Addressed Raw-data Key

A Method of Building Trustworthy Blockchain by Using Bitcoin Transaction

Paul Baoyong Liu
Paul@bindpay.com
Www.ArkBlockchain.org

1. Introduction

In January 2009, Satoshi Nakamoto mined the first block of bitcoins ever (known as the "genesis block") with the words engraved in it: "The Times 03 / Jan / 2009 Chancellor on brink of second bailout for banks ", which is a title of front page news of the Times that day.

Since then the decentralized Bitcoin has been successful, and the blockchain technology, which is the basis of Bitcoin network is called the God Chain also by its origination and nature, is becoming hot popular. Compared to a centralized system, its data integrity and accuracy are more trustworthy, and its transaction processing is easier, securer and more efficient. Blockchain technology has been widely accepted as the foundation of next-generation Internet value-based Internet. It will reconstruct the modern society and commercial civilization system, will be adopted in a wide range of fields such as finance, Internet of things, medical service, education, commerce and social management.

However, Bitcoin system's block and transaction data structure is relatively simple, it contains necessary information only for the implementation of its cryptocurrency Bitcoin transactions, which is unable to serve a wide range of practical business requirements.

Nowadays, there are many blockchain projects in development aim to establish better functionality featured blockchains to serve as standards or universal frameworks of next-generation internet. A successful block chain system is not only need to be safe, stable, reliable, functional, but also have enough mutual mistrusted nodes to participate, which is a huge challenge.

Instead of developing a new blockchain, extending functionality of Bitcoin blockchain is another choice.

A well-established extension to the Bitcoin system is Sidechain first proposed by Adam Back et al in 2014, which works like fix-exchange mechanism allows Bitcoins move from the Bitcoin system into the new blockchain and can move back if necessary, its core concept is to maintain cryptocurrencies two-way price anchor between the new blockchain and Bitcoin network.

In fact in 2012, earlier than Sidechain concept, JR Willett released the white paper of Mastercoin which known as the Omni Layer later, in which he proposed that existing bitcoin protocol "can be used as a protocol layer, on top of which new currency layers with new rules can be built without changing the foundation.", the digital tokens that the protocol uses to conduct transactions – by sending bitcoins to a special "Exodus Address", it emphasizes loyalty and faith in Bitcoin, only extends protocol and functionality.

Sidechain and Omni Layer is worthy of recognition, however, their purpose is still focusing on maintain a crypto currency.

Is there a way to maintain business logic and data integrity only instead of crypto currency in a side-chain but with perfect value management ability?

This article will propose a method - Addressed Raw-data Key (ARK), which signing and validating external data block by using bitcoin transaction, by this way to keep external data integrity and build up relation between external data and Bitcoin transaction then further to construct another trustworthy blockchain as companion of bitcoin, it will focus on data integrity and business logic management, bitcoin is still the only currency.

2. definition

Main-blockchain - it refers to the Bitcoin blockchain or God Chain;

Transaction - Transaction record in the Main- blockchain;

External Block – external data block independent of Main- blockchain;

ARK - short for Addressed Raw-data Key, transaction address signed, converted from external block.

Ark Block - an external block that established signature validation relationship with Main-blockchain by using ARK;

Ark Chain – a blockchain which blocks contain Ark Blocks, call Ark Blockchain also;

Full Ark Chain – a blockchain that all blocks are Ark Blocks.

3. Ark block construction method

For an designated external data-block independent of main-blockchain, perform the following operations:

(1) Perform hash operation on the data block to generate a number as a private key k;

(2) Generate a public key K according to the ellipse encryption algorithm (K = G * k) of the main blockchain;

(3) Convert and transform the public key into a valid transaction address of the main blockchain (Public Key, P2PKH, P2SH or Data-Output address);

(4) Create a transaction for main blockchain by using address generated above;

(5) Submit the transaction to the main blockchain;

(6) Put the transaction number (ID) into the external block.

Ark blocks may contain any type and complex format data, including transactions, contracts, documents, images, videos and audios, hash script of other data or smart

contract even rules of consensus, while the address generated from external data could be either public key, P2PKH, P2SH or Data-Output.

