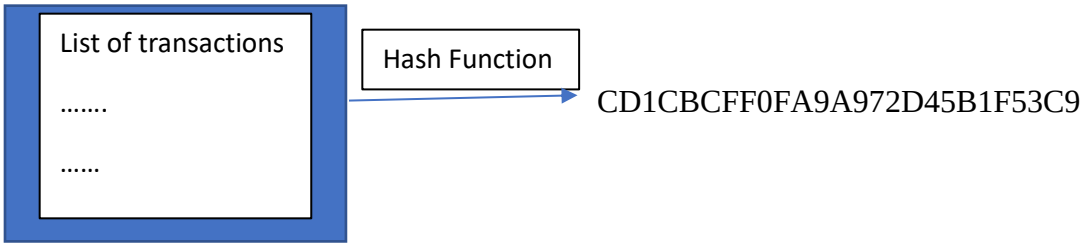
Elliptic Curve Digital Signature within Blockchain

Grant Keller

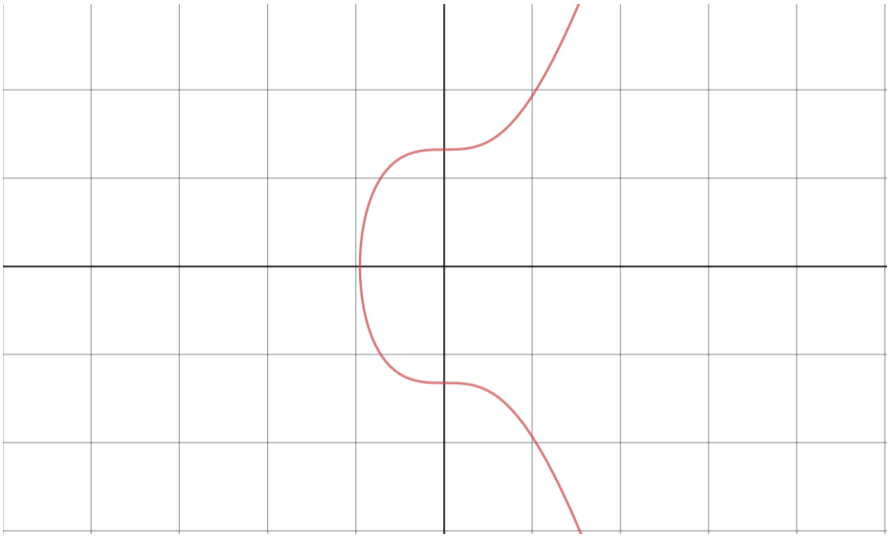
Blockchain is a way to store public transactions, while keeping the information of the users safe and encrypted. But how do you allow for public trading while keeping the transactions encrypted? This is attained by employing a special elliptic curve to encrypt transactions and implementing hashes as the vehicle to publicity.

The blockchain is a public ledger, or record sheet, of transactions. Each block or "page" of the blockchain contains a group of transactions. Each block of transactions is linked to the next block through a hash. A hash is implemented because the blockchain needs to be unchangeable and the hash's properties guarantee this. A hash function is always unique, and therefore a hash never has two outputs that are the same unless the input is the exact same to begin with. Hashes also have mathematical complexity and are irreversible which gives security to the blockchain.

In essence, a hash is a 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. Here, a hash function is like a transformation matrix that converts vector X into a new vector B. In linear algebra the process of solving for X when you have the transformed vector B has four possible outcomes: one answer, multiple answers, having no answers or the transformation process is not invertible. Thus, hashing is like the last possibility in that the transformation process cannot be reversed in the first place. The purpose of modern hash functions is to encrypt data. The hash takes the data, converts it to binary numbers, and performs many rounds of XOR bitwise operations, which is an additive cipher used in many cryptographic projects.



