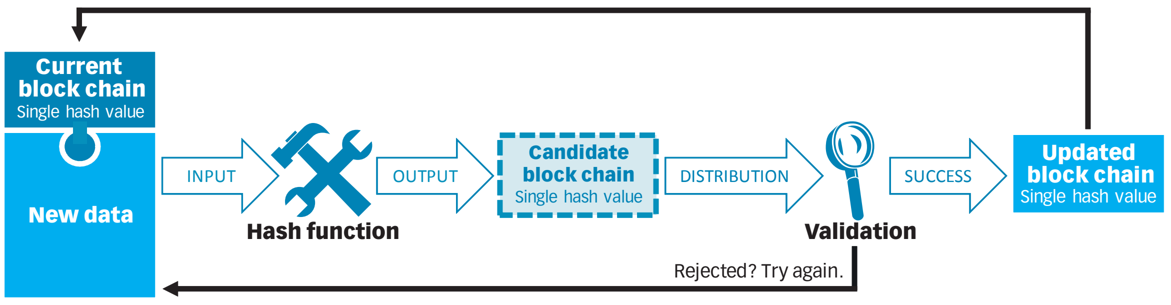
BT Explains

Blocks, chains and hashes

A block chain is very simply a way to maintain a database without a central authority. One of the most closely studied areas of financial technology, it came into prominence in the past few years as the core mechanism behind the Bitcoin cryptocurrency. Block chains are already being tested for post-trade services and trade financing ledgers, and pundits expect the innovation to usher in disruptions in many other fields. *– By* ***KENNETH LIM***

What is a block chain?

A block chain is a database in which each update comprises new data and a full description of the database before the current update. When applied with certain rules and protocols, the block chain makes it feasible to have a fully distributed database in which users always have the most updated version of the database, there is confidence in the integrity of the data, and many parties may independently update the data.



Step 1: : Take a bunch of new data. If there is an existing version of the block chain, add it to the new data.

Step 2: Run the combined data-and-block-chain through an encryption algorithm called a hash function, which will give you a hash value.

Step 3: Send this hash value and the new data that you added to the rest of the network for validation.

Step 4: If your candidate is rejected, everyone carries on as before and you will have to start over.

Step 5: If your candidate is accepted, everyone adopts your candidate as the latest version of the block chain.

Hash functions and hash values

Hash functions are the engine that enable many of the main functions of a block chain. Here's how they work:

Fixed length
The output of a hash function is a hash value, which is always the same size regardless of the input. But it must also be long enough to reduce the chances of two inputs resulting in the same hash value.

Input		Output
Apple	➡	5 g 7 K
Apple Banana	➡	N v h 8

Variability and direction
A small change in the input can result in a vastly different hash value. It is also extremely difficult to figure out the input from a hash value, making it practically impossible to work backwards.

Input		Output
Apple	➡	5 g 7 K
Apples	➡	9 w z 9

Replicability
The same input always results in the same hash value.

Input		Output
Apple	➡	5 g 7 K
Apple	➡	5 g 7 K

Why use block chains?

Distributed and decentralised database
A block chain can work without a centralised authority. This can be more efficient in some cases, and generally reduces the risk of errors because everybody has a set of the data.

Information integrity
The rules provide a process to verify new data, and when the new data is validated, that everybody on the network has access to the most current and correct version. It is also extremely difficult to try to tamper with historical records.

What to look for in block chain products

While there are general principles that describe what a block chain is, specific rules and algorithms are entirely up to a block chain's creator. These are some issues that every block chain should address.

Public or private
Anyone can add a block to the chain in a public system, while only some are conferred that right in a private model. Rules and incentives for mining and validation may therefore be different.

Conflict resolution
Rules must be established to resolve conflicts that arise as a result of the distributed nature of a block chain. For instance, what happens if two parties submit new and differing versions of the block chain at the same time?

Addition of new blocks
What goes into a block and what goes into each version of the block chain must be determined. Bitcoin requires the addition of a number called a nonce whose sole purpose is to slow down the rate at which new blocks are added, but such a delay mechanism might not make sense in cases such as trade repositories.

Certainty of settlement
There can be uncertainty in terms of when an intended transaction is included in a block chain, and whether inclusion may be voided as a result of a conflict. For example, requiring a certain number of blocks to be added before accepting the validity of the data is a way of trying to address the efficiency and reliability of the block chain.