Ark block construction method shown as below:

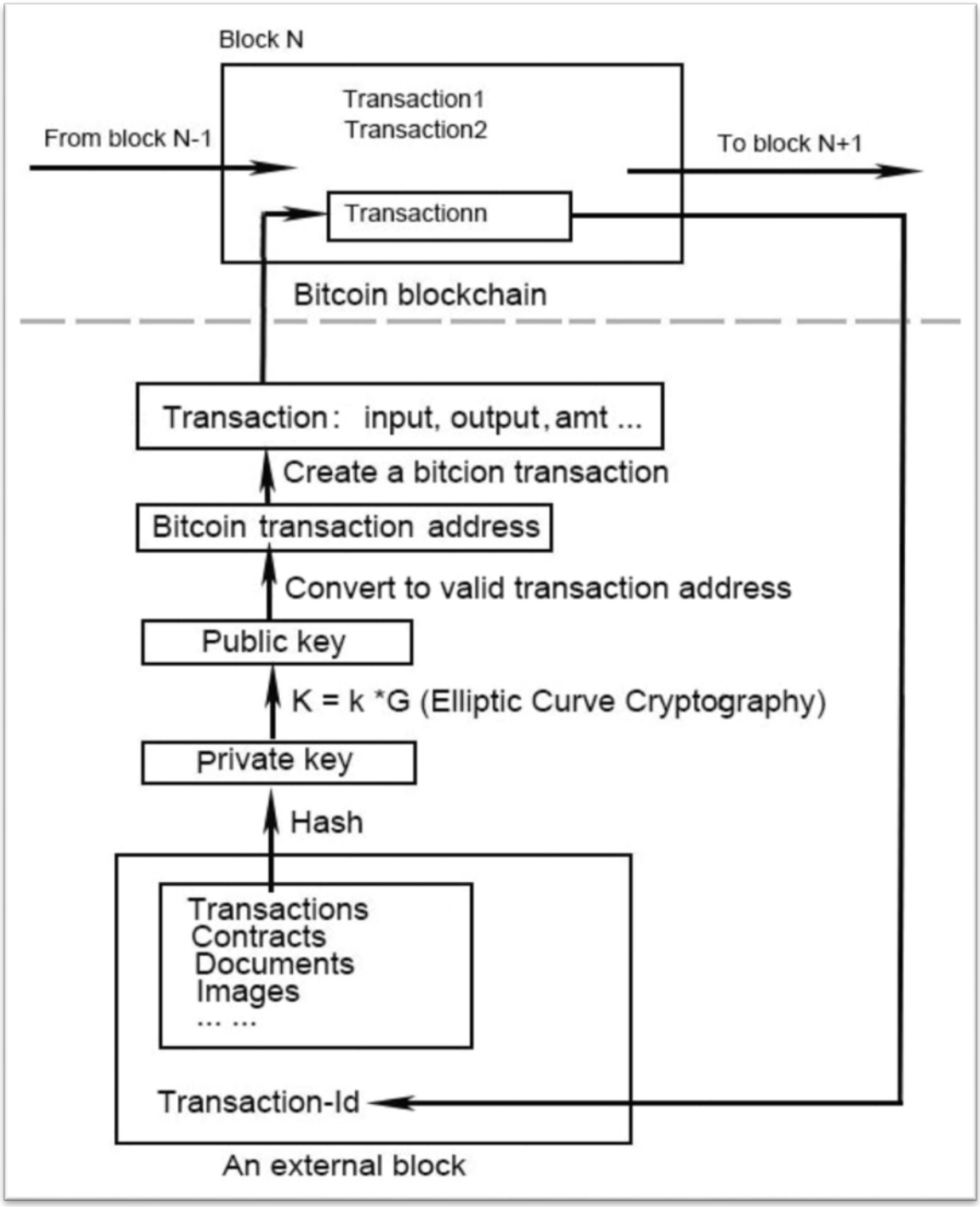

Figure 1. Ark block construction method

Now, the external data block's integrity can be validated by repeating the same process to get the same transaction address, the transaction will exist in the main blockchain forever, and the transaction id is stored along with the external data block so it is convenient to perform the validation.

