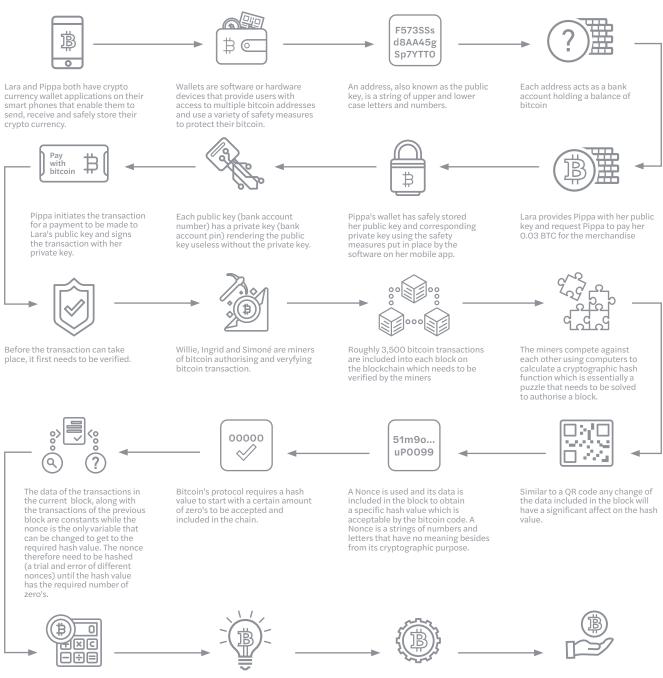
A bitcoin transaction

Lara is a bespoke handbag vendor and has decided to expand her business enabling customers to pay with bitcoin. Pippa found Lara's handbag website online and wants to purchase one of her advertised handbags.



Imagine calculators do not exist and you have not yet learned how subtraction works. Someone asks you what do you need to subtract from 8,511,235 to get 4,512,624. You need to now guess the number until you get to 3,998,611 which is the nonce. This may take a while, but you will eventually get to the answer. Cryptography used in bitcoin works very much in the same manner.

By way of trial and error different nonces are added to the block by the miners until the required amount of zero's in the hash value is obtained which is known as the winning hash, once this is achieved a transaction is approved and recorded on the chain. The winning miner is then rewarded in the form of bitcoin for the work he/she performed to solve the cryptographic puzzle.

Once the payment is approved the transaction is recorded on the blockchain and the bitcoins are reflected in Lara's wallet.



Wiehann Olivier
Partner
+27 21 818 5218 / +27 82 722 0429
wiehann.olivier@mazars.co.za