Blockchain Basics

An introduction to blockchains

Primechain Technologies Pvt. Ltd.
www.primechain.in

Blockchain basics

- ☑ Hash functions
- ○ Proof of work
- ○ Merkle Tree
- ○ Blockchain
- ○ Miners
- ○ Key issues

One-way Hash Functions

Input	Hash
sanya	834ac48d8e6d1d7f0b8d21a5b3e81446f5a4caa63765cc23836f61844b67fb83
SANYA	4247bff9d41c0f2da68ef43c5624531da9ca5bc31b39760a67e32265082e1ba8
Sanya	513a15ed036e62c14b41b2608a5bb18aa7af2a3502c90b892f9dddabaf136bc2

Input	Hash
	b48928ef0131d6fb61b5cee25163ae104a25f0edbd4230f2e7b3daa4a9b057d3
	043a718774c572bd8a25adbeb1bfcd5c0256ae11cecf9f9c3f925d0e52beaf89

Blockchain basics

- ☑ Hash functions
- ○ Proof of work
- ○ Merkle Tree
- ○ Blockchain
- ○ Miners
- ○ Key issues

- **Hash functions** take an electronic record (such as a PDF file, a video, an email etc.) and produce a fixed-length output e.g. 64 characters.
- If the information is changed in any way – even a comma is changed in a 3000 page document – a different output value is produced.
- There's no way to calculate the original record from the hash.

Blockchain basics

- ☑ Hash functions
- ○ Proof of work
- ○ Merkle Tree
- ○ Blockchain
- ○ Miners
- ○ Key issues

Practical activity 1

Calculate hash values for random inputs

http://www.primechain.in/academy/1_hash/

Blockchain basics

- Hash functions
- ☑ Proof of work
- Merkle Tree
- Blockchain
- Miners
- Key issues

1. Sender^Receiver^Date^Nonce
2. Hash begins with 4 zeros

input	d@blockchain.org.in^info@primechain.in^10092016^1
hash	288721860bec3a490811981c831702d4f41e54c3f8c183c5650ac73ff231659c

input	d@blockchain.org.in^info@primechain.in^10092016^2
hash	241e2b81192c0aa918c14f2896522428ccb77e937cade900d8f052ec3966c9cf

... increase nonce till ....

input	d@blockchain.org.in^info@primechain.in^10092016^66504
hash	00006bcc72f130eedbe9830c47e8d9f500d1e232540b03e095950aa798e2b97d

Computing hash is not trivial, verification is.

Blockchain basics

- Hash functions
- ☑ Proof of work
- Merkle Tree
- Blockchain
- Miners
- Key issues

Practical activity 2

http://www.primechain.in/academy/2_pow/nonce.php

```
<?php
$block= "d@blockchain.org.in^info@primechain.in^10092016^";
$nonce=0;
while ($nonce < 500000)
{
$myString = $block . $nonce;
$hash = hash('sha256', $myString);
$result = mb_substr($hash, 0, 4);
if ($result==="0000") {echo $nonce." : ".$hash."<br/>";}
$nonce++;
}
?>
```

Blockchain basics

- Hash functions
- ☑ Proof of work
- Merkle Tree
- Blockchain
- Miners
- Key issues

Practical activity 3

http://www.primechain.in/academy/2_pow/nonce2.php

```
<?php
$block= "d@blockchain.org.in^info@primechain.in^10092016^";
$nonce=0;
while ($nonce < 99999)
{
$myString = $block . $nonce;
$hash = hash('sha256', $myString);
$result = mb_substr($hash, 0, 4);
echo $nonce." : ".$hash."<br/>";
$nonce++;
}
?>
```

