7CCSMDLC: Distributed Ledgers & Cryptocurrencies

Lecture 2: Cryptography

Peter McBurney
Professor of Computer Science
Department of Informatics
King’s College London

Email: peter.mcburney@kcl.ac.uk

2021

Outline for today

- Cryptography & Hashing
- Operations of the Bitcoin Blockchain

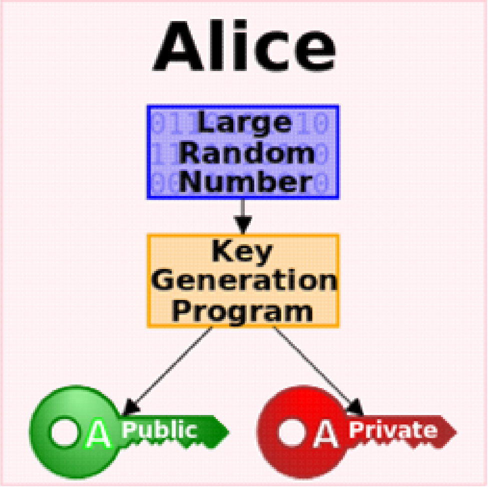
Licence terms

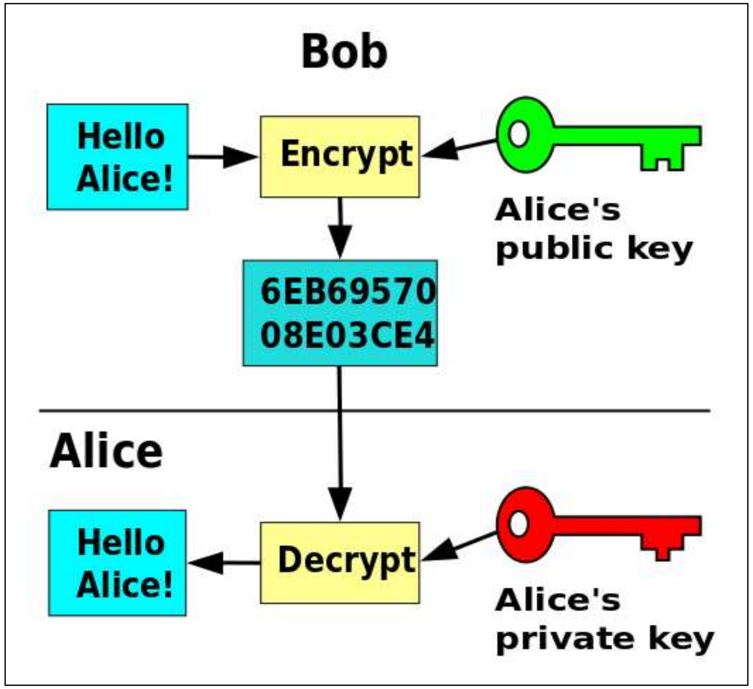
- Unless otherwise stated, the diagrams are taken from:
  - Andreas Antonopoulos [2017]: *Mastering Bitcoin.* 2nd Edition. O'Reilly.
  - Version on Github at:

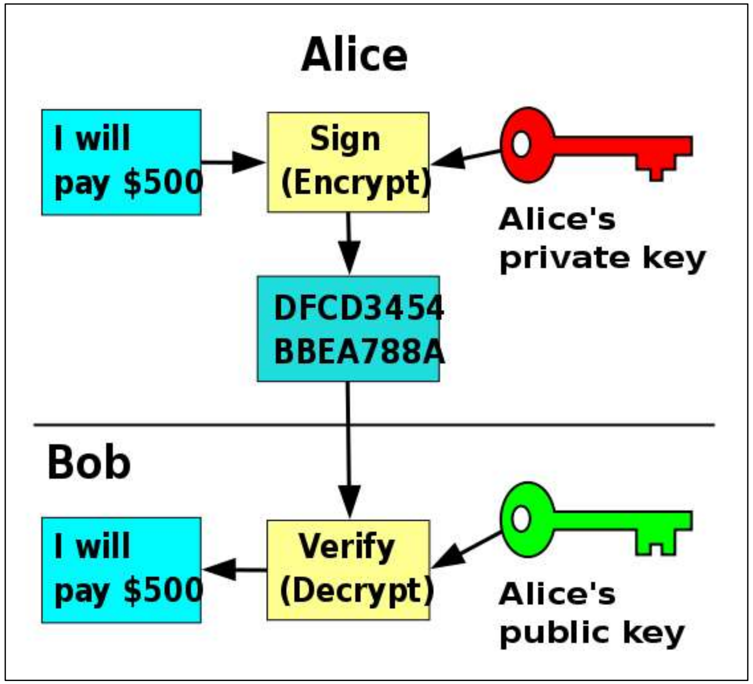
    https://github.com/bitcoinbook/bitcoinbook/
- The licence allowing this is the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.
  - A copy of this license is at: http://creativecommons.org/licenses/by-nc-nd/4.0/
- Any subsequent use of this content is under this this licence.

Cryptography & Hashing

Public & Private Keys







Source: WikiBooks: Communications & Networking

Hashing

- Converts a digital object of arbitrary length (eg, a document, an image) into a single string of fixed length (a hash)
  - Not continuous
    - Two similar documents result in very different hashes.
  - Very hard to reverse engineer
  - Thus, a form of encryption.

See examples next slide.

