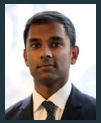
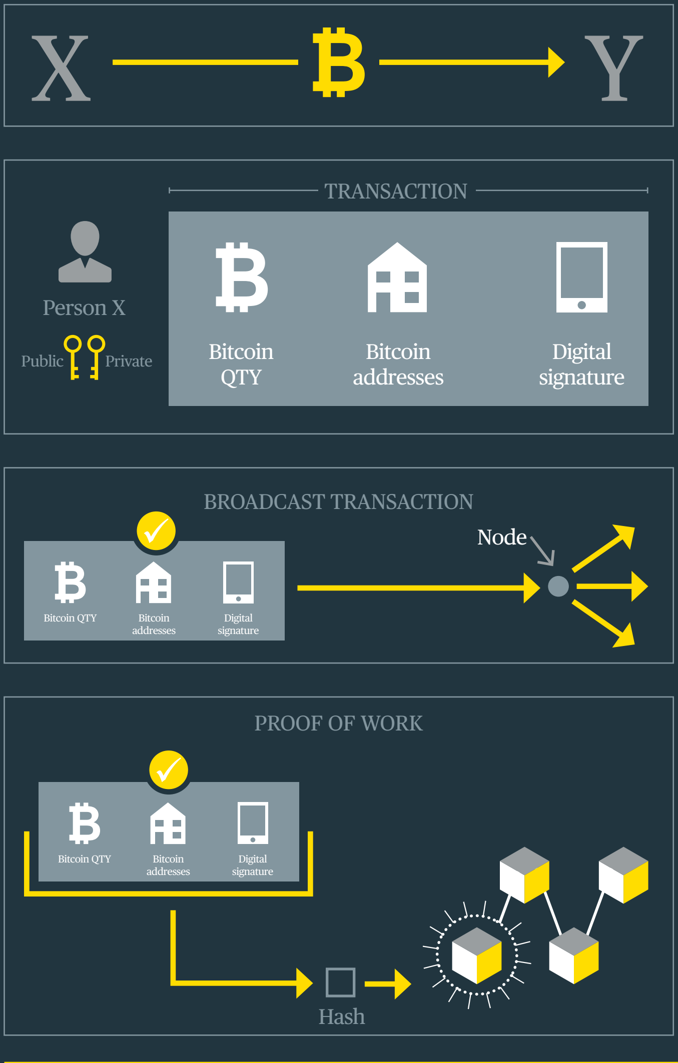
# Bird & Bird & Bitcoin transaction



*Jonathan Emmanuel*
*Partner*
Tel +44 (0)20 7415 6052
jonathan.emmanuel@twobirds.com

## Bitcoin transaction from start to finish



## Breaking down a blockchain transaction

Let's use bitcoin as an example as it's the most famous example of a blockchain network. First, let's explain some of the terminology.

### General

- A wallet stores your public and private cryptographic keys (a string of numbers generated as a pair and mathematically related). The public key is a unique, publicly available number and the private key is private to a user.
- An account is defined by this pair of keys. An account is operated by a user using the relevant private key and identified on the blockchain network by its bitcoin address (which is derived from the relevant public key). The bitcoin address enables users to identify each other on the bitcoin blockchain network so they can send bitcoins to each other (it is also referred to as the public address).
- You will have different public keys and private keys for each account.
- A wallet can store multiple pairs of keys and therefore accounts. A user can have multiple pairs of keys / accounts.

### Bitcoin and sending transactions

- Bitcoin is not stored in a wallet. It is decentrally 'stored' on the blockchain (the database recording the list of transactions that have taken place across the blockchain network). For example, if a transaction (X sends Y bitcoins to Z) is validated and added to a new block on the blockchain then we know that Z now has Y additional bitcoins and X has Y fewer bitcoins.
- On the bitcoin blockchain network every bitcoin is tied to a public and private key pair / account.
- The private key is your means of access to and authority for use of any bitcoin. It enables you to create transactions (e.g. I want to send X bitcoins to Y) and digitally sign transactions (i.e. sign them off) before they are broadcast to the blockchain network using a client.

### Clients / nodes

- In order to send a transaction to the network you need a client.
- A client is a piece of hardware or software that connects to a server. For example, an internet browser is a client: it connects to a website's server in order to request its content. In blockchain, a client is software that connects to other clients in a peer-to-peer manner. These clients talk to each other, forming a network (blockchain network). That is why when a client is set up and running (online and capable of communicating with other running clients) it is referred to as a "node" on the blockchain network (where the blockchain network is the network of nodes interacting with each other).
- These nodes are responsible for verifying and relaying the transactions on the blockchain network but they can also act as end-user software that allows a user to create transactions and / or mine / verify transactions before they are added to the blockchain.
- Often a client will include a wallet but sometimes they will be separate.

### Bitcoin transaction from start to finish:

- Let's take the following transaction: X transfers bitcoin to Y.
- X logs into his wallet and selects an account and creates the transaction. The transaction includes the number of bitcoins to send; X's bitcoin address so people know who's sending the transaction and Y's bitcoin address so people know who's receiving the transaction. The transaction needs to be signed by X using his/her digital signature.
- X uses a node to broadcast the signed transaction to the blockchain network.
- The transaction is broadcast to the blockchain and nearby nodes check the transaction is correct (has it been digitally signed etc.) ("Transactions").
- Mining nodes (miners), which are running implementations of the client that include special mining software and are responsible for verifying transactions, collect the Transactions and compete to verify them in accordance with the consensus algorithm embedded in the client (which is called proof of work for bitcoin).
- Proof of work involves miners competing to verify Transactions by solving a complex algorithmic problem. The miners prove they've completed the work when they can identify the hash that solves the problem (hence the name "proof of work").
- Once the problem is solved the miners create a block with the Transaction and the hash in it and add it to the blockchain.
- The blockchain is then updated with the new block and all the nodes' copies of the blockchain are updated.

### Wallets

- There are multiple kinds of wallets:
  - » *Software wallets* - applications that you can download and use on a desktop or mobile device, or access and use online.
  - » *Hardware wallets* - Hardware wallets store a user's keys on a hardware device, for example a USB device like the Nano Ledger S. These wallets have compatibility with various web interfaces. A hardware wallet is typically more secure than a software wallet as it will store your keys on the device, offline.
  - » *Paper wallets* - For paper wallets, private and public keys are generated using a software application and are then printed on to paper. Paper wallets generally work with software wallets - for example, the public address of a user's software wallet might receive bitcoin and then the user may decide to transfer the bitcoin to the public address printed on the piece of paper (relating to the Paper Wallet).

twobirds.com