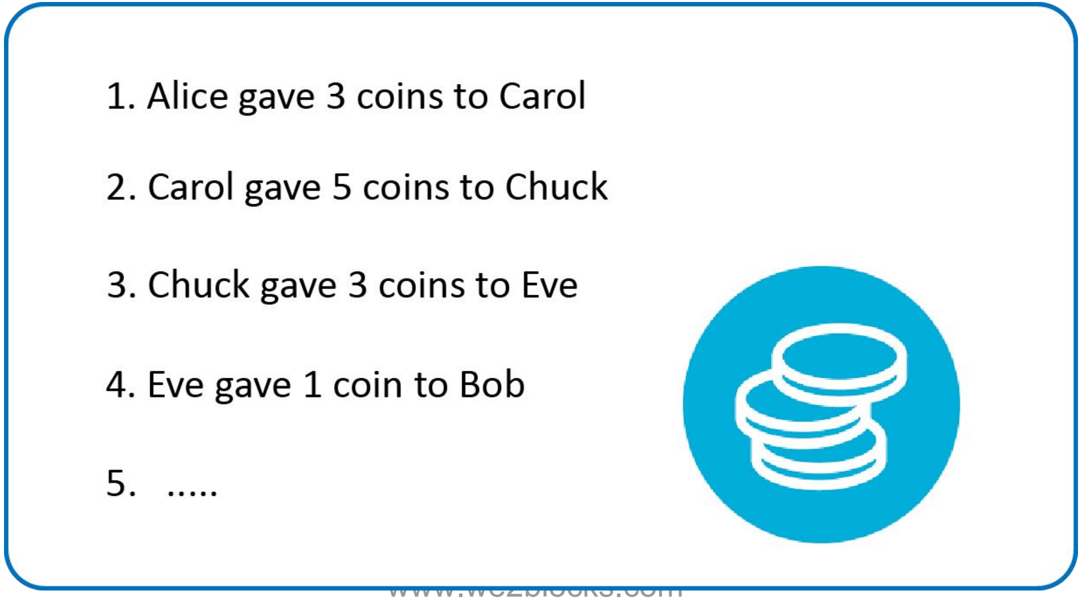
Professional Blockchain Course

How Blockchain works?

How Blockchain Works?

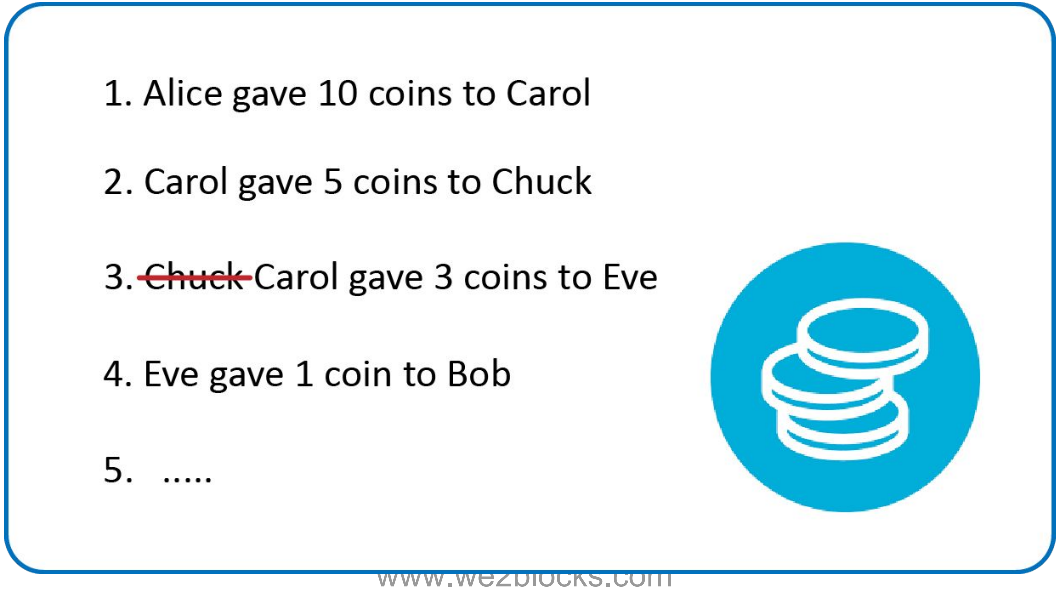
- Let's imagine that ten people in one room decided to make their currency. They need to know the flow of the funds. One person – let's call him Dave– chose to keep a list of all actions in a diary:



1. Alice gave 3 coins to Carol
2. Carol gave 5 coins to Chuck
3. Chuck gave 3 coins to Eve
4. Eve gave 1 coin to Bob
5. .....

