

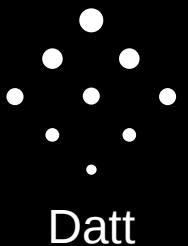
Transactions and Blocks in Bitwise Detail

Ryan X. Charles
Blockchain University
San Francisco, Oct. 26 – Oct. 30, 2015



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
<https://github.com/ryanxcharles/blockchain-university>



Outline

Blockchain Overview

Number Formats

Public Keys, Signatures, & Addresses

Inputs & Outputs

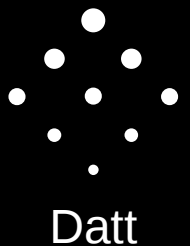
Transactions

Blocks



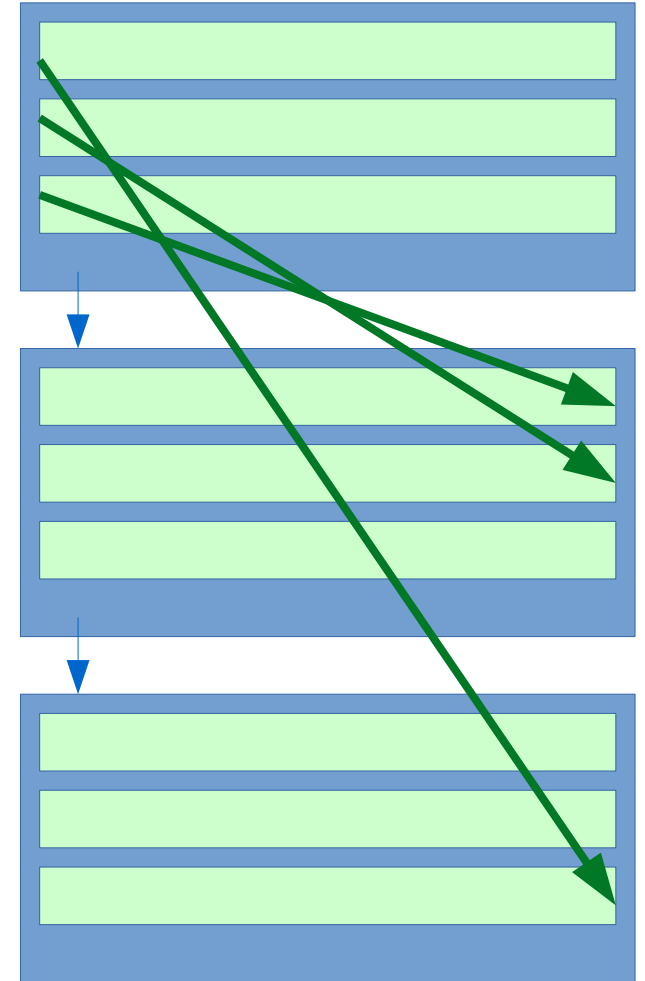
Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
<https://github.com/ryanxcharles/blockchain-university>



Blockchain Overview

- Blocks contain transactions and a proof-of-work hash
- Each block links to previous block
- Each transaction links to outputs of earlier transactions



