgkHrDLVLkE8FMs1",
  "token": "cmFpc2VkIGJ5",
  "sender": "8PdeEpvqfyL3uZFHRZG5PS3JngYUzFFUGPvCg29C2dBn-a000:0.0.1",
  "items": [
    {
      "_hint": "mitum-currency-create-accounts-single-amount-v0.0.1",
      "keys": {
        "_hint": "mitum-currency-keys-v0.0.1",
        "keys": [
          {
            "_hint": "mitum-currency-key-v0.0.1",
            "weight": 100,
            "key": "2Aopgs1nSzNCWLvQx5fkBJCi2uxjYBfN8TqneqFd9DzGcmpu"
          }
        ],
```


[4] The operations include generation of an account, transfer of a token, update of a key, registration of a cryptocurrency, update of a cryptocurrency policy to name a few.

```
            "threshold": 100
        },
        "amounts": [
            {
                "_hint": "mitum-currency-amount-v0.0.1",
                "amount": "333",
                "currency": "MCC"
            }
        ]
    }
  ]
}
```


[Figure 4] (Ex.) The Structure of an Account Generation Operation Fact

[Fig. 4] Represents the operation of an account generation, one of the major examples for hash. The fact consists of "_hint", which explains its contents; "hash", the hash value of the fact defined as a Fact Hash; "token", which ensures the uniqueness of the fact; "sender", the address of the account that generated the fact; and "item" indicating the contents of the operation.

Element	Description
hint	Explains the contents of a fact
hash	Hash value of the fact defined by a Fact Hash
token	Value intended to endure the uniqueness of the fact
sender	Address of the account that generated the fact
item	Contents of the operation

[Figure 5] (Ex.) Elements Constituting an Account Generation Operation Fact

As described above, the figure shows that as the fact does not contain information relating to a digital signature, anyone can reconstitute the fact and calculate a Fact Hash as long as one recognizes the contents and token value of the operation.

3.2 Fact Hash

A Fact Hash refers to the hash value of the fact.

Here, a value called 'token' is utilized as an element of the fact that guarantees the uniqueness of fact. A token is used as an element that renders fact more unique, and it can be implemented as a random number.

In Mitum blockchain, the timestamp captured at the moment when an operation is performed, and thereby a fact gets to be generated is utilized as a token. This satisfies the requirement applicable to a token that it must ensure uniqueness.

3.3 Benefits of Fact Hash

Fact Hash does not simply mean a hash value for a datum. In the Mitum blockchain, Fact Hash possesses the following important attributes.

First, Fact Hash has a unique value in a blockchain. Each operation has a unique Fact Hash value which can be also utilized as a key identifying an operation.

In other words, thanks to its uniqueness, a Fact Hash can be used as a search key to track and confirm whether a certain operation has been completely processed or whether the transaction has been stored in a block.

Second, such uniqueness can prevent duplicating the transactions. A Fact Hash is calculated and recorded in a fact whenever an operation is performed. The fact generated in such a way is then stored in a blockchain.

Let's suppose that a duplicated processing request has been made for an operation which has already been processed[5]. In Mitum, whenever a fact is processed, it is inquired whether the identical Fact Hash is presented in the blockchain; when a Fact Hash of the same value is found, it categorizes the fact as 'processed' and rejects the request in order to prevent duplicate processing.

Third, Fact Hashes can be calculated even through off-chain, which enables verification of a specific operation. To put it differently, even if a node does not belong to a blockchain, a Fact Hash can be easily calculated as long as the information on the specific operation (sender, receiver, currency ID, amount) and token associated with the operation are recognized.

This feature is useful in implementing a cross-chain bridge between heterogeneous blockchains. For example, when a cross-chain bridge linking Ethereum and Protocon blockchains is to be implemented, operations can be verified simply by configuring a binary tree of operations related to the bridge action. Also one can verify certain operations by calculating those Fact Hashes.