How Blockchain Works?

- One man – let’s call him Chuck – decided to steal money. To hide this, he changed the entries present in the diary:



1. Alice gave 10 coins to Carol
2. Carol gave 5 coins to Chuck
3. ~~Chuck~~ Carol gave 3 coins to Eve
4. Eve gave 1 coin to Bob
5. .....

How Blockchain Works?

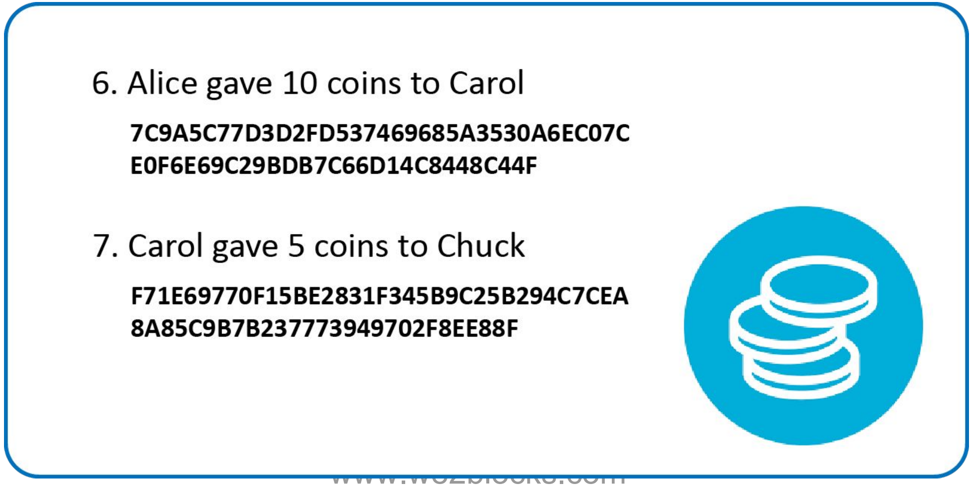
- Dave noticed that someone had interfered with his diary. He decided to stop this from happening. He created a program called a Hash function that turns text into a set of numbers and letters as in the table below:

Attack	4CD548F3CC29CF9C99A0134A971B1BE03C8F6BF80BA8F03E174E030B0D292396
Can’t Attack	88F5E3FED928950C36A67A11CA068F38CCB2E7DA01421C087BC11C842C869282
Can Attack	4AB7698451F8A85580ABED2E2BC94F6CCF05B6B95A587C2BFD771CCDCB4E450D

How Blockchain Works?

A hash is a fixed string of alphanumeric characters, created by a hash function. A hash function is a mathematical function that takes a variable number of string characters and converts them into a fixed number of alphanumeric characters. Even a small change in a line creates an entirely new hash.

- After each record, he inserted a hash. The new diary was as follows:



6. Alice gave 10 coins to Carol

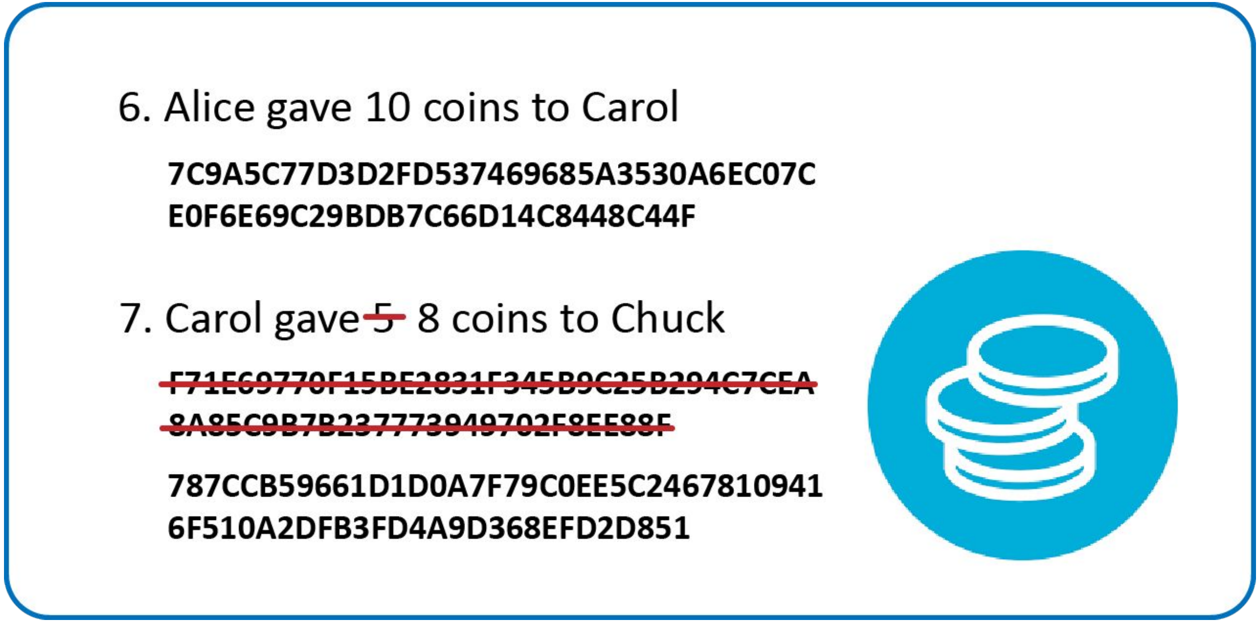
7C9A5C77D3D2FD537469685A3530A6EC07C
E0F6E69C29BDB7C66D14C8448C44F

7. Carol gave 5 coins to Chuck

F71E69770F15BE2831F345B9C25B294C7CEA
8A85C9B7B237773949702F8EE88F

How Blockchain Works?

- Chuck decided to manipulate entries again. He got to the diary at night, changed the record and generated a new hash.



6. Alice gave 10 coins to Carol

7C9A5C77D3D2FD537469685A3530A6EC07C
E0F6E69C29BDB7C66D14C8448C44F

7. Carol gave ~~5~~ 8 coins to Chuck

~~F71E69770F15BE2831F345B9C25B294C7CEA~~
~~8A85C9B7B237773949702F8EE88F~~

787CCB59661D1D0A7F79C0EE5C2467810941
6F510A2DFB3FD4A9D368EFD2D851

How Blockchain Works?

- Dave noticed that somebody had sifted through the diary again. He decided to complicate the record of each transaction. After each record, he inserted a hash generated from the record+last hash. So each entry depends on the previous.
- If Attacker tries to change the record, he will have to change the hash in all previous entries.

How Blockchain Works?