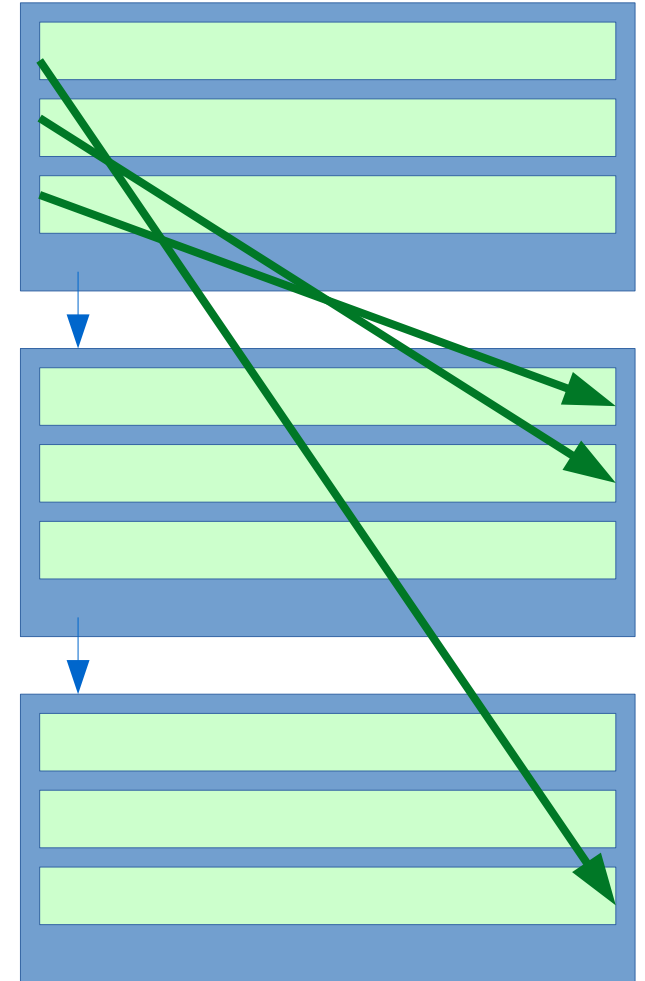
Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
<https://github.com/ryanxcharles/blockchain-university>



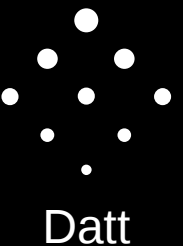
Blockchain Overview

- Genesis Block:
 - The First Block
- Coinbase Transaction:
 - First transaction in a block
 - Mining reward
 - Has “null” inputs



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
<https://github.com/ryanxcharles/blockchain-university>



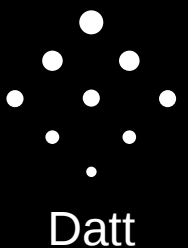
Blockchain Overview

- Each block has:
 - Proof-of-Work Hash (PoW)
 - Nonce
 - Meta data and transactions
- Example PoW with data “test data”
 - Nonce: 0, Hash: `df59bb7272f144dc7d3620e6f9e14234`
 - Nonce: 1, Hash: `460142d2a0349c13a48b422261d708eb`
 - Nonce: 2, Hash: `71be158053f58c9e1f094fb3f7da282e`
 - ...
 - Nonce: 146, Hash: `00f82186722b46b2adb57f321793e44f`



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
<https://github.com/ryanxcharles/blockchain-university>



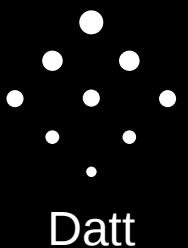
Blockchain Overview

- Each block has:
 - Proof-of-Work Hash (PoW)
 - Nonce
 - Meta data and transactions
- Example PoW with data “test data”
 - Nonce: 0, Hash: `df59bb7272f144dc7d3620e6f9e14234`
 - Nonce: 1, Hash: `460142d2a0349c13a48b422261d708eb`
 - Nonce: 2, Hash: `71be158053f58c9e1f094fb3f7da282e`
 - ...
 - Nonce: 146, Hash: `00f82186722b46b2adb57f321793e44f`