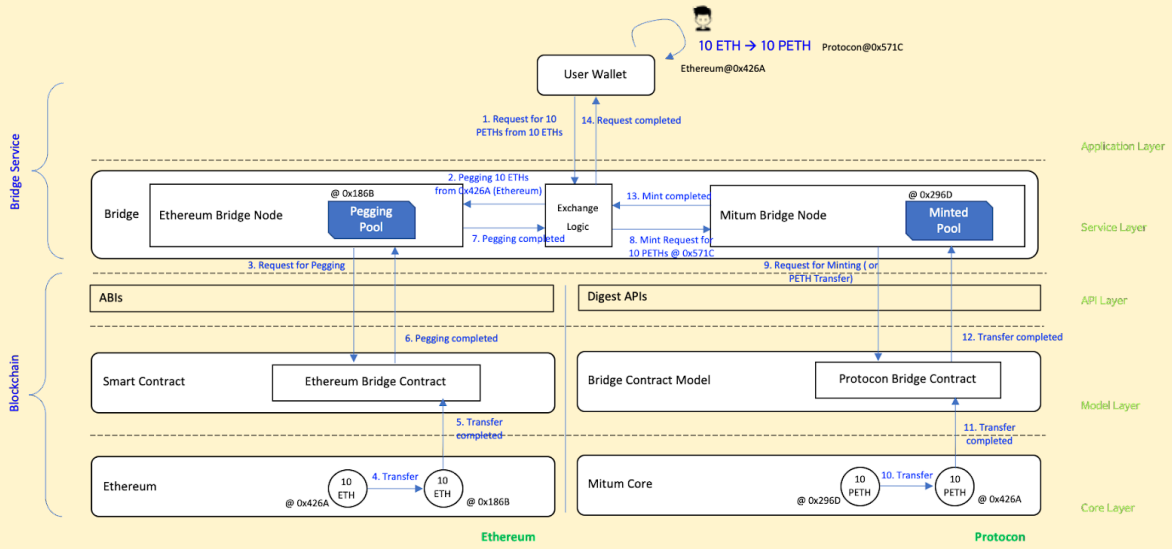
[5] Due to the loss of Acknowledge packets on the network, it may be determined that the request has not been processed and re-requested. In this case, the request receiving side may have already processed the request, but the requesting side may determine that it has not been processed and request it again.

4. Fact Hash & Cross-chain Bridge

Section 4 explains how a general cross-chain bridge is structured and how it operates. It also describes how Fact Hashes can be utilized in terms of implementing a cross-chain bridge to interconnect Protocon network with heterogeneous blockchains.

4.1 Cross-chain Bridge

A cross-chain bridge-utilized for interoperations between heterogeneous blockchains-basically operates in a process through minting a token with the same identical value which has been pegged to another blockchain from an interconnected blockchain[6].



[Figure 6] Basic Operation of Protocon Cross-chain Bridge
(e.g. Ethereum-Protocon Bridge)

The figure above illustrates the Protocon cross-chain bridge operation. It describes a process in which a user pegging 10ETH under one's possession to the bridge service of the Ethereum blockchain and obtaining PETH which is Wrapped ETH with the identical value in the Protocon blockchain.

The user remits 10ETH to the bridge service and requests 10PETH to be generated in the Protocon blockchain. At the time, 10ETH gets transferred to the Ethereum bridge service node.[7]

---

[6] The token having the identical value to the pegged token is called 'Wrapped Token'.For instance, tokens conceived under this concept are Wrapped BTC, Wrapped ETH, etc.
[7] In general, it is remitted to the account address of the bridge smart contract, and this is referred to as 'pegging'. Herein, a smart contract account is generalized as a 'pegging pool'.

The 10ETH which has been transferred is pegged by the ‘Ethereum Bridge Contract’-a smart contract in Ethereum-and the pegged information is transferred to the Mitum bridge node via ‘Exchange Logic’ of the bridge service.

Then, the Mitum bridge node mints 10PTH via ‘Protocon Bridge Contract’ as much as the amount pegged in Ethereum, and remits it to the wallet address of the user who made the request.

4.2 Cross-chain Bridge Issue

Interconnecting heterogeneous blockchains accompanies the issue of ‘trust’-the bridge service linking two blockchains in an off-chain format must be credible.

As each blockchain has a respective independent consensus mechanism, it is essential to interconnect two different blockchains off-chains. Subsequently, data exchanged off-chain may be exposed to potential falsification risks with or without intention; hence transparency and verifiability of each blockchain transaction need to be secured to ensure the reliability of the bridge service.

To ensure transparency, a tool may be utilized to allow all users to easily view transaction processing steps at a moment of their choice. For instance, as shown in Figure 7 below, tokens being pegged/unpegged by a bridge can be readily confirmed by a blockchain explorer.

FACT HASH	CONFIRMED AT	BLOCK HEIGHT
32ds7KXj7dRYumaVBPJ9tG24U3MUt4g5q7trBABkADoX	2022-03-22, 15:20:07.328	224932
5enBkWRYE4TqVhZtMmx7TMELJcD3xYRNLtmS4Ud92933	2022-03-22, 15:20:07.328	224932
ExF9xUvNScSQ9iZ8Ju8CeMKZvDx2Vo8YjBYJ7LuPzJMG	2022-03-22, 15:20:07.328	224932
Arc322wWGG5octZL9G5r9YCwEX41soeCZs61HH7AgRwL	2022-03-22, 15:20:07.328	224932
5U7vRD58a3TYuPscoaviQwYjXbRPBLfYw1CQPXrarCSq	2022-03-22, 15:19:07.772	224904
5yXb8wgn9UdyzLcK1ECrvtacwajjHxyzv8d6W1RGwWTq	2022-03-22, 15:19:07.772	224904
S3wiZHL9V26QYoFtR7n9RJoqVGUhgkGUNwD8eySAufk	2022-03-22, 15:19:07.772	224904
1xQTfPnmn2wm6SxK4Mcy4VLErN2vpLboTvbjw7XUQC5	2022-03-22, 15:19:07.772	224904
2fQAwisr7JCPGsNU5MghTJzT5eQcTgt2zFReV13WQDFk	2022-03-22, 15:18:08.574	224876
BrRBedK5Yc3hMNMUWRoKBdZVLpbCnFUNr6eQkwAGg9aS	2022-03-22, 15:18:08.574	224876

[Figure 7] Fact Hash Information Exposed in the Blockchain Explorer of the Protocon Testnet [8]

Verifiability can be also strengthened by securing a large number of 3rd party verification nodes and allowing multiple parties to monitor and verify pegging/unpegging transactions performed via a bridge.