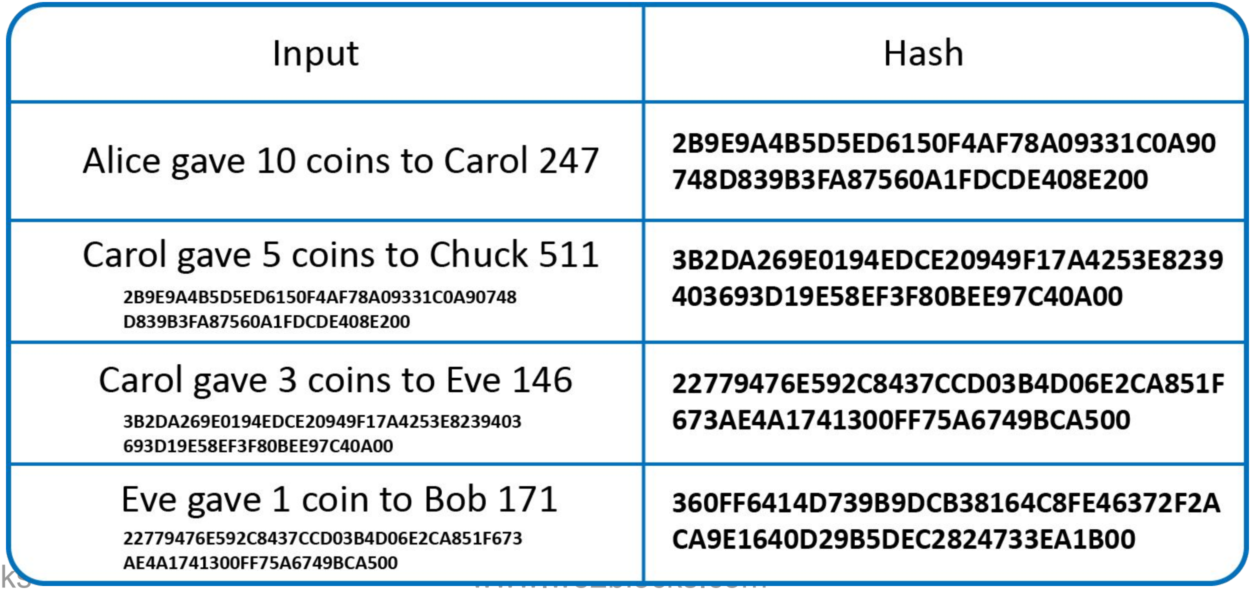
Input	Hash
Alice gave 10 coins to Carol	7C9A5C77D3D2FD537469685A3530A6EC 07CE0F6E69C29BDB7C66D14C8448C44F
Carol gave 5 coins to Chuck 7C9A5C77D3D2FD537469685A3530A6EC 07CE0F6E69C29BDB7C66D14C8448C44F	F71E69770F15BE2831F345B9C25B294C7 CEA8A85C9B7B237773949702F8EE88F
Carol gave 3 coins to Eve F71E69770F15BE2831F345B9C25B294C7 CEA8A85C9B7B237773949702F8EE88F	5C19F496C977AA7798EFF57C939B3AE5E FB442B69D63CAFE8D41203884C5BAC1
Eve gave 1 coin to Bob 5C19F496C977AA7798EFF57C939B3AE5E FB442B69D63CAFE8D41203884C5BAC1	C4BDA779BE74375BC6FF1FFE6DC158EDB D645E8BAB0F1334AEA39EA061D853D0

How Blockchain Works?

- Chuck wanted more money, and he spent the whole night counting all the hashes.
- Finally changing all the hash entries accordingly. He replaced all the hashes with the corresponding cheat hashes.

How Blockchain Works?

- Dave did not want to give up. He decided to add a random number after each record. This number is called “Nonce.” Nonce should be chosen so that the generated hash ends in two zeros.



Input	Hash
Alice gave 10 coins to Carol 247	2B9E9A4B5D5ED6150F4AF78A09331C0A90748D839B3FA87560A1FDCDE408E200
Carol gave 5 coins to Chuck 511 2B9E9A4B5D5ED6150F4AF78A09331C0A90748D839B3FA87560A1FDCDE408E200	3B2DA269E0194EDCE20949F17A4253E8239403693D19E58EF3F80BEE97C40A00
Carol gave 3 coins to Eve 146 3B2DA269E0194EDCE20949F17A4253E8239403693D19E58EF3F80BEE97C40A00	22779476E592C8437CCD03B4D06E2CA851F673AE4A1741300FF75A6749BCA500
Eve gave 1 coin to Bob 171 22779476E592C8437CCD03B4D06E2CA851F673AE4A1741300FF75A6749BCA500	360FF6414D739B9DCB38164C8FE46372F2ACA9E1640D29B5DEC2824733EA1B00

How Blockchain Works?

- Now, to forge transactions, Chuck would need to spend hours choosing Nonce for each line.
- More importantly, its very hard for even the computers to figure out the nonce quickly.
- Sometime after, Dave realized that there were too many transaction records and that he couldn’t keep the diary like this forever. After reaching 10,000 transactions, he converted them to a one-page spreadsheet. Carol checked that all transactions are right.
- Dave spread his spreadsheet diary over 10,000 computers located globally.
- These computers are called nodes. Every time a new transaction occurs, it has to be validated by the nodes.
- Once every node has received/checked a transaction there is a sort of electronic vote, as some nodes may think the transaction is valid and others believe it is a fraud.
- Now, if Chuck changes one entry, all the other computers will have the original entries. They would not allow fraud entries to occur.

Summarising

- This spreadsheet created in the example is called a block.
- The whole chain of blocks is collectively called as Blockchain. Every node holds a copy of the Blockchain. Once a block reaches a certain number of approved transactions, then a new block is formed.
- The Bitcoin Blockchain updates itself every ten minutes.
- As soon as the spreadsheet or ledger or registry is updated, it can no longer be changed. Thus, it’s impossible to forge it.

THANK YOU

For more information contact
info@we2blocks.com