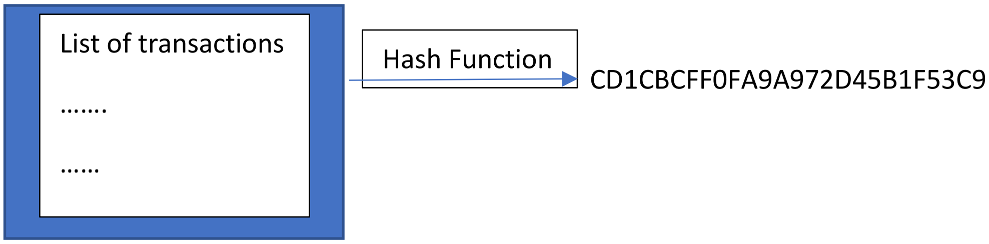
Elliptic Curve Digital Signature within Blockchain

Grant Keller

Blockchain, simply put, is a public leger with highly encrypted transactions. But how do you have a public leger but keep the transactions encrypted? Employing the elliptic curve for encrypted transactions and implementing hashes as the vehicle to publicity. Both the private transactions and the hashing of the blocks relies heavily on linear algebra and math.

The blockchain is a posted leger of transactions. Each "page" of the blockchain is really a block of transaction. Each block of transactions is linked to the next block through a hash. A hash is performed by taking all the data in the previous block and performing mathematical operations until the data is in a new irreversible from. Essentially a hash is not a bijective function that takes the data and sends it down a one-way road to transform it into a different form. This can be likened unto the linear algebra concept of moving between vector spaces a hash function is like a transformation matrix that converts vector X into a new vector B. In linear algebra this process has four possible outcomes, one answer, multiple answers, having no answers or A is not invertible, thus hashing is like the last possibility in that the transformation process cannot be reversed in the first place.

The backbone of modern hashing functions is basic encryption of bits of data. The hash takes the data, converts it to numbers, and performs many rounds of Xor bitwise operations, which is an additive cipher used in many cryptographic projects.



In creating a transaction, one uses the elliptic curve y^2 = x^3 + 7. The curve has special properties such that if one draws a line between any two points on the curve the line will intercept a third point; as long as the original two points are not vertical. This allows for the exchange of public and private keys while only knowing two of the other points. What happens is person A can do elliptic 'addition' with their public and private key to get a new point on the graph. If person B does the same with their points person A and B can trade their respective results, perform one more round of elliptic addition and find the position of the other person without having to vocalize their current whereabouts. An eavesdropper would have been able to gathered the result of each person's addition but wouldn't have enough information to find either of the individuals.