

dive deep into
blockchain

Tomasz Kowalczyk / @tmmx





blockwhat?

database



chain of blocks

block of data

data structure

cryptocurrency

general purpose

blockwhy?

The background is a solid purple color with a subtle, textured pattern that resembles a canyon or layered rock formations. The word "immutability" is centered in the middle of the image in a white, lowercase, sans-serif font. The 'i' is slightly smaller and more compact than the other letters.

immutability

append only

The background of the image is a photograph of a mountain range, heavily tinted with a deep purple color. The mountains have a rugged, layered appearance with visible geological strata. The lighting is soft, creating a serene and somewhat ethereal atmosphere. The word "traceability" is centered in the lower half of the image in a white, lowercase, sans-serif font.

traceability

verifiability

tamper proof

integrity

decentralization

trust(less)

transparency

blockwhen?

voting
medical records
cloud storage
financial transactions
decentralized messaging
property registry
land sales
insurance

digital wallets
smart contracts
crowdfunding
property ownership
social networking
P2P finances
virtual countries
asset trading

few hours later...

smart contracts
e-commerce

digital identity

anti-counterfeiting
mechanisms

loyalty programs

internal currency

regulatory reporting

cross-border payments

blockhow?

public
shared
private

The background of the image is a dark purple grid. Overlaid on this grid are faint, handwritten mathematical notes in a light purple or white color. These notes include various mathematical expressions, equations, and diagrams. For example, there are expressions like $2F$, 136° , and 100 scattered across the grid. Some of the notes appear to be related to geometry or trigonometry, with lines and angles drawn. The overall aesthetic is that of a mathematician's workspace or a notebook page.

cryptography

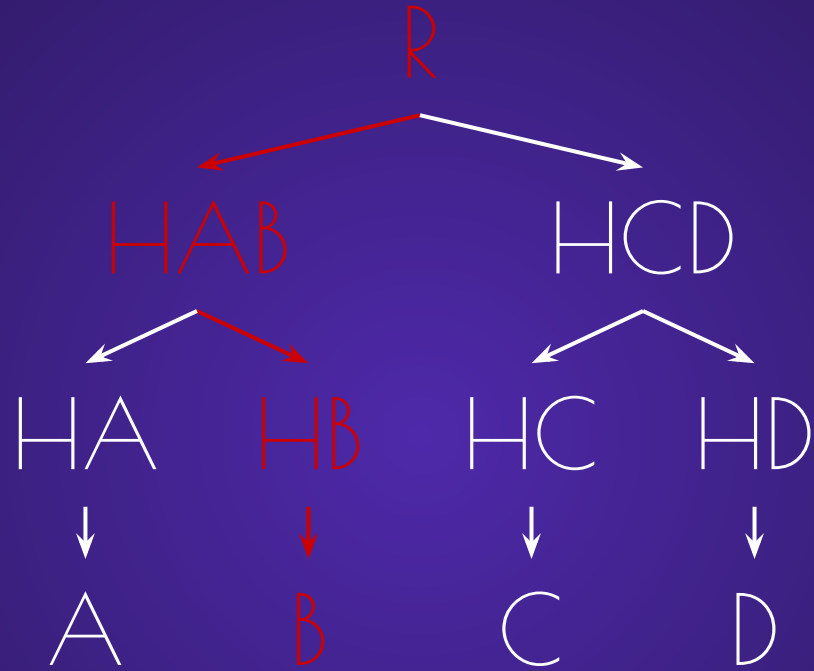
addresses

hash algorithm



Merkle tree

aka. binary hash tree



B Merkle path: $R-HAB-HB$

genesis block

A close-up photograph of two hands shaking in a firm grip, symbolizing agreement or partnership. The image is overlaid with a semi-transparent purple filter. The word "consensus" is written in a white, lowercase, sans-serif font across the center of the handshake.

