Nakacoin: Peer-to-Peer crypto-currency and application based on bitcoin protocol

Nakacoin

(nakacoin@gmail.com, BM-2cUdNA1F9Hnq6GzyyfgBf2AD1WgHqnYhod)

November 28th, 2013

ABSTRACT

There are six years growths of bitcoin since bitcoin has been invented in 2008 by Satoshi Nakamoto. Many alternate coins were also invented after that. We have lots of alternate coins nowadays and the quantities of alternate coins are rising rapidly. We believe that we are living in a crypto-currency period and you can imagine how the wold will be impacted by crypto-currencies. Our goal is structuring a peer-to-peer system that pleople can trade freely themselves and not depend on a third escrow in the future. People can not only trade bitcoins but also alternate coins in the system. We will not add Nakacoin blockchain upon bitcoin or alternate coin blockchain. What we want to do is using a Naka Protocol System (NPS) to map bitcoin and alternate coin blockchain to Nakacoin blockchain (Like an API).

BACKGROUND

Bitcoin has been invented for six years and there are more than 12 million bitcoins being mined out, the total of bitcoins will be mined out in 2140 finally. Bitcoin will lead the revolution of internet. People can double spend their bitcoins hardly due to its transations and timestamp system. But bitcoin consumes large of energe due to its Proof-of-Work (POW) system. However Peercoin (PPC) is a supplement of BTC as PPC use Proof-of-Stake (POS) system. But it is still difficult to buy food or do business via BTC or PPC because the merchants are marked by local fiat currency and business men prefer local currency. If somebody accept BTC, they have to sell BTC on an escrow platform to get local fiat currency, then buy food or do business using local fiat currency. People usually take BTC as gold, and actually it is. BTC is hard to mine and limited the total amounts. People do not use gold to exchange in real life, neither do BTC. Our goal is to establish a bridge between reality (food, clothes, business, etc.) and BTC, we call it Nakacoin, the system is based on NPS. People can create their own alternate coin based on Nakacoin and exchange alternate coin with Nakacoin system.

NAKACOIN TRANSACTION

The NPS is a peer-to-peer protocol which is based on bitcoin protocol. The NPS is efficiently supports distributed realtime control with a very high level of security.

Its domain of application ranges from small to large amounts.

In crypto-currencies, bitcoins, litecoins, peercoins, etc. are based on their unique electronic cash system, most of them are consuming lots of CPU or GPU power. At the same time it is cost effective to build into bitcoins. The intention of this paper is to achieve compatibility between

any two or more crypto-currencies application implementations. Compatibility, however, has different aspects regarding e.g. POW/POS features and the interpretation of coin to be transferred. To achieve design transparency and implementation flexibility NPS has been subdivided into different layers.

THE NPS OBJECT LAYER

- The NPS transfer layer
- The physical layer (bitcoin layer)

The object layer and the transfer layer comprise all services and functions of the coin link layer defined by the bitcoin layer.

The scope of the object layer includes finding which coins are to be transmitted

- Deciding which coins received by the transfer layer are actually to be used.
- Providing an interface to the application layer related bitcoin or alternate coin protocol.

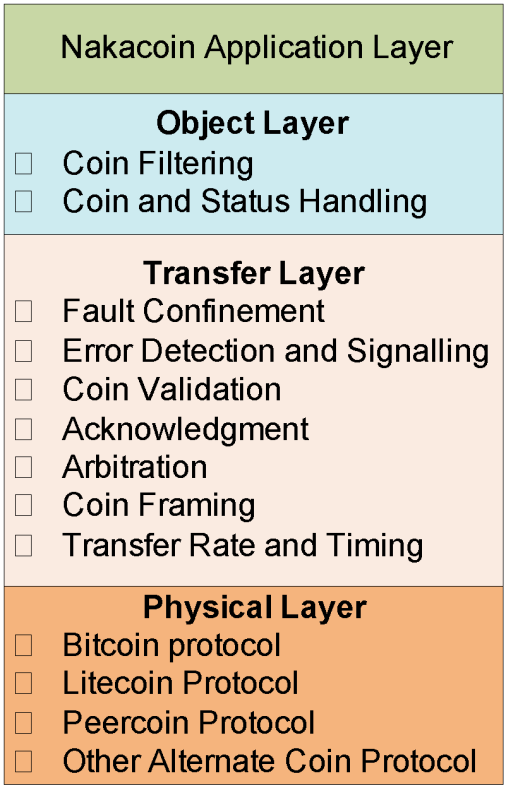
There is much freedom in defining object handling. The scope of the transfer layer mainly is the NPS protocol, i.e. controlling the framing, performing arbitration, error checking, error signalling and fault confinement. Within the transfer layer it is decided whether the node is free for starting a new transmission or whether a reception is just starting. Also some general features of the coins timing are regarded as part of the transfer layer. It is in the nature of the transfer layer that there is no freedom for modifications.

