CLAIMS

1. A computer-implemented method of performing a computation, the method comprising, by target computer equipment of a target party, being the computer equipment which is to perform the computation:

obtaining a cryptographic key derived from a response generated by PUF module comprising a physically unclonable function, PUF, the response having been generated by the PUF module based on the PUF in response to a corresponding challenge input to the PUF module, wherein key information comprising the cryptographic key or a corresponding public key is also made available to a verifying party;

from an issuing party, receiving a computation request specifying the computation to be performed;

in response to the computation request, performing the computation in order to generate a computation result;

signing a message comprising the computation result with the cryptographic key; and

making the signed message available to the verifying party by sending the signed message to be recorded on a blockchain.

2. The method of claim 1, wherein the issuing party is the verifying party.

3. The method of claim 1 or 2, wherein the sending of the signed message comprises:

- the target party formulating a template blockchain transaction comprising the signed message; and

- the target party sending the template transaction to the verifying party, thereby causing the verifying party to verify the signature on the message, and in dependence thereon to complete the template transaction at least by signing with a signature of the verifying party, and forward the completed transaction to be recorded on the blockchain.

4. The method of claim 3, wherein the message comprises at least part of the template transaction.

5. The method of claim 3 or 4, wherein the completed transaction pays the target party for the computation once recorded on the blockchain.

6. The method of any preceding claim, wherein the obtaining of the cryptographic key is performed, and the key information made available to the verifying party, in a set-up phase prior to the target party receiving the computation request.

7. The method of any preceding claim, wherein said obtaining comprises:

receiving the response from the issuing party, verifying party or a trusted third party, the challenge having been input into the PUF module to generate the response by the issuing party, verifying party or trusted third party on behalf of the target party, and generating of the public-private key pair being based on the received response.

8. The method of any of claims 1 to 6, wherein said obtaining comprises:

receiving the public key from the issuing party, verifying party or a trusted third party, the challenge having been input into the PUF by the issuing party, verifying party or trusted third party to generate the response and derive the cryptographic key pair on behalf of the target party.

9. The method of any of claims 1 to 6, wherein said obtaining comprises: the target party performing the inputting of the challenge to the PUF module to generate the response and derive the cryptographic key by the target party.

10. The method of any preceding claim, wherein the making available of the key information to the verifying party comprises: storing the key information linked to an identity of the target party or target computer equipment, in a key information storage medium accessible to the verifying party;

wherein the key information storage medium is implemented in third party server equipment comprising one or more server units at one or more physical sites, wherein the key information storage medium is a blockchain or other peer-to-peer publication medium.

11. The method of any preceding claim, comprising encrypting the computation result so as to require a decryption key to decrypt, wherein the computation result is made available able to the verifying party only in encrypted form, and the decryption key is made available to the verifying party and/or issuing party.

12. The method of claim 11, wherein the encryption comprises encrypting the computation result before signing with the private key.

13. The method of claim 11, wherein the encryption comprises encrypting the message after signing with the private key.

14. The method of any of claims 11 to 13, wherein the decryption key is derived from another response generated by the PUF module, or another PUF module, in response to another challenge input to the PUF module by the target party, verifying party, issuing party or a trusted third party.

15. The method of claim 14, wherein the method comprises the target party inputting said other response to generate the other challenge, and deriving the decryption key.

16. The method of any of claims 11 to 15, comprising the target party making the decryption key available to the verifying party and/or issuing party.

17. The method of any of claims 11 to 16, wherein the making available of the decryption key to the verifying party and/or issuing party comprises: sending the decryption key to the verifying party and/or issuing party.

18. The method of any of claims 11 to 16, wherein the making available of the decryption key to the verifying party and/or issuing party comprises: storing the decryption key in a decryption key storage medium accessible to the verifying and/or issuing party.

19. The method of claim 18, wherein the decryption key storage medium is implemented in third party server equipment comprising one or more server units at one or more physical sites.

20. The method of claim 18, wherein the decryption key storage medium is a blockchain or other peer-to-peer publication medium.

21. The method of any preceding claim, wherein the receiving of the computation request comprises accessing an electronic advertisement medium to retrieve the computation request, wherein the electronic advertisement medium is a blockchain or other peer-to-peer publication medium.

22. The method of any preceding claim, wherein the target computer equipment is one of a plurality of pieces of computer equipment involved in a distributed computing system performing distributed computing, said computation being part of the distributed computing.

23. The method of claim 22, wherein the distributed computing is performed on a pay per computation basis, wherein the target party receives a payment for performing the computation on condition that the verifying party verifies the signature of the target party based on the key information.

24. Computer equipment comprising:

memory comprising one or more memory units; and

processing apparatus comprising one or more processing units, wherein the memory stores code arranged to run on the processing apparatus, the code being configured so as when on the processing apparatus to perform the method of any preceding claim.

25. A computer program embodied on a non-transitory computer-readable medium and configured so as, when run on one or more processors, to perform the method of any of claims 1 to 23.