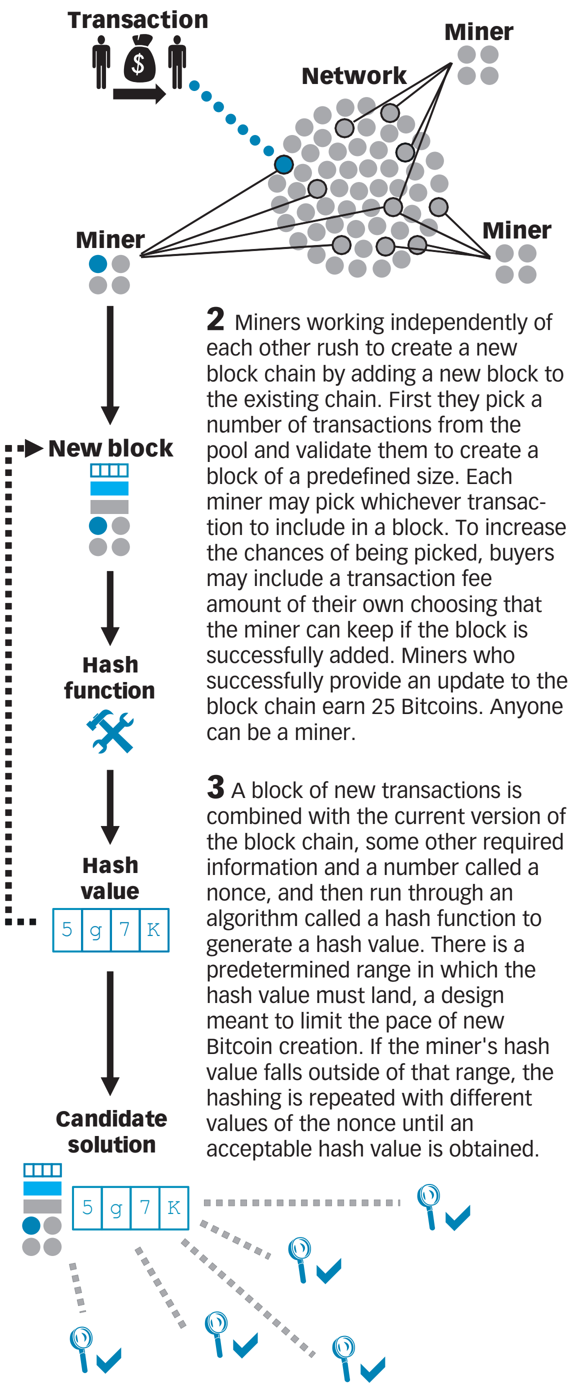
Who uses block chains?

Trade finance ledgers
DBS Bank and Standard Chartered have teamed up to share records for trade finance contracts and transactions. By having a distributed ledger, the banks hope to avoid falling victim to companies that pledge a single contract or asset to more than one lender.

Trade settlement and clearing
The Australian Securities Exchange is trying to develop a block chain-based clearing and settlement system as a way to reduce administrative and reconciliation costs.

The Bitcoin block chain

1 A buyer who wants to pay with Bitcoin must first declare to the Bitcoin network how much he plans to transfer and to whom, and that declaration joins a network-wide pool of announced transactions. Transactions in the pool remain unsettled until they are successfully added to a new version of the block chain.



2 Miners working independently of each other rush to create a new block chain by adding a new block to the existing chain. First they pick a number of transactions from the pool and validate them to create a block of a predefined size. Each miner may pick whichever transaction to include in a block. To increase the chances of being picked, buyers may include a transaction fee amount of their own choosing that the miner can keep if the block is successfully added. Miners who successfully provide an update to the block chain earn 25 Bitcoins. Anyone can be a miner.

3 A block of new transactions is combined with the current version of the block chain, some other required information and a number called a nonce, and then run through an algorithm called a hash function to generate a hash value. There is a predetermined range in which the hash value must land, a design meant to limit the pace of new Bitcoin creation. If the miner's hash value falls outside of that range, the hashing is repeated with different values of the nonce until an acceptable hash value is obtained.

4 When a miner obtains an acceptable hash value, that hash value and all of the data that were fed into the hash function are broadcast to the Bitcoin network, where other miners will verify the solution. If the majority of the computing power accepts the new hash function as correct, the candidate will become the latest version of the block chain.

5 If differing candidates emerge at the same time, a fork is deemed to have occurred in the block chain. Each prong of the fork exists as long as they remain the same length, and miners may try to add to either fork. But when one prong becomes longer than the other, the shorter prong is abandoned, and all of the transactions in that prong return to the pool of unsettled transactions.

BT Graphics:Elenita Sarah Loyola