The scope of the physical layer is the actual transfer of the coins between the different nodes with respect to all bitcoin properties. Within one P2P network the physical layer, of course, has to be the same for all nodes. There may be, however, much freedom in selecting a physical layer (bitcoin or alternate coin).

BASIC CONCEPTS

- NPS has the following properties:
- Prioritization of coins (Nakacoin, bitcoin or any other alternate coin)
- Guarantee of latency times
- Configuration flexibility
- Multicast reception with time synchronization
- System wide coins consistency
- Multimaster
- Error detection and signalling
- Automatic retransmission of corrupted coins as soon as the blockchain is ready again
- Autonomous preventing 51% attack.

LAYERED STRUCTURE OF NAKACOIN



- The Physical Layer defines how coins are actually transmitted. Within this specification the physical layer is bitcoin layer.
- The Transfer Layer represents the kernel of the NPS protocol. It presents coins received to the object layer and accepts coins to be transmitted from the object layer. The transfer layer is responsible for coin timing and synchronization, coin framing, arbitration, acknowledgment, error detection and signalling, and fault confinement.
- The Object Layer is concerned with coin filtering as well as status and Coin handling to avoid double spend and 51% attack.

The scope of this paper is to define the transfer layer and the consequences of the NPS protocol on the surrounding layers.

NAKACOINS TRANSACTION

Information on the node is sent in fixed format Nakacoins of different but limited length. NPS will handle how Nakacoins transfer between bitcoins and alternate coins.

INFORMATION ROUTING

In NPS a Nakacoin node does not make use of any information about the system configuration (e.g. public addresses). This has several important consequences.

System Flexibility: Nodes can be added to the NPS without requiring any change in the software

of any node and application layer.

Nakacoin Routing: The content of a Nakacoin is named by an IDENTIFIER. The IDENTIFIER does not indicate the destination of the Nakacoin, but describes the meaning of the Nakacoin (amount, transaction ID, timestamp, etc.) so that all nodes in the network are able to decide by COIN FILTERING whether the coin is to be acted upon by them or not.

Multicast: As a consequence of the concept of COIN FILTERING any number of nodes can receive and simultaneously act upon the same Nakacoin.

Coin Consistency: Within a NPS it is guaranteed that a coin is simultaneously accepted either by all nodes or by no node. Thus coin consistency of a system is achieved by the concepts of and by error handling.

COIN RATE

The speed of Nakacoin may be different in different coins (bitcoins and alternate coins). However, in a given system the coin rate is uniform and fixed.

Priorities

The IDENTIFIER defines a static coin priority during NPS access.

Remote Coin Request

By sending a REMOTE FRAME a node requiring coin may request another node to send the corresponding COIN FRAME. The COIN FRAME and the corresponding REMOTE FRAME are named by the same IDENTIFIER.

Multimaster

Any coins may start to transmit a coin. The coin with the higher priority to be transmitted gains NPS access.

Arbitration

Any alternate coin may start to transmit a coin. If two or more coins start transmitting coins at the same time, the NPS access conflict is resolved by coin wise arbitration using the IDENTIFIER. The mechanism of arbitration guarantees that neither information nor time is lost. If a COIN FRAME and a REMOTE FRAME with the same IDENTIFIER are initiated at the same time, the COIN FRAME prevails over the REMOTE FRAME. During arbitration every transmitter compares the level of the coin transmitted with the level that is monitored on the NPS. If these levels are equal the coin may continue to send. When a ’recessive’ level is sent and a ’dominant’ level is

monitored (see Coin Values), the node has lost arbitration and must withdraw without sending one more coin.

Security

In order to achieve the utmost security of coin transfer, powerful measures for error detection, signalling and self-checking are implemented in every NPS node.

Error Detection

For detecting errors the following measures have been taken:

- Monitoring (transmitters compare the coin levels to be transmitted with the coin levels detected on the NPS)
- Cyclic Redundancy Check
- Coin Stuffing
- Coin Frame Check

Performance of Error Detection

The error detection mechanisms have the following properties:

- All global errors are detected.
- All local errors at transmitters are detected.
- Up to 5 randomly distributed errors in a Nakacoin are detected.
- Burst errors of length less than 15 in a Nakacoin are detected.
- Errors of any odd number in a Nakacoin are detected.

Total residual error probability for undetected corrupted Nakacoin: less than

Nakacoin error rate * 4.7 * 10^{-11}.

Conclusion

After six years growth of bitcoin, we believe that crypto-currency would change the way people live, change the way people exchange. Bitcoin blockchain is stable and large now, the total hash rate are more than 12.5 million GH/s today. It is very secure. We can establish lots of application based on bitcoin blockchain like HTTP basen upon TCP/IP. Nakacoin is one of the solution, it is totally based on bitcoin protocol and alternate coin protocol is the additional feature.

References

Bitcoin blockchain : https://blockchain.info/charts/hash-rate

Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system.

(http://www.bitcoin.org/bitcoin.pdf)