Yet, it is not easy to perform the two aforementioned operations with the conventional blockchain data processing architecture. The hacking incident[9] that recently erupted in the Wormhole network bridging Solana-Ethereum[10] and another incident[11] that happened between Ronin network-Axie Infinity-Ethereum[12] clearly indicate that a fully effective verification method for cross-chain transactions is still nowhere in sight. In those two incidents, assets valued approximately $320M and $650M respectively were stolen.

In particular, the Ronin network was hacked by a 51% attack based on keys obtained from the bridge verification nodes, which has revealed serious drawbacks in securing the integrity of bridges on the basis of off-chain verification nodes.

4.3 Fact Hash-based Solution

As mentioned above, Protocon can inspect the normality of an operation simply by configuring a binary tree of operation Fact Hashes related to bridge operations and calculating Fact Hashes of operations required to be verified.

Let's suppose there's a request for unpegging the ETH which was previously pegged in the Ethereum blockchain; it needs to be confirmed whether the request is falsified or related to a normal operation to be performed in the Protocon blockchain.

The bridge node receiving the unpegging request from the Ethereum blockchain must perform an unpegging procedure after verifying the normality of the request (whether it has been sent by the owner of the applicable token).

Then the Ethereum bridge node can calculate a Fact Hash on its own, not depending on a Protocon node. By inquiring and verifying the binary tree of the Fact Hash calculated above[13], the normality of the unpegging request can be confirmed.

---

[8] https://info.demo.protocon.network/dashboard/protocon
This site is the test version of Protocon blockchain explorer. Connections might be temporarily unavailable due to frequent maintenance.
[9] Hacking incident that broke out in February, 2022 and where 120,000ETH was leaked.
https://extropy-io.medium.com/solanas-wormhole-hack-post-mortem-analysis-3b68b9e88e13
[10] https://solana.com/wormhole
[11] Hacking incident that erupted in March, 2022 and where 173,600ETH and 25,500,000USDC were leaked.
https://www.gmw3.com/2022/04/the-ronin-bridge-hack-recapping-cryptos-largest-hack-ever/
[12] https://bridge.roninchain.com/
[13] Mitum applies a binary tree similar in concept to a Merkle tree.

Furthermore, if a Fact Hash is utilized, when off-chain or side-chain needs to be configured in the Protocon ecosystem for certain reason, reliability may be ensured at a level comparable to the mainnet. As the global game companies started to do research on applying blockchain to their games, there are many attempts to utilize off-chains or side-chains in securing network speed, cutting down costs, and enhancing the convenience of user experience. When the application of blockchain extends much further as described above, a Fact Hash will be used as an important tool for ensuring trust.

5. Conclusion

This yellow paper introduces and defines ‘Fact’ and ‘Fact Hash’, the core tech elements of the Mitum blockchain, and describes their features and benefits.

In response to the recent hacking incidents and token leaks of massive scale that have frequently broken out in cross-chain, the feature on verifying the bridge operation enabled by a Fact Hash can dramatically enhance the reliability of the data-processing process.

It is confirmed that the uniqueness of a Fact Hash could facilitate inquiring operations and prevent duplicate processing. In addition, the paper shows that even on off-chain the Fact Hash can be calculated and the normality of operations can be verified. In particular, it is confirmed that a Fact Hash can be a very useful feature for boosting up reliability of interoperations between heterogeneous blockchains and for significantly enhancing the trustability of off-chain. Furthermore, without the need of splitting up the structural roles of blockchain such as Avalanche, it is expected that a more secure and highly efficient off-chain, side-chain or multi-chain structure can naturally emerge within the protocon network.

Project Info

Homepage : https://protocon.io/

Github : https://github.com/ProtoconNet

Protocon Yellow Paper
Part 1 : Contract Model
https://protocon.io/wp-content/uploads/Protocon-Yellowpaper-Part-1-Contract-Model-ENG.pdf

Contact : contact@protocon.io