consensus



proof of work

proof of stake



mining

smart contracts

case study

Hashchain?


```
$storage = new SqliteStorage('chain.sq3');  
$signer = new OpenSslSigner('private.key', 'public.key');  
$genesis = new Block(new Entries([  
    new GenesisEntry('fiat lux'),  
]));
```

```
$chain = new Hashchain($storage, $signer, $genesis);
```

```
$db = new PDO('read.sqlite3');

$events = new EventDispatcher();
$events->addListener(Events::BLOCK_CREATED, function(Block $block) use($db) {
    array_map(function(EntryInterface $entry) use($db) {
        if($entry instanceof NewEntityEntry) {
            $db->insertEntry($entry);
        }
    }, $block->getEntries());
});
$chain = $chain->withEvents($events);

$chain->createBlock(new Entries([
    new NewEntityEntry(Uuid::uuid4(), 'E#1', new \DateTimeImmutable()),
]));
```



```
$chain->createBlock(new Entries([  
    new UpdateEntityEntry($uuidE1, 'UE#1', new \DateTimeImmutable()),  
    new NewEntityEntry(Uuid::uuid4(), 'E#2', new \DateTimeImmutable()),  
]));
```

```
$chain->createBlock(new Entries([  
    new RemoveEntityEntry($uuidE2, new \DateTimeImmutable()),  
]));
```

```
$events = new EventDispatcher();
$events->addListener(Events::BLOCK_CREATED, function(Block $block) use($db) {
    array_map(function(EntryInterface $entry) use($db) {
        switch(get_class($entry)) {
            case NewEntityEntry::class: { $db->insertEntry($entry); }
            case UpdateEntityEntry::class: { $db->updateEntry($entry); }
            case RemoveEntityEntry::class: { $db->removeEntry($entry); }
        }
    }, $block->getEntries);
});
```

game of chess

```
$storage = new SqliteStorage('chess.sq3');  
$connection = new Connection($ip, $port);  
$genesis = new GenesisBlock('You vs Blockchain');  
  
$chain = new ChessChain($storage, $connection, $genesis);
```

```
// Four Knights Game  
// 1. e4 e5 2. Nf3 Nc6 3. Nc3 Nf6  
// White begins
```

```
$chain->add(new MoveBlock('E4'));  
$chain->add(new MoveBlock('E5'));  
$chain->add(new MoveBlock('Nf3'));  
$chain->add(new MoveBlock('Nc6'));  
$chain->add(new MoveBlock('Nc3'));  
$chain->add(new MoveBlock('Nf6'));
```



source: lichess.org

```
// Knight is already there!  
$chain->add(new MoveBlock('Nf3'));
```

challenges

fault tolerance

integration

security

privacy

access

(hard) forks

51%

summary

right solution
for the right problem

Event Sourcing

scratching surface

BlocQuestions?

BlocThanks!

Resources

<http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html>
<http://chimera.labs.oreilly.com/books/1234000001802/index.html> (Mastering Bitcoin)
<https://www.coindesk.com/math-behind-bitcoin> (EC)
https://en.wikipedia.org/wiki/Four_Knights_Game (Chess)
<http://queue.acm.org/detail.cfm?id=3136559> (Bitcoin)
<https://blog.acolyer.org/2017/08/30/a-concurrent-perspective-on-smart-contracts> (smart contracts)
<https://en.bitcoin.it/wiki/Secp256k1> (Bitcoin Elliptic Curve)

Pictures (Creative Commons)

<https://www.flickr.com/photos/skyseeker/14404947216> (lightning)
<https://www.flickr.com/photos/atermath/3053484935> (stripes)
<https://www.flickr.com/photos/randnotizenorg/32110828536> (electronic)
<https://www.flickr.com/photos/23221002@N00/7204014842> (equations)
<https://www.flickr.com/photos/spookyamd/14184019077> (mountain)
<https://www.flickr.com/photos/s1ng0/5445857570> (trees)
<https://www.flickr.com/photos/95213174@N08/10329928973> (handshake)
<https://www.flickr.com/photos/wiertz/4563720850> (signature)
<https://www.flickr.com/photos/33279673@N03/5482493912> (chains)