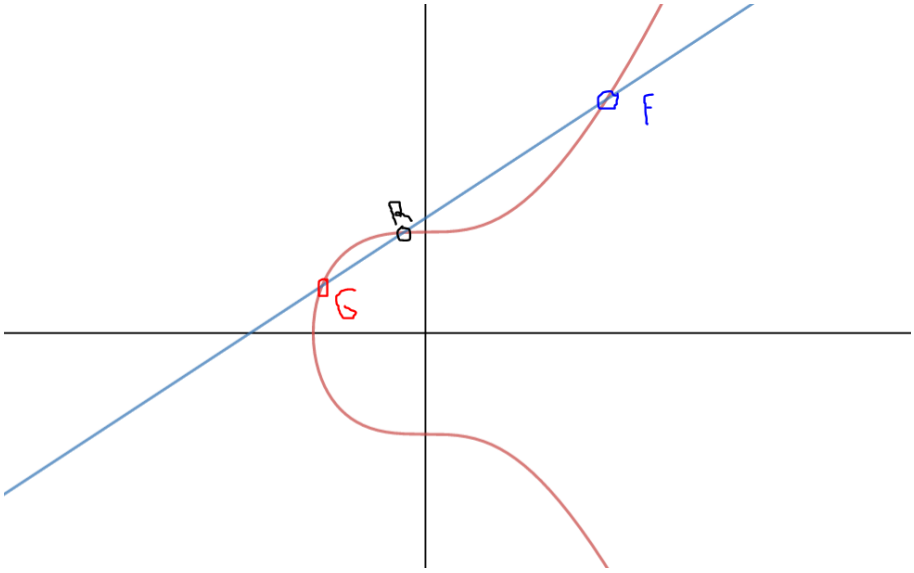
When actually creating transaction in a public fashion where anyone can see the information being shared it is vital that both parties can secure themselves from eavesdroppers or entities wanting to influence the transaction. In creating a public and secure transaction, one uses the elliptic curve y^2 = x^3 + 7. This curve was developed by Diffie Hellman to solve the problem of exchanging information publicly while keeping all parties involved secure and private.



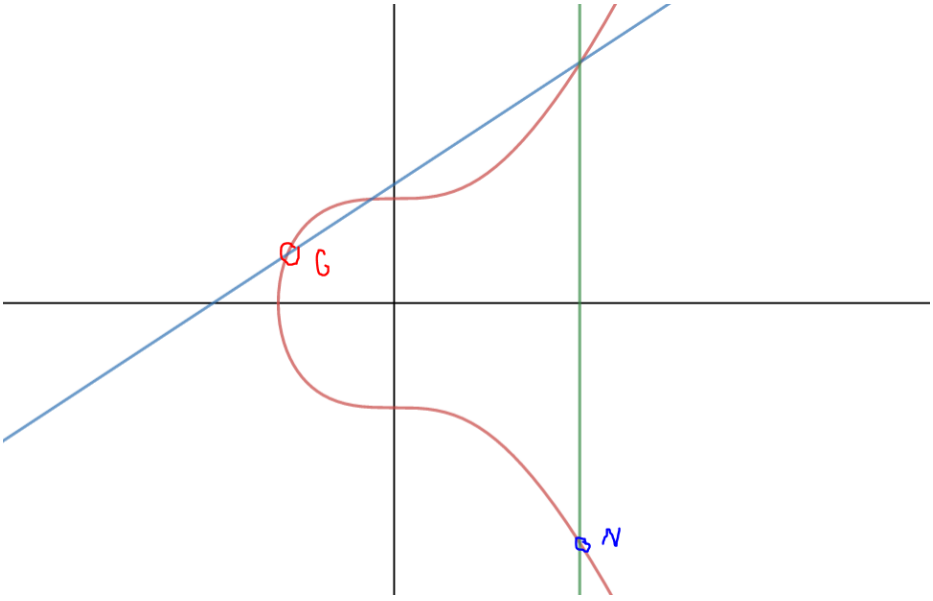
The main idea Diffie Hellman had was that through employing this elliptic curve you can create “rings” or groups of points on the graph that are unique and when each party selects one point to share then a private key can be generated that is unique to the two parties.