Blockchain basics

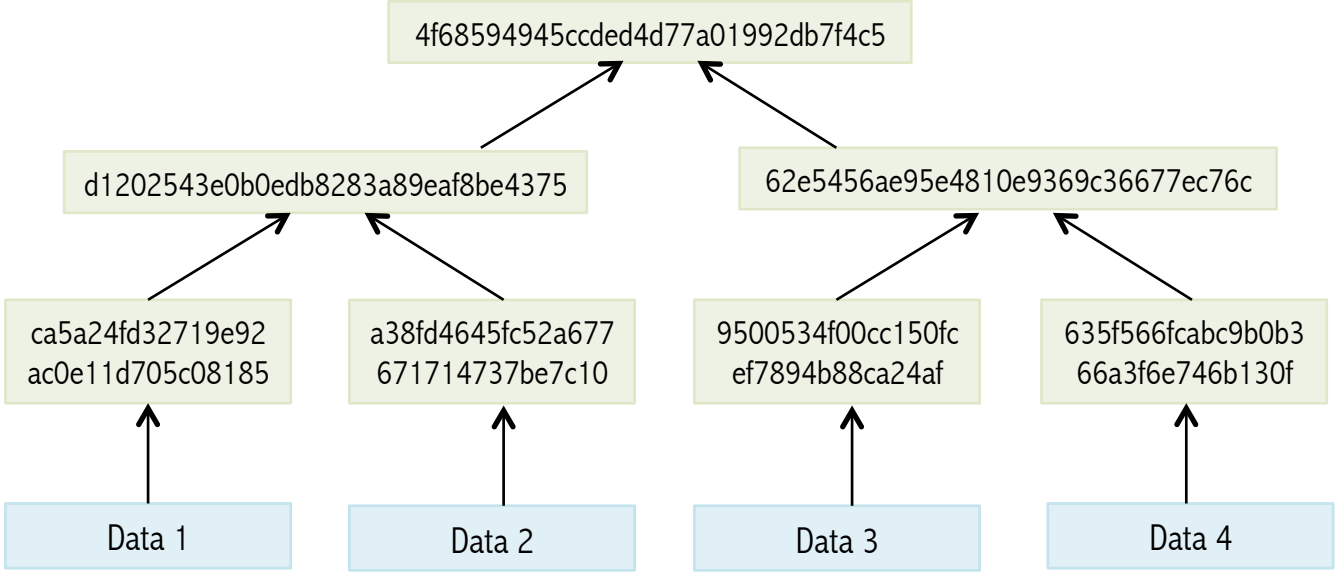
- Hash functions
- ☑ Proof of work
- Merkle Tree
- Blockchain
- Miners
- Key issues

Practical activity 4

Run nonce.php and nonce2.php on your computers.

