CLAIMS:

1. A computer-implemented method for enabling secure escrow and safekeeping of a cryptocurrency, the computer-implemented method comprising the steps of:

establishing a secure communication between a first party device associated with a depositor of the cryptocurrency and a second party device associated with a secure cryptocurrency depository, in a cryptocurrency network;

creating and signing a deposit transaction by the first party device transferring all available funds/tokens or part thereof to a multi-signature address;

creating a provisional transaction template by the first party device spending either all of the funds/tokens or a part thereof, sent to the multi-signature address in the deposit transaction;

transmitting an unsigned copy of the provisional transaction template to the second party device;

adding a signature generated using a first party private key and a signature generated by a first party hardware token by the first party device to the provisional transaction template, thereby generating a first partially signed provisional transaction template and transmitting the first partially signed provisional transaction template to the second party device;

adding a signature generated using a second party private key corresponding to the first party private key, by the second party device to the provisional transaction template, thereby generating a second partially signed provisional transaction template and sending the second partially signed provisional transaction template to the first party device;

broadcasting the deposit transaction by the first party device after the first party device and the second party device exchange the first partially signed provisional transaction template and the second partially signed provisional transaction template;

facilitating the provisional transaction by the first party device by adding the signature generated using the first party private key and the signature generated by the first party hardware token to the second partially signed provisional transaction template in possession, forming a fully signed provisional transaction template;

facilitating the provisional transaction by the second party device by adding the signature generated using the second party private key to the first partially signed provisional transaction template in possession, forming the fully signed provisional transaction template, thereby presenting an alternate way;

broadcasting a fully signed provisional transaction template by the first party device and/or the second party device to the cryptocurrency network, when necessary;

wherein the first party device and/or the second party device is enabled to transfer the available funds/tokens away from the multi-signature address using the second partially signed provisional transaction template and/or the first partially signed provisional transaction template in possession of the first party device and second party device respectively, in case the first party and/or second party private-keys/secrets and/or the hardware tokens are lost/stolen, thereby preventing theft.

2. The computer-implemented method as claimed in claim 1, wherein the secure cryptocurrency depository associated with the second party device is a secure cryptocurrency escrow and/or a secure cryptocurrency vault.
3. The computer-implemented method as claimed in claim 1, further comprising the step of creating the provisional transaction template by the second party device in case a transaction ID and a corresponding transaction output index of the deposit transaction is transmitted to the second party device by the first party device.
4. The computer-implemented method as claimed in claim 1, wherein signing the deposit transaction and the provisional transaction template prevents the corresponding inputs and outputs of the deposit transaction and the provisional transaction template from modification once the signature generated using the respective private keys/secrets and/or signatures generated by respective hardware tokens are added to the deposit transaction and the provisional transaction template.
5. The computer-implemented method as claimed in claim 1, wherein the first party device and the second party device are computing devices selected from a group comprising a server, a microcontroller, a laptop, a desktop and a portable handheld device having computing capabilities and comprising at least a processor, a memory unit, a display module, an input module and a user interface.
6. The computer-implemented method as claimed in claim 1, further comprising the step of monitoring the transactions on the cryptocurrency network by the first party device, the second party device and/or a third-party device on behalf of the first and/or second party device.
7. The computer-implemented method as claimed in claim 1, further comprising the step of enforcing a settlement albeit with a predefined delay and does not require exclusive custody of the funds/tokens beforehand to guarantee settlement.

8. The computer-implemented method as claimed in claim 1, further comprising the step of taking exclusive custody of the respective funds/tokens to enforce the settlement, in case of disagreement between a first party device and a fourth party device during a trade/transaction, thereby functioning as a regular custodial escrow.
9. A computer system for enabling secure escrow and safekeeping of a cryptocurrency, the computer system comprising:

a memory unit configured to store machine-readable instructions; and

a processor operably connected with the memory unit, the processor obtaining the machine-readable instructions from the memory unit, and being configured by the machine-readable instructions to:

establish a secure communication between a first party device associated with a depositor of the cryptocurrency and a second party device associated with a secure cryptocurrency depository, in a cryptocurrency network;

create and sign a deposit transaction on the first party device transferring all available funds/tokens or part thereof to a multi-signature address;

create a provisional transaction template on the first party device spending either all of the funds/tokens or a part thereof, sent to the multi-signature address in the deposit transaction;

transmit an unsigned copy of the provisional transaction template to the second party device;

generate a first partially signed provisional transaction template by adding a signature generated using a first party private key and a signature generated by a first party hardware token on the first party device to the provisional transaction template and transmit the first partially signed provisional transaction template to the second party device;

generate a second partially signed provisional transaction template by adding a signature generated using a second party private key corresponding to the first party private key, on the second party device to the provisional transaction template and transmit the second partially signed provisional transaction template to the first party device;

broadcast the deposit transaction from the first party device after the first party device and the second party device exchange the first partially signed provisional transaction template and the second partially signed provisional transaction template respectively;

facilitate the provisional transaction by the first party device by adding the signature generated using the first party private key and the signature generated by the first party

hardware token to the second partially signed provisional transaction template in possession of the first party device, forming a fully signed provisional transaction template;

facilitate the provisional transaction by the second party device by adding the signature generated using the second party private key to the first partially signed provisional transaction template in possession of the second party device, forming the fully signed provisional transaction template, thereby presenting an alternate way;

broadcast a fully signed provisional transaction template by the first party device and/or the second party device to the cryptocurrency network, when necessary;

wherein the first party device and/or the second party device is enabled to transfer the available funds/tokens away from the multi-signature address using the second partially signed provisional transaction template and/or the first partially signed provisional transaction template in possession of the first party device and second party device respectively, in case the first party and/or second party private-keys/secrets and/or the hardware tokens are lost/stolen, thereby preventing theft.

10. The computer system as claimed in claim 9, wherein the secure cryptocurrency depository associated with the second party device is a secure cryptocurrency escrow and/or a secure cryptocurrency vault.
11. The computer system as claimed in claim 9, wherein the processor is further configured to create the provisional transaction template by the second party device in case a transaction ID and a corresponding transaction output index of the deposit transaction is transmitted to the second party device by the first party device.
12. The computer system as claimed in claim 9, wherein the processor is further configured to prevent the corresponding inputs and outputs of the deposit transaction and the provisional transaction template from modification once the signatures generated using the respective private keys/secrets and/or signatures generated by respective hardware tokens are added to the provisional transaction template.
13. The computer system as claimed in claim 9, wherein the first party device and the second party device are computing devices selected from a group comprising a server, a microcontroller, a laptop, a desktop and a portable handheld device having computing capabilities and comprising at least a processor, a memory unit, a display module, an input module and a user interface.
14. The computer system as claimed in claim 9, wherein the processor is further configured to monitor the transactions on the cryptocurrency network by the first party device, the second

party device and/or a third-party device on behalf of the first party device and/or second party device.

15. The computer system as claimed in claim 9, wherein the processor further configures the second party device to enforce a settlement albeit with a predefined delay and does not require exclusive custody of the funds/tokens beforehand to guarantee settlement.
16. The computer system as claimed in claim 9, wherein the processor further configures the second party device to take exclusive custody of the respective funds/tokens to enforce the settlement, in case of disagreement between a first party device and a fourth party device during a trade/transaction, thereby functioning as a regular custodial escrow.