The blockchain banknotes for Currencies

Summary

The ownership blockchain banknotes can offer full decentralization and good scalability for cryptocurrencies.

As we all know, the PoW-based blockchains have serious flaws in terms of scaling. Because the performance is too low and the cost of electricity is too large, they can never become global-scale currencies.

And they are not as well decentralized as stated. PoW tries to get decentralization with voting of computing power. While computing power can be purchased freely. In fact PoW is PoWealth. If someone among the mega-rich wanted to attack Bitcoin, he could do it by simply buying or renting 51% of the computing power.

We remember, the banknote-based currencies work much better. They are efficient, they cost less, and they could not be attacked by the rich. For these reasons, some people have tried to print physical banknotes for Bitcoin.

This is obviously not a good idea. Physical banknotes can not be transferred online and can not be guaranteed to be unique. Instead, we can make banknotes by the ownership blockchains. Each blockchain for one banknote.

The banknotes

An ownership blockchain is private. It has an owner and only the owner can add blocks. Blocks added on a private blockchain do not require a consensus algorithm.

When adding a block, the owner can write in the block: I would give the blockchain to Alice. Then, Alice becomes the new owner of the blockchain. Only she can give the blockchain to another user by adding the next block.

In this way, the ownership blockchain can be passed through the crowd with no need of consensus algorithms. If there are many ownership blockchains, they run separately and do not interfere with each other. The blockchains constitute a highly decentralized and scalable system. There is no disadvantage caused by PoW.

Every ownership blockchain can record the history of its ownership well. It is enough to act as a banknote, because ownership is the only variable for a working banknote.

Like a physical banknote, every Ownership Blockchain Banknote(OBB) has a fixed denomination, which never changes in payments. The payer selects some OBBs from his, makes up the amount to be paid, transfers the selected OBBs to the payee, and the payment is completed.

Security

An ownership blockchain could be forked if the current owner adds multiple blocks at the same location. This is clearly a violation. We have three methods to deal with it.

1. To punish the offender. Users should make sure every block has been broadcast, whatever he is the payer or payee. Once we see multiple conflict blocks are broadcast, we should block the offender at once. Although there is no real account and we can not punish the real people, we may set a rule for every new account to destroy some OBBs before activation. Once the account is blocked, the offender will suffer losses to build a new account.
2. To choose the branch that broadcasts first. For the multiple conflict blocks, we determine that the first broadcast block is valid. If the blocks were broadcast in such a short time that users in the network do not get the same order, all the payees of the conflict blocks may notice the violation soon and reject the payment at once. Double spending will never succeed. We must stay online to record the broadcast order. Otherwise, we can reject the forked OBBs for all branches. With a very small probability of network problems, honest users may get different orders, then they may reject the forked OBB from each other and pay with other OBBs.
3. To merge forked OBBs. When the branches of one OBB are transferred to the same user, the user can add one block on all branches to merge it. As a reward, the merge block offers its maker the right to build a new OBB with random denomination. So we can guarantee the number of forked OBBs is limited.

Methods 1 and 2 guarantee that there is no benefit but loss in forking an OBB. Method 3 guarantees even if someone would attack with significant losses, he can not harm the system.

We never make decisions through any forms of voting to avoid Sybil Attacks. All decisions are based on reliable evidence and not on the free will of people.

We can guarantee each OBB to be unique by setting the Id to a signature of the inherent information.

Grouping

For security reasons, we have to broadcast every block immediately. It may cause performance problems when the network grows large. We may solve it by grouping.

Randomly divide the OBBs into multiple groups. Each user may join some groups and try to use the OBBs in the groups first. New blocks are broadcast only to the users in the group of the OBB. If two users have frequent transactions, they should join the same group and pay by the banknotes in the common group for security and performance.

For Bitcoin

The OBBs can be used for any currency. The central banks can make OBBs for CBDCs. Everyone can make OBBs for independent decentralized cryptocurrencies. Also it can be used for existing cryptocurrencies, such as Bitcoin.

Assuming Alice has 1 BTC, she can make an OBB with a denomination no more than 1 BTC by the steps below.

1. Create an ownership blockchain, write the denomination and her public key as constant information into the root block. Sign the constant information and get the signature as the ID of the ownership blockchain.
2. Transfer enough BTC in the Bitcoin network to the OBB's ID as the destination wallet address. Record the UTXO. Since the ID is not a valid wallet address, this portion of BTC will be frozen.
3. After the transaction is confirmed by the Bitcoin blockchain, add the second block with the UTXO written in it to the ownership blockchain.

Now Alice can transfer the blockchain as a Bitcoin banknote to others. We can trust there is enough BTC not less than the denomination in the banknote by confirming the UTXO.

The banknote-based Bitcoin also offers good scalability and perfect decentralization. The only risk is a possible 51% attack on the Bitcoin blockchain before the block added in step 2.

To return the BTC to the Bitcoin blockchain requires some new features of Bitcoin. Assuming Bob gets the OBB made by Alice, he can return the BTC to the Bitcoin blockchain by the steps below.

1. Add a destroy block to the OBB and broadcast, write his own wallet address of Bitcoin into the block. The destroyed OBB can not be transferred any more.
2. Create a transaction in the Bitcoin network to take out the BTC from the OBB, the source wallet address should be the same as the address written in the destroy block.
3. The BitCoin miners should always watch the OBB network. If a miner trusts the destroyed block is valid, he may insert the transaction and the whole ownership blockchain to the next Bitcoin block. This is the new feature needed for Bitcoin.

Exchange

An ownership blockchain is object oriented. It can be a banknote when describing a certain amount of money. And It can also describe other things.

For the ownership blockchains describing different kinds of objects, they can share the same network. We can easily exchange several ownership blockchains for several others. The two sides of the exchange could be different currencies. Or if they are currencies and goods, then the exchange means a purchase.

So, ownership of everything can be recorded. All disputes over ownership can be terminated. I think that is the future.