The external data block became into Ark Block, it can be stored anywhere such as desktops, mobile phones, cloud servers, smart cards, etc., as long as it is accessible when required, it can be independently verified through the Bitcoin system, this makes the fine grind data trustworthy and can be stored in a loose distributed way.

4. Construction method of inherited ARK output

Most likely, an ark block will be used in a blockchain, in order to strengthen the proof of the main blockchain's signature verification relationship, the transaction number (ID) can be taken into parameters along block data, previous block's output, timestamp and nonce if applicable to calculate the block's output according to its consensus mechanism.

See below for Ark block output construction:

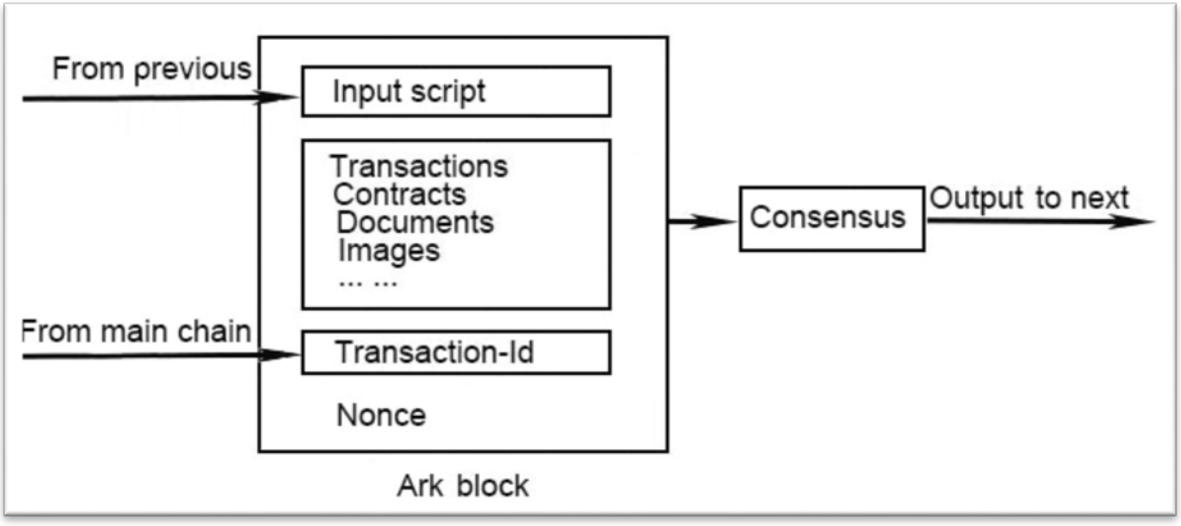

Figure 2. Ark block output construction

Transaction-Id should be the one in segwit format or the transaction gets confirmed in bitcoin blockchain, with transaction-id joined in output calculation, the trustworthy of the ark block will be enhanced.

5. Ark Blockchain Construction Method

If all blocks in a blockchain are ark blocks that is all nodes are validated by main blockchain, then it is full nodes ark blockchain.

More often, an actual application may only partial blocks through the blockchain are ark blocks, only the nodes at key points need to be signed and validated by main blockchain, as shown below:

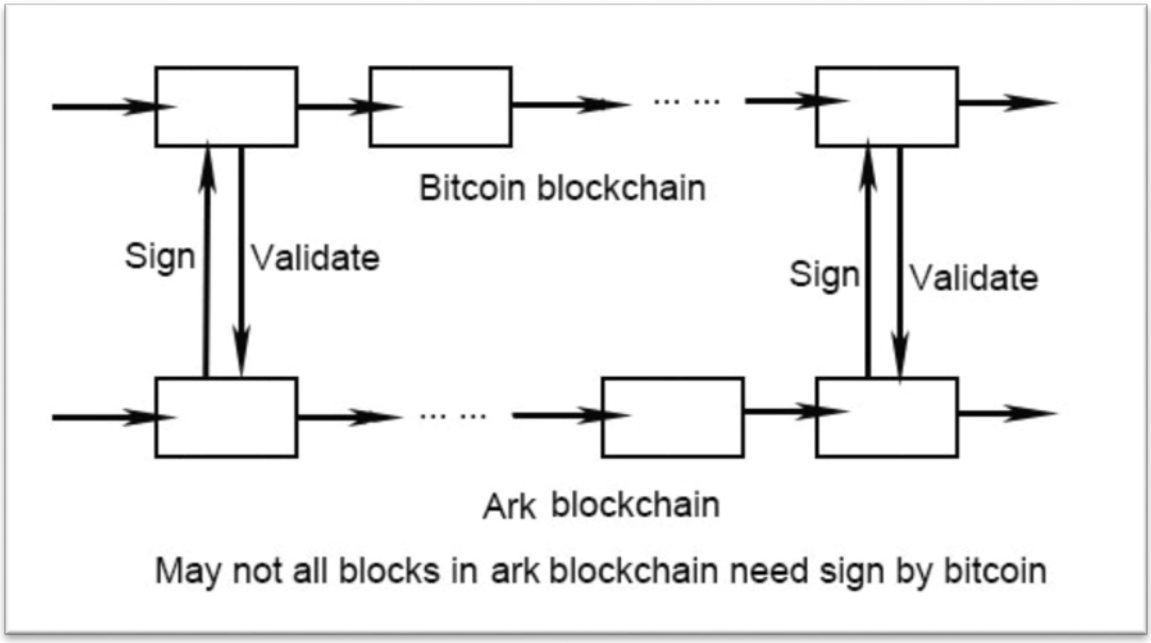

Figure 3. Partial nodes of an ark blockchain are ark blocks

6. Ark Block and Ark Blockchain Application Prospect

Without internal cryptocurrency to maintain, ark block and ark blockchain making data integrity and trust mechanisms diversified, in some cases may only need a single ark block, such as a simple one-time transaction process such as a certificate generation; sometimes may serve as a limited work-flow control to construct a short ark block-chain cross-over a few blocks on the main blockchain, while the most common scenario is to build up an universal ark blockchain, which is infinitely extending along with the main block-chain, for applications such as business finance management, the ark blockchain is still need to maintain a ledger, but just need to bind a bitcoin wallet to the ark blockchain instead of maintain internal cryptocurrency for all users.

7. Conclusion

The ark block and ark blockchain concepts open a door for extending bitcoin blockchain to serve a wide range of business needs, focusing on data integrity, work-flow control instead of crypto-currency management, ark blockchain could be the basis of any application or application framework in the coming value internet era, it enables the dream of building up powerful and trustworthy blockchain for next generation applications such as supply chain, e-commerce, medical service as well as internet-of-thing comes true easily.

Only one blockchain matters, bitcoin is the choice! like Noah's obedience to the will of God, the ark blockchain, by virtue of loyalty to the bitcoin, connects values and assets in real world to bitcoin platform seamlessly by means of integrating data integrity, trustworthiness with business logic as well as workflow management.

Note: This article only introduces the basic concepts of ark blockchain, for detailed information and consensus used in it, please visit www.arkblockchain.org.

As an open source project, ark blockchain will be published github.

Our blow applications will be based on ark blockchain:

Internet of Things payment platform: www.BindPay.com

Customized e-commerce platform: www.diyPlant.com

Contact author: paul@bindpay.com

References：

1. Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto.
2. The Business Blockchain – promise, practice and application of the next internet technology, William Mougayar
3. Omni Layer Specification, https://github.com/OmniLayer/spec
4. Enabling Blockchain Innovations with Pegged Sidechains, Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille∗† 2014-10-22 (commit 5620e43)
5. Blockchain – Blueprint for a new economy, Melanie Swan
6. Mastering Bitcoin, Andreas M. Antonopoulos, O'REILLAY, First Edition, December 2014.