WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a recipient node computer, a digital asset comprising a sender identifier associated with a sender, a recipient identifier associated with a recipient, a first digital signature created by an issuer node computer based on the digital asset and a first private key associated with the issuer node computer, and a second digital signature created by an administrative node computer based on the digital asset and a second private key associated with the administrative node computer;

verifying, by the recipient node computer, an authenticity of the digital asset by:

verifying the first digital signature using a first public key corresponding to the first private key; and

verifying the second digital signature using a second public key corresponding to the second private key; and

forwarding, by the recipient node computer, the digital asset to a recipient institution computer associated with the recipient.

2. The method of claim 1, wherein the recipient institution computer stores the digital asset in association with an account of the recipient.

3. The method of claim 1, wherein the digital asset indicates a transfer of a value from the sender to the recipient.

4. The method of claim 3, wherein the value is a currency value.

5. The method of claim 3, further comprising:

recording, by the recipient node computer, the digital asset in a ledger.

6. The method of claim 5, wherein the ledger is a blockchain ledger.

7. The method of claim 1, wherein the administrative node computer validated the digital asset and verified the first digital signature with the first private key before creating the second digital signature.

8. The method of claim 1, wherein the administrative node computer validated the digital asset, verified the first digital signature with the first public key associated with the issuer node computer and corresponding to the first private key, and generated the second digital signature after validating the digital asset and verifying the first digital signature.

9. The method of claim 1, wherein the recipient node computer has a filtered view a full ledger maintained by the administrative node computer.

10. The method of claim 9, wherein the administrative node computer generates a block for a blockchain stored by the administrative node computer, the block including information about the digital asset, and wherein, after generating the block, the administrative node computer coordinates a settlement based on the digital asset, the settlement comprising debiting a value from a sending institution account and crediting the value to a recipient institution account, and wherein recipient institution computer immediately credits a second account of the recipient with the value indicated in the digital asset even if the value has not actually been received.

11. A recipient node computer comprising:

a processor; and

a computer readable medium, the computer readable medium comprising code executable by the processor to implement a method comprising:

receiving a digital asset comprising a sender identifier associated with a sender, a recipient identifier associated with a recipient, a first digital signature created by an issuer node computer based on the digital asset and a first private key associated with the issuer node computer, and a second digital signature created by an administrative node computer based on the digital asset and a second private key associated with the administrative node computer;

verifying an authenticity of the digital asset by verifying the first digital signature using a first public key corresponding to the first private key and further by verifying the second digital signature using a second public key corresponding to the second private key; and

forwarding the digital asset to a recipient institution computer associated with the recipient.

12. The recipient node computer of claim 11, wherein the digital asset and the first digital signature are received from the issuer node computer.

13. The recipient node computer of claim 11, wherein the digital asset and the second digital signature are received from the administrative node computer.

14. The recipient node computer of claim 11, wherein the digital asset further comprises a currency type, a timestamp, and a value.

15. The recipient node computer of claim 14, wherein the administrative node computer coordinates an interaction based on the digital asset.

16. The recipient node computer of claim 14, wherein the recipient node computer is operated by a financial institution.

17. The recipient node computer of claim 14, wherein the method further comprises looking up the first public key based upon the sender identifier.

18. The recipient node computer of claim 17, further comprising:
updating a blockchain with the digital asset including generating a block for the blockchain, the block including the digital asset, the first digital signature, and the second digital signature.

19. The recipient node computer of claim 11, wherein the issuer node computer generated the first digital signature by digitally signing at least some information of the digital asset with the first private key, the administrative node computer generated the second digital signature by digitally signing at least some information of the digital asset with the second private key, and wherein the first digital signature and the second digital signature are both generated by digitally signing the same digital asset but with different private keys.

20. A system comprising:

the recipient node computer of claim 11;

the administrative node computer; and
the issuer node computer.