Under the surroundings of anonymous system and unauthorisated supervision, this section will utilise the mainstream of cryptocurrency named Bitcoin that introducing how the cryptocurrency guarantees its cryptography and security. From the working components to understand the reason of necessary digital signature algorithm ECDSA to evaluate the security and efficiency of ECDSA applied in this scenario.

Efficiency

When a distributed miner needed to valid the right of sending mining, who applies ECDSA to encapsulate the data in the blackchin. Then through network to broadcast transaction for all nodes. This transaction needs to put the significant concern on the cracked message encryption issue, because which is related to currency in the real world. In order to earn more Bitcoin, miners usually rely on high efficiency computation. Therefore, the speed of generation key and spending cost should be considered. The table presents the comparation of public key size between ECDSA, DSA, and RSA. ECDSA only takes 256 bits that resulting in the same security level of DSA and RSA when which size is 1024 bit and 2048 bit respectively. Furthermore, from the table of signing time, ECDSA can product much more signatures than RSA in a second. It means that ECDSA reduces dramatically cost on private key operation as the miners sign the signature.

Security

From the security perspective, According to Goldwasser, Micali, and Rivest, the security of digital signature depends on key size and algorithm [3]. When there are many applications adopt with RSA, the Bitcoin applies algorithm is ECDSA rather than RSA. The reason is that under the same level of security, breaking RSA is easier than ECDSA, because the attacker could utilise brute force method to figure two prime factors in RSA. However, ECDSA needed to solve the elliptic curve discrete logarithm problem, which is rather difficult to calculate from the mathematical way.

Therefore, from the Efficiency and Security aspects concludes that the advantage of ECDSA applied in the Bitcoin. It supports the smaller public key size but the same level security as other digital signature algorithms and faster private key computation.

The advantage of elliptic curves is that it allows a smaller key size for the same level of security which saves on storage and computation costs.

This means that with ECDSA you can get the same level of security as RSA but with smaller keys.