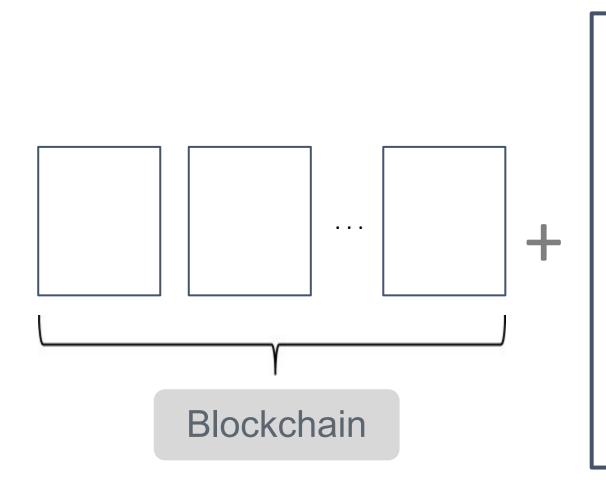
From Blocks to a Blockchain



Alice: 5 BTC
Bob: 2 BTC
John: 21 BTC
Joe: 1 BTC
Amy: 0.6 BTC
Leslie: 43 BTC

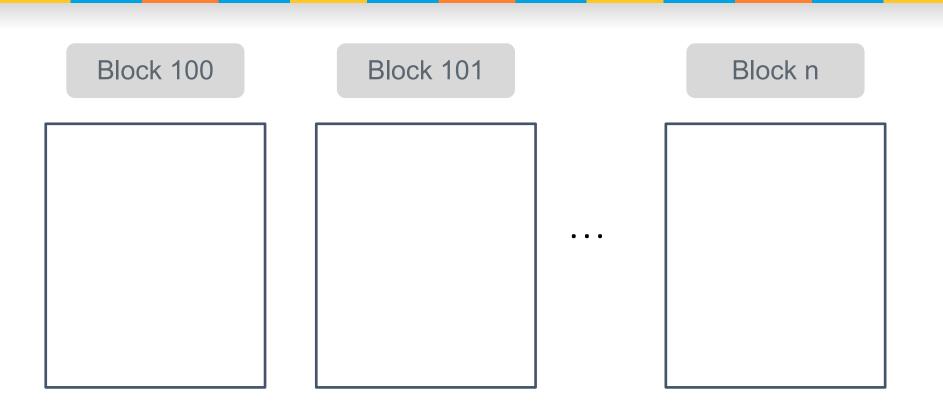
.

Tim: 8 BTC
Nicole: 0.3 BTC
Jesse: 11 BTC
Steven: 17 BTC
Darren: 3 BTC

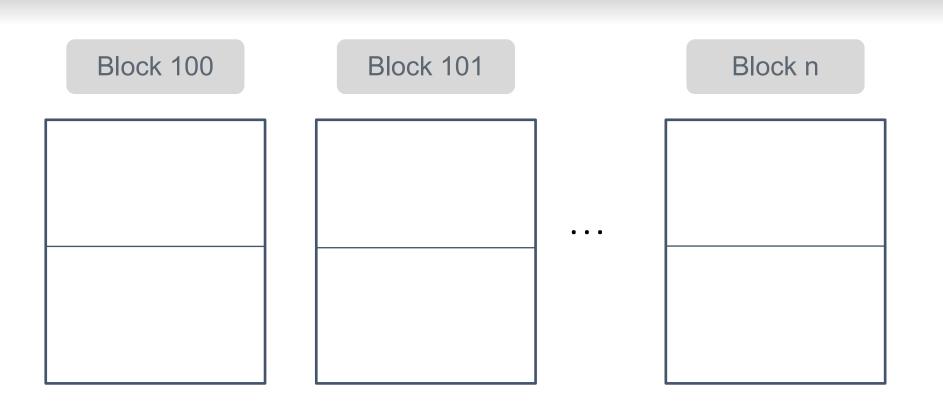
Jose:

0.1 BTC

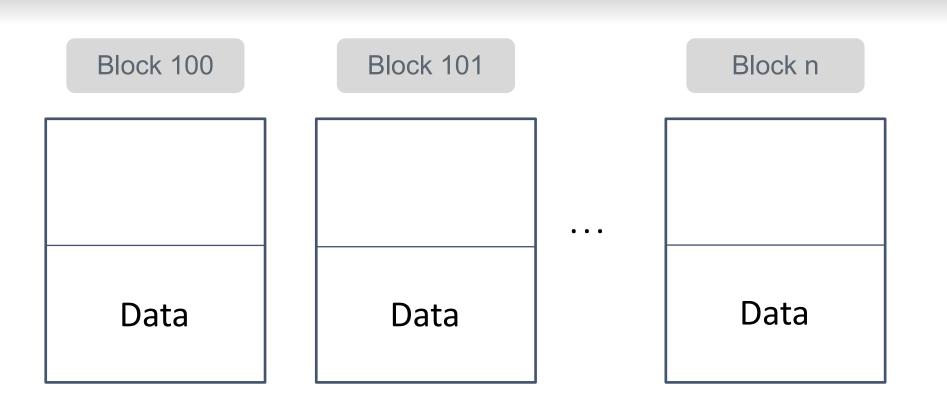
Blockchain - Detail



Blockchain - Two Main Components



Blockchain Component – 1) Data to Store



Blockchain Component – 2) Block Header

Block 100

Block 101

Block n

Block Header

Data

Block Header

Data

Block Header

Data

From Data to Transactions

Block 100

Block 101

Block n

Block Header

Transactions

Block Header

Transactions

Block Header

Transactions

Transaction Model with Two Accounts

Block 100

Block 101

Block n

Block Header

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC Block Header

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC Block Header

What Goes in the Block Header?

Block 100

Timestamp
Hash of Previous
Block Header

Hash of Transactions

Nonce

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC Block 101

Timestamp
Hash of Previous
Block Header

Hash of Transactions

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC Block n

Block Header

Block Header Detail (1/5)

Block 100

10:49 PM Hash of Previous

Block Header

Hash of Transactions

Nonce

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC Block 101

11:01 PM

Hash of Previous Block Header

Hash of

Transactions

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC Block n

Block Header

Block Header Detail (2/5)

Block 100

10:49 PM
Hash of Previous
Block Header

Hash of Transactions

Nonce

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC Block 101

11:01 PM Hash of Previous Block Header

Hash of Transactions

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC Block n

Block Header

Block Header Detail (3/5)

Block 100

10:49 PM Hash of Previous **Block Header**

> Hash of **Transactions**

> > Nonce

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC



Hash Function



Block 101

11:01 PM Hash of Previous Block Header

Hash of **Transactions**

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC

Block n

Block Header

Hunter -> Kyle 0.2 BTC Megan -> Ryan 13 BTC Justin -> Jose 7 BTC

8f434...9b2dc327aa4

Block Header Detail (4/5)

Block 100

10:49 PM Hash of Previous Block Header

8f434...9b2dc327aa4

Nonce

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC



Hash Function



Block 101

11:01 PM Hash of Previous Block Header

Hash of Transactions

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC Block n

Block Header

Hunter -> Kyle 0.2 BTC Megan -> Ryan 13 BTC Justin -> Jose 7 BTC

V

8f434...9b2dc327aa4

Block Header Detail (5/5)

Block 100

10:49 PM
Hash of Previous
Block Header

8f434...9b2dc327aa4

Nonce

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC Block 101

11:01 PM
Hash of Previous
Block Header

0466d...ae8376bbc67

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC Block n

Block Header

Hash of the Previous Block Header

Block 100

10:49 PM

19d7c...0723301e493

8f434...9b2dc327aa4

Nonce

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC

Block 101

11:01 PM

Hash of Previous Block Header

0466d...ae8376bbc67

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC

Block n

Block Header

Block 101 Process: See Block 100 (1/4)