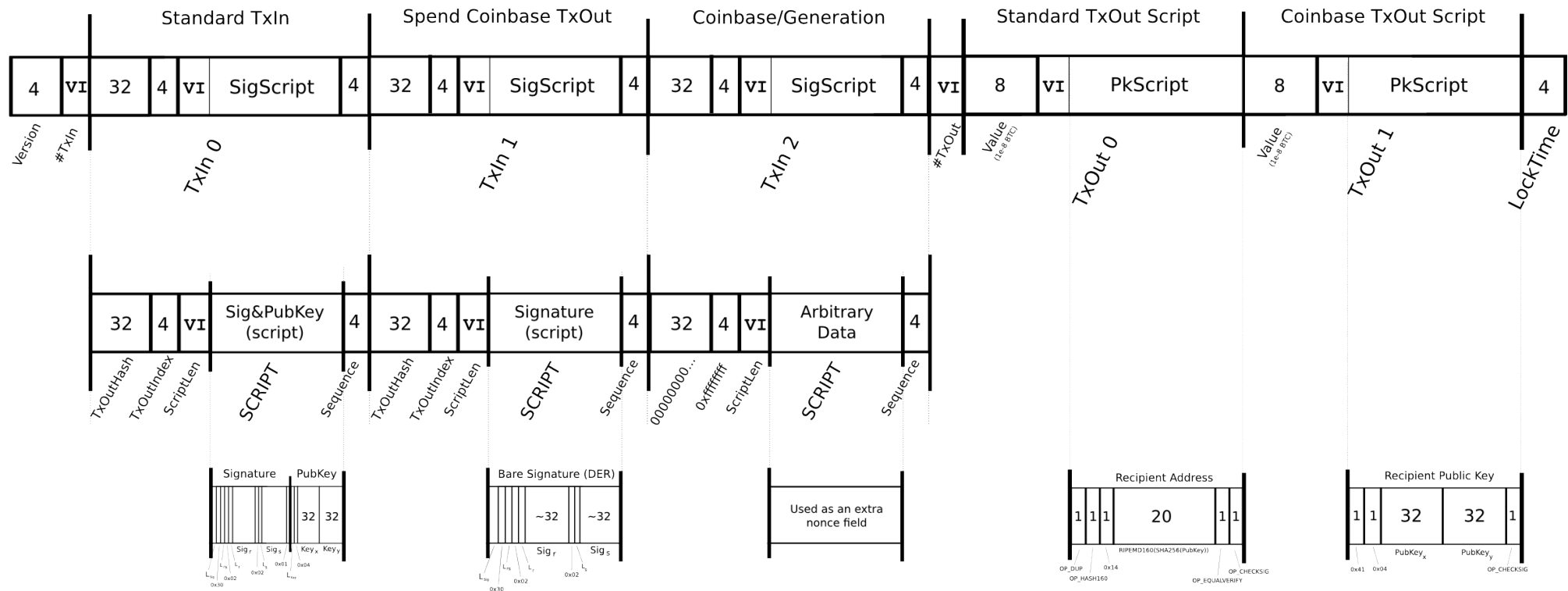


Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
<https://github.com/ryanxcharles/blockchain-university>



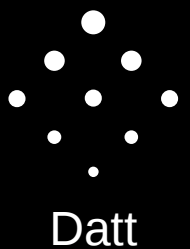
Transaction Detail Overview



Summary: Transactions have inputs and outputs. Plot by Alan Rainer.

Ryan X. Charles
 Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
<https://github.com/ryanxcharles/blockchain-university>



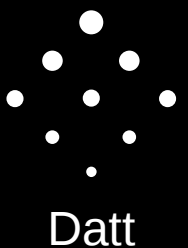
Blockchain Overview

- Each block has:
 - Proof-of-Work Hash (PoW)
 - Nonce
 - Meta data and transactions
- Example PoW with data “test data”
 - Nonce: 0, Hash: `df59bb7272f144dc7d3620e6f9e14234`
 - Nonce: 1, Hash: `460142d2a0349c13a48b422261d708eb`
 - Nonce: 2, Hash: `71be158053f58c9e1f094fb3f7da282e`
 - ...
 - Nonce: 146, Hash: `00f82186722b46b2adb57f321793e44f`



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
<https://github.com/ryanxcharles/blockchain-university>



Number Formats

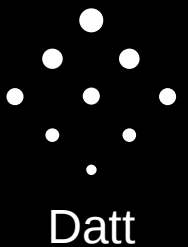
Which number format does bitcoin use?

- Big endian
- Little endian
- Sign+magnitude
- Two's complement
- Fixed point
- Floating point
- String
- 8 bit
- 16 bit
- 32 bit
- 64 bit
- 256 bit
- Custom variable size
- Another variable size



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
<https://github.com/ryanxcharles/blockchain-university>



Number Formats

Which number format does bitcoin use?

- Big endian
- Little endian
- Sign+magnitude
- Two's complement
- Fixed point
- Floating point
- String
- 8 bit
- 16 bit
- 32 bit
- 64 bit
- 256 bit
- Custom variable size
- Another variable size

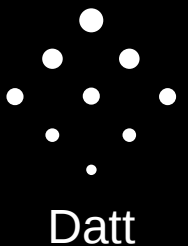
All of them.

Ryan X. Charles

Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:

<https://github.com/ryanxcharles/blockchain-university>



Datt