When creating a ring of points a few things need to be established. The curve itself, the generator point, and the max value, of which is a value on the X axis that binds the ring. In the image below, it shows elliptic addition to find the first point in the ring. The curve has a special property such that if

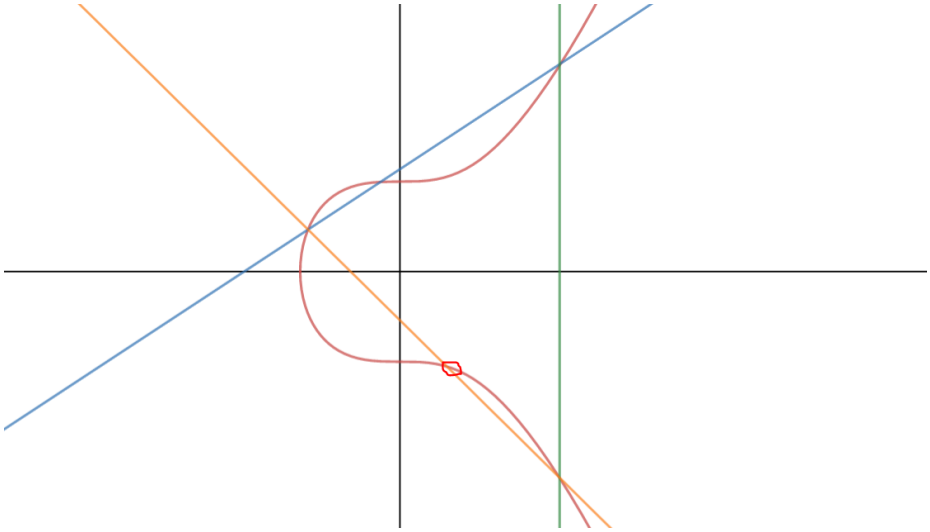
one draws a line between any two points on the curve the line will intercept a third point, as long as the original two points are not vertical. Here, we use the generator point G= (-6,3) our randomly chosen point R= (-1, 7) and our first point in the ring is F =(13, 16).



To continue finding points on the curve we take the point opposite the found point F and find this new point N which is an exact reflection of F.



Now if we draw a line from the generator point to N we are given a new point to add to our ring. And if we reflect that new point across the X axis we are given another new point to add to our ring and so on so forth. Continuing this method eventually produces points outside of the max value. Once that is reached all the points in the ring have been found.



Now that we have our ring we only need to understand elliptic multiplication before we can begin exchanging information.

Elliptic multiplication looks like 5G = (12,7) The way it works is you take the fifth point generated from your ring. Because our ring is bound, what if our set is smaller than the point we try and multiply? We take a modulus of the number being multiplied. Eg: our ring has 12 points on it, and we try and multiply 14. We subtract 14 by 12 to give us 2 and then perform the multiplication.

We are ready to exchange information. If George and Frank want to exchange information without their younger sibling Evan knowing then they use the Diffie Hellman elliptic curve to do it.

George and Frank think of a random number and compute it on the elliptic curve. (C = elliptic curve)

CG = M and CF = N

They trade M and N while Evan watches. All three of them know M and N, and because the elliptic curve was decided on before hand they all know that info too. However, now George computes (CG)N = A and Frank computes (CF)M = A and Evan is stumped because he can't compute A without either G or F. A becomes the secret key that George and Frank use to encrypt their information.

As shown, the Diffie Hellman allows for the exchange of public and private keys while only knowing two of the other points. Thus, the elliptic curve is the backbone of private and secure transactions over the blockchain. Overall blockchain is a complex process that uses many forms of math to ensure that users can make secure transactions that are publicly displayed, unalterable and at the same time accessible.