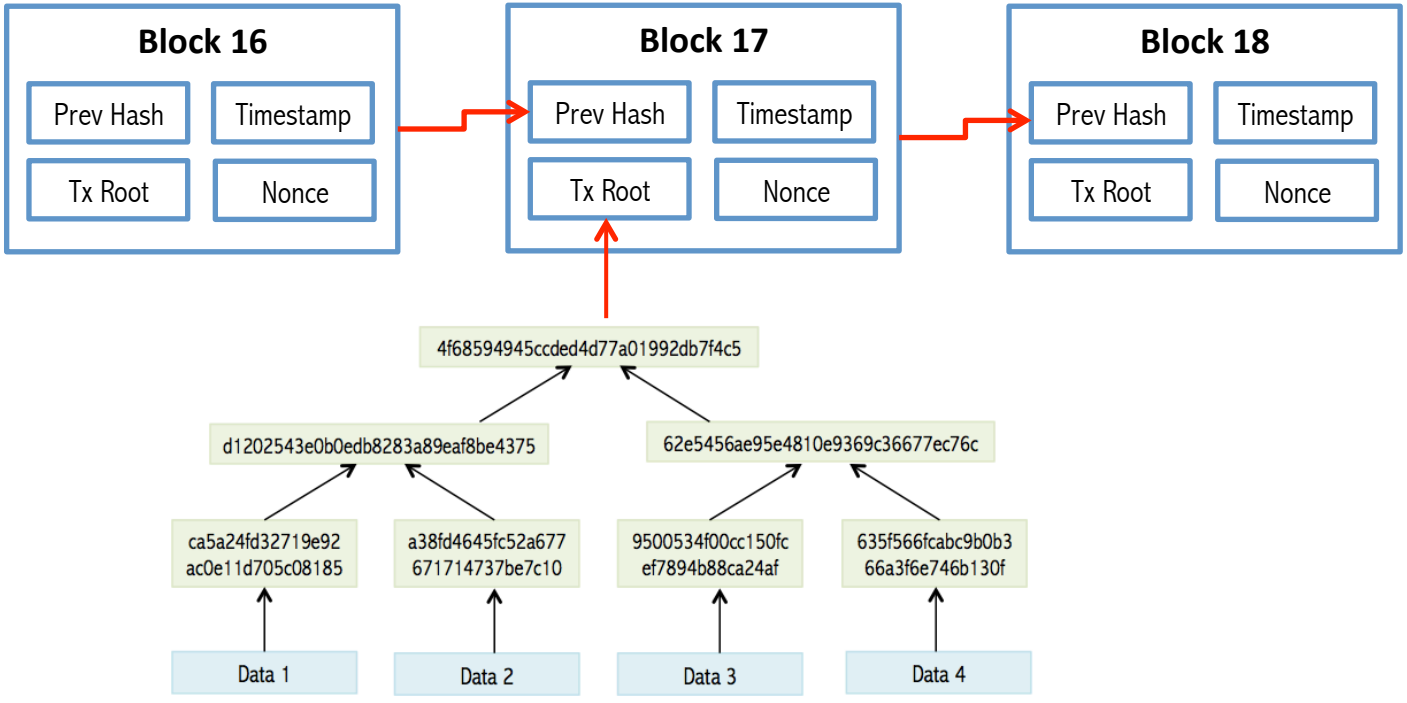
Blockchain basics

- Hash functions
- Proof of work
- ☑ Merkle Tree
- Blockchain
- Miners
- Key issues



Blockchain basics

- Hash functions
- Proof of work
- Merkle Tree
- ☑ Blockchain
- Miners
- Key issues



1. Ordered and time-stamped record.
2. Prevents double-spending.
3. Prevents modification of previous records.

Blockchain basics

- ○ Hash functions
- ○ Proof of work
- ○ Merkle Tree
- ○ Blockchain
- ☑ Miners
- ○ Key issues

- While a gold miner digs into the earth to discover gold, a bitcoin miner uses computational power to calculate hashes.
- To add an entire block to the block chain, a Bitcoin miner must successfully hash a block header to a value below the target threshold.
- Miners spend on **computational power** and **electricity** and are compensated by way of a **reward** for each block they mine and **transaction fees**.
- Miners usually operate as part of a large pool instead of as individuals.

Blockchain basics

- ○ Hash functions
- ○ Proof of work
- ○ Merkle Tree
- ○ Blockchain
- ☑ Miners
- ○ Key issues

Blockchain basics

- ○ Hash functions
- ○ Proof of work
- ○ Merkle Tree
- ○ Blockchain
- ☑ Miners
- ○ Key issues

Blockchain basics

- ○ Hash functions
- ○ Proof of work
- ○ Merkle Tree
- ○ Blockchain
- ☑ Miners
- ○ Key issues

Blockchain basics

- ○ Hash functions
- ○ Proof of work
- ○ Merkle Tree
- ○ Blockchain
- ○ Miners
- ☑ Key issues

- ❑ Bitcoin platform vs. the bitcoin cryptocurrency
- ❑ The Blockchain vs. blockchains
- ❑ Permissioned blockchains

Stuff that only blockchains CAN do	Stuff that blockchains CAN do better	Stuff that blockchains CANNOT do
Crypto-currencies	• Data auth & verification • Securities settlement	High speed trading