

WHAT IS CLAIMED IS:

1. A method of enabling one or more entities of a blockchain system to carry out a series of operations, wherein the blockchain system comprises
 - a main chain,
 - a co-chain, wherein the co-chain has a corresponding account on the main chain,
 - an asset owned by the corresponding account on the main chain and owned by an account on the co-chain, ~~and~~
 - a wherein the co-chain account ~~possessing-possesses~~ the asset,
 - the operations comprising:
 - posting an authenticated transaction on the co-chain, the authenticated transaction authorizing a transfer of the asset from the co-chain account to the main chain;
 - authenticating, by validators of the co-chain, a data string specifying the asset to be transferred and a destination public key;
 - delivering the authenticated data string to the account of the main chain corresponding to the co-chain; and
 - posting, on the main chain, a transaction transferring the asset to the destination public key from the account of the main chain corresponding to the co-chain.
2. The method of claim 1, the operations comprising generating the public key.
3. The method of claim 1, wherein the validators authenticate the data string using a digital signature of a threshold signature scheme.
4. The method of claim 3, wherein the digital signature is generated relative to a public key that is associated with the account in the main chain, wherein a corresponding secret key is collectively held by the validators of the co-chain.
5. The method of claim 1, wherein the account of the main chain corresponding to the co-chain is controlled by an entity that controls ~~an~~ the account on the co-chain.
6. A method of enabling one or more entities of a blockchain system to carry out a series of operations, wherein the blockchain system comprises

a main chain,
a co-chain, wherein the co-chain has a corresponding account on the main chain,
an asset owned by the corresponding account on the main chain and owned by an account on the co-chain, ~~and~~

~~a wherein the~~ co-chain account ~~possessing~~ possesses the asset,
the operations comprising:
posting an authenticated transaction on the co-chain, the authenticated transaction authorizing a transfer of the asset from the co-chain account to ~~an~~ the account of the main chain;
determining that the authenticated transaction is posted on the co-chain; and
posting, on the main chain, a transaction assigning the asset to the account of the main chain.

7. The method of claim 6, the operations comprising generating ~~the~~ a public key.

8. The method of claim 6, wherein ~~the~~ validators authenticate a ~~the~~ data string using a digital signature of a threshold signature scheme.

9. The method of claim 8, wherein the digital signature is generated relative to a public key that is associated with the account of the main chain, wherein a corresponding secret key is collectively held by the validators of the co-chain.

10. The method of claim 6, wherein the account of the main chain corresponding to the co-chain is controlled by an entity that controls ~~an~~ the account on the co-chain.

11. A method of enabling one or more entities of a blockchain system to carry out a series of operations, wherein the blockchain system comprises

a main chain,
a co-chain, wherein the co-chain has a corresponding account on the main chain,
an asset owned by the corresponding account on the main chain and owned by an account on the co-chain, ~~and~~

~~a wherein the~~ co-chain account ~~possessing~~ possesses the asset,
the operations comprising:

posting an authenticated transaction on the co-chain, the authenticated transaction authorizing a transfer of the asset from the co-chain account to an account of the main chain; producing, by validators of the co-chain, partial signatures usable to compute a digital signature based on a destination public key, the digital signature usable to authenticate the transfer of the asset to the account of the main chain; and posting the digital signature on the main chain.

12. A system comprising:

one or more computer processors; and

one or more non-transitory storage media storing instructions which, when executed by

the one or more computer processors, cause performance of a methods recited in any one of claims 1-11.

13. One or more non-transitory storage media storing instructions which, when executed by one or more computing devices, cause performance of a methods recited in any one of claims 1-11.