Model for Bitcoins

The Founders start a virtual currency by creating a spreadsheet with two columns and giving themselves 1000 units of currency. The first column is labeled "owners" and the second column is labeled "amount of coins." The first row reads Founders-1,000. At this point, the coins have no purchasing power because they cannot be used increase anyone's happiness. But then, the Founders persuade Bob to do something for them in exchange for 100 coins. The rows now read: Founders–900 and Bob-100. Now the coins have purchasing power, and Alice may want to trade with Bob or the Founder and asks for her own row: Alice-0. As more and more people start using the spreadsheet for transactions, the purchasing power of the imaginary coins will increase. According to the regression theory of money: The purchasing power of money in the present is determined by its purchasing power in the immediate past.

Ownership of the coins can be protected to a certain extent by linking a secret password to the cell with amounts known only by the owner of the coins. If Bob gives Alice 1 coin, Bob must use his password to decrease his amount and Alice must use her password to increase her amount. Everyone on the spreadsheet will make sure no there are no fraudulent increases or decreases in the amount column.

You can prevent fraud by making the passwords prime numbers (1, 3, 5, 7, 11, 13, 17, 19, 23, etc.) and replacing the name of the owner of the coins with a number that is the product of another prime number and the password. If the password chosen for Bob is 17 and the other prime number is chosen to be 13, "Bob" will be replaced with 221 because that is the product of 17 and 13. It is difficult to figure out that Bob's password is 17 from the number 221. Bob-100 now reads 221-100. In the language of Bitcoins, the public address is 221 and the private key is 17.

Let's suppose Bob wants to give Alice his 100 coins. Alice's cell has a password of 19, and the other prime is 11, so Alice-0 becomes 209-0. Bob multiplies 209 by his password (17) to get 3553 and gives this number to Alice. Alice divides 3553 by her password (19) and gets 187. She then divides 187 by 11 to get the password of Bob: 17. Alice is now the owner of 221-100.