Los bitcoines contienen la dirección pública de su dueño. Cuando un usuario A transfiere algo a un usuario B, A entrega la propiedad agregando la clave pública de B y después firmando con su clave privada.31 A entonces incluye esos bitcoines en una transacción, y la difunde a los nodos de la red P2P a los que está conectado. Estos nodos validan las firmas criptográficas y el valor de la transacción antes de aceptarla y retransmitirla. Este procedimiento propaga la transacción de manera indefinida hasta alcanzar a todos los nodos de la red P2P.

Todos los nodos que forman parte de la red bitcoin mantienen una lista colectiva de todas las transacciones conocidas, a la que se denomina cadena de bloques.  
Los nodos generadores crean nuevos bloques añadiendo en cada uno de ellos el hash del ultimo bloque de la cadena mas larga de la que tienen conocimiento, asi como las nuevas transacciones pulicadas en la red. En el caso de que resulte un bloque valido, estos nodos lo agregan a la cadena y lo vuelven a retransmitir(indefinidamente hasta que alcance todos los nodos de la red).

HASH CASH : es un metodo para añadir un sello de texto al encabezado de un correo electronico para probar que el remitente a gastado una modesta cantidad de tiempo de cpu para calcular el sello antes de enviar el correo electronico. El receptor puede a un costo computacional despreciable, verifique que el sello es valido.

Se calcula la sha-1 de 160 bits (hash de la cabecera + numero aleatorio) . Si los primeros 20 bits son 0 entonces es un encabezado aceptable. Sino incrementa en 1 el numero aleatorio. Dado que aproximadamente 2²⁰ cabeceras tendran 20 ceros como el comienzo de la almohadilla, el remitente tiene que probar muchos valores aleatorios. Esto es muy barato de chequear para el receptor .

La cabecera mencionada anteriormente tiene la direccion del destinatario y la hora.