Initial Setup – Central Authority
Pick \( p \) a large prime so that \( q = \frac{p-1}{2} \) is also prime.
Find a primitive root of \( p \) and form \( g \) its square. (Then if \( g^{k_1} \equiv g^{k_2} \pmod{p} \), then \( k_1 \equiv k_2 \pmod{q} \))
Pick random integers \( a \) and \( b \).
Find \( g_1 \equiv g^a \pmod{p} \) and \( g_2 \equiv g^b \pmod{p} \).
Throw away \( a \) and \( b \).
Release \( g \), \( g_1 \), and \( g_2 \). Also release a hash function \( H \) that maps a quintuple into an integer mod \( q \) and a hash function \( H_0 \) that maps a quaduple into an integer mod \( q \).

Initial Setup – Bank
Each bank picks a secret identity number \( x \).
Compute and make public the triplet: \( h \equiv g^x \pmod{p} \), \( h_1 \equiv g_1^x \pmod{p} \), \( h_2 \equiv g_2^x \pmod{p} \).
This triplet identifies the bank.

Customer Account Opening
The customer picks a secret \( u \) and computes \( I = g_1^u \pmod{p} \).
The customer gives \( I \) and his name, etc. to the bank. The bank computes \( z' \equiv (Ig_2)^x \pmod{p} \) and gives this to the customer.

Merchant Registration
The merchant picks a number \( M \) and registers it with the bank.

Customer Withdraws Coin
All coins have the same value. A coin is a sextuple \((A, B, Z, a, b, R)\).

1. The bank chooses a random \( w \) and computes \( g_w \equiv g^w \pmod{p} \) and \( \beta \equiv (Ig_2)^w \pmod{p} \).
The bank gives \( g_w \) and \( \beta \) to the customer.
2. The customer choose secret random \( s \), \( x_1 \), \( x_2 \), \( \alpha_1 \), and \( \alpha_2 \).
3. The customer computes (all \( \pmod{p} \)): \( A \equiv (Ig_2)^s \), \( B \equiv g_1^{x_1}g_2^{x_2} \), \( z \equiv z'^s \), \( a \equiv g_w^{\alpha_1}g^{\alpha_2} \), and \( b \equiv \beta^{\alpha_1}A^{\alpha_2} \).
We now have the first 5 values in the coin.
4. The customer computes \( c \equiv \alpha_1^{-1}H(A, B, z, a, b) \pmod{q} \) and sends it to the bank.
5. The bank computes \( c_1 \equiv cx + w \pmod{q} \) and send this to the customer.
6. The customer computes \( r \equiv \alpha_1c_1 + \alpha_2 \pmod{q} \) to complete the coin.

Both the bank’s \( w \) and the customer’s 5-tuple in step 2 should be different for each coin.
### Spending the Coin

The customer gives the coin \((A, B, z, a, b, r)\) to the merchant. The merchant check

1. The merchant check for valid coin by ensuring that \(g^r \equiv ah^{H(A,B,z,a,b)} \pmod{p}\) 
   and \(A^r \equiv bz^{h(A,B,z,a,b)} \pmod{p}\). 
   The remainder is to catch double spending.
2. The merchant computes \(d = H_0(A, B, M, t)\) \([t \text{ is a timestamp}]\) and sends this to the customer.
3. The customer computes \(r_1 \equiv dus + x_1 \pmod{q}\) and \(r_2 \equiv ds + x_2 \pmod{q}\). 
   He sends these to the merchant.
4. The merchant check that \(g^r g^s \equiv A^d B \pmod{p}\). 
   If so, accept else reject.

### Merchant Deposits Coin

Merchant submits both the coin \((A, B, z, a, b, r)\) and the triple \((r_1, r_2, d)\) to the bank. 
The bank checks that the coin has not been previously deposited. If it has, goto Fraud Dept. 
If not previously deposited, the bank checks \(g^r \equiv ah^{H(A,B,z,a,b)} \pmod{p}\) and \(A^r \equiv bz^{h(A,B,z,a,b)} \pmod{p}\) just like the merchant did. 

### Fraud Dept.

1. The customer spends the coin with the merchant and also with a vendor. The same coin is seen with different (valid) triplets: \((r_1, r_2, d)\) and \((r'_1, r'_2, d')\). 
   The bank computes \(r_1 - r'_1 \equiv us(d-d') \pmod{q}\) and \(r_2 - r'_2 \equiv s(d-d') \pmod{q}\) and division give \(u\). The bank can compute the corresponding \(I\) and identify the criminal. 
2. The merchant submits the coin with 2 different triplets, the original one and a forged one (trying to make it look like the customer used it twice). Producing the forged triple would involve solving the discrete logarithm problem to get \(u\). 
3. A customer tries to produce and unauthorized coin. The last field in the 6-tuple depends on the bank’s \(x\) or on by solving a discrete logarithm problem. 
4. The merchant tries to both deposit the coin and to spend it with merchant2. To match merchant2’s value of \(d\), the merchant would have to find \(r_1\) and \(r_2\) which depend on field in the coin (or the original customer). 
5. A bank teller forges a coin in the name of the customer. Since he has access to \(I\), he can create one. However, it can never be spent, the the \(r_1\) in the merchant’s triplet depends on the customer’s \(u\), which he doesn’t know. 
6. A thief steals the coin from the customer. The thief does not know \(u\), so the coin can not be spent. 
7. An evil vendor steals the coin and the triplet \((r_1, r_2, d)\) from the merchant. The theft will be successful. This is a problem with paper money too.