Block 100

10:49 PM

19d7c...0723301e493

8f434...9b2dc327aa4

Nonce

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC

Block 101

11:01 PM

Hash of Previous Block Header

0466d...ae8376bbc67

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC

Block n

Block Header

Block 101 Process: See Block 100 (2/4)

Block 100

10:49 PM

19d7c...0723301e493

8f434...9b2dc327aa4

Nonce

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC

Block 101

11:01 PM

Hash of Previous Block Header

0466d...ae8376bbc67

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC

Block n

Block Header

Hunter -> Kyle 0.2 BTC Megan -> Ryan 13 BTC Justin -> Jose 7 BTC

Hash Function



d5cc1...0f95ecfdd413

Block 101 Process: See Block 100 (3/4)

Block 100

10:49 PM

19d7c...0723301e493

8f434...9b2dc327aa4

Nonce

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC

Block 101

11:01 PM

d5cc1...0f95ecfdd413

0466d...ae8376bbc67

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC

Block n

Block Header

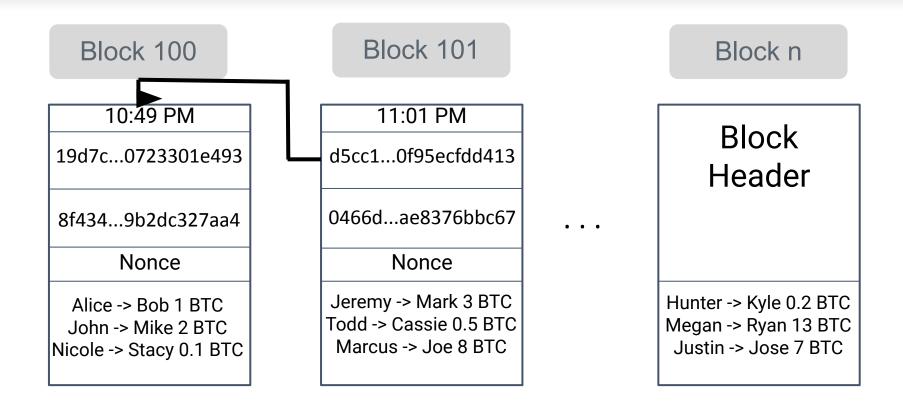
Hunter -> Kyle 0.2 BTC Megan -> Ryan 13 BTC Justin -> Jose 7 BTC

Hash Function

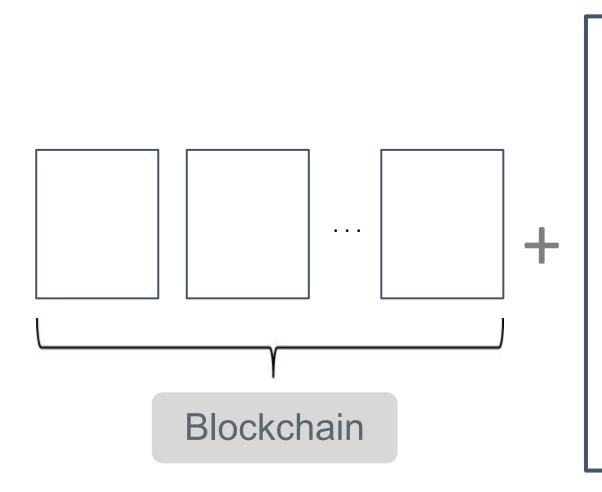


d5cc1...0f95ecfdd413

Block 101 Process: See Block 100 (4/4)



Back to the Big Picture (1/2)



Alice: 5 BTC
Bob: 2 BTC
John: 21 BTC
Joe: 1 BTC
Amy: 0.6 BTC
Leslie: 43 BTC

•

.

Tim: 8 BTC
Nicole: 0.3 BTC
Jesse: 11 BTC
Steven: 17 BTC
Darren: 3 BTC

Janen.

) 1 RTC

Jose:

0.1 BTC

Back to the Big Picture (2/2)