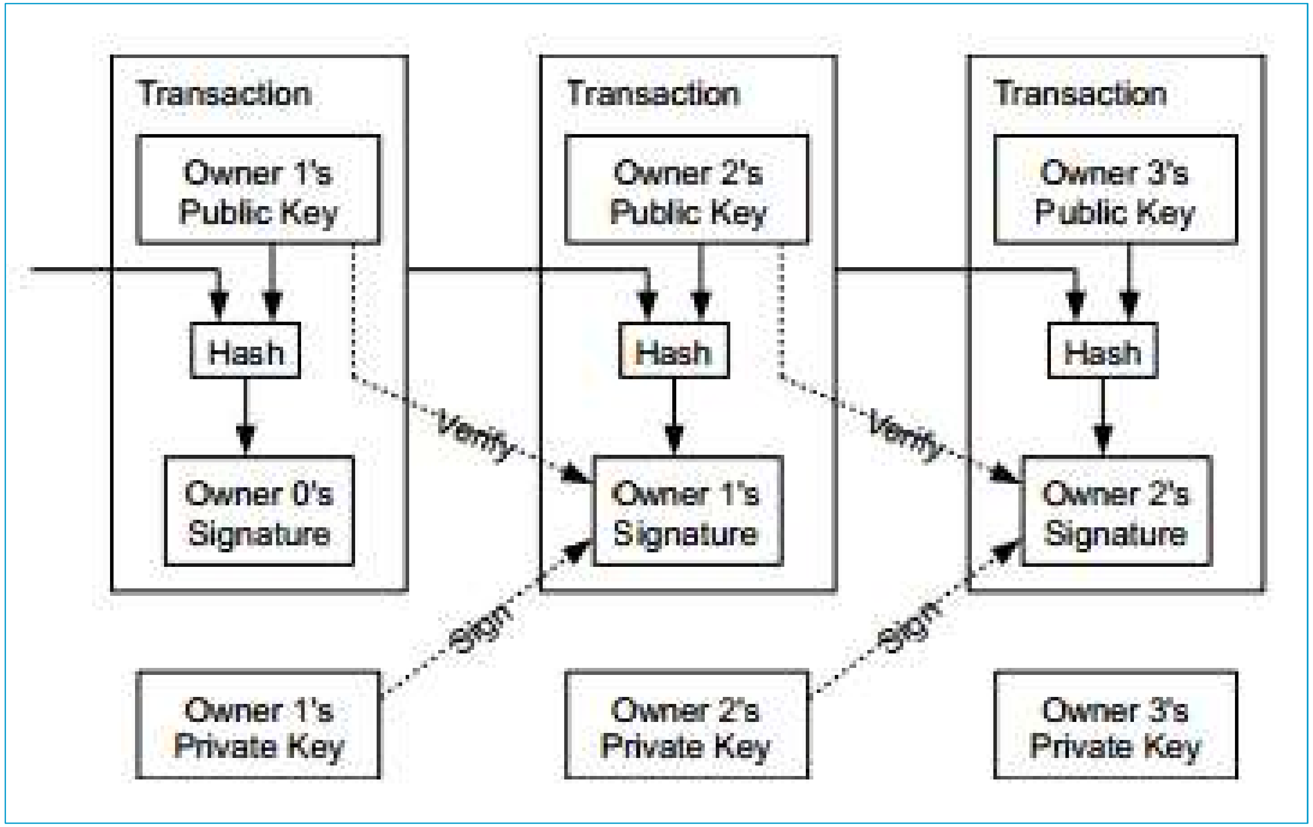
Hashing in Bitcoin blockchain:

- Hashing of public keys for bitcoin address
- Encryption of private keys
- The work for Proof-of-Work (PoW) (hashcash algorithm)
- Each block contains hash of the merkle root of the transactions in that block.
- Each block contains hash of the header of the previous block
- Payloads may be hashed.

Examples of hashing similar phrases

```
I am Satoshi Nakamoto0 => a80a81401765c8eddee25df36728d732...
I am Satoshi Nakamoto1 => f7bc9a6304a4647bb41241a677b5345f...
I am Satoshi Nakamoto2 => ea758a8134b115298a1583ffb80ae629...
I am Satoshi Nakamoto3 => bfa9779618ff072c903d773de30c99bd...
I am Satoshi Nakamoto4 => bce8564de9a83c18c31944a66bde992f...
I am Satoshi Nakamoto5 => eb362c3cf3479be0a97a20163589038e...
I am Satoshi Nakamoto6 => 4a2fd48e3be420d0d28e202360cfbaba...
I am Satoshi Nakamoto7 => 790b5a1349a5f2b909bf74d0d166b17a...
I am Satoshi Nakamoto8 => 702c45e5b15aa54b625d68dd947f1597...
I am Satoshi Nakamoto9 => 7007cf7dd40f5e933cd89fff5b791ff0...
I am Satoshi Nakamoto10 => c2f38c81992f4614206a21537bd634a...
I am Satoshi Nakamoto11 => 7045da6ed8a914690f087690e1e8d66...
I am Satoshi Nakamoto12 => 60f01db30c1a0d4cbce2b4b22e88b9b...
I am Satoshi Nakamoto13 => 0ebc56d59a34f5082aaef3d66b37a66...
I am Satoshi Nakamoto14 => 27ead1ca85da66981fd9da01a8c6816...
I am Satoshi Nakamoto15 => 394809fb809c5f83ce97ab554a2812c...
```

Hashing used to chain blocks together



Source: Nakamoto 2008

Bitcoin "address"

A bitcoin address is a string of 26-35 alphanumeric characters in Base58Check encoding, beginning with the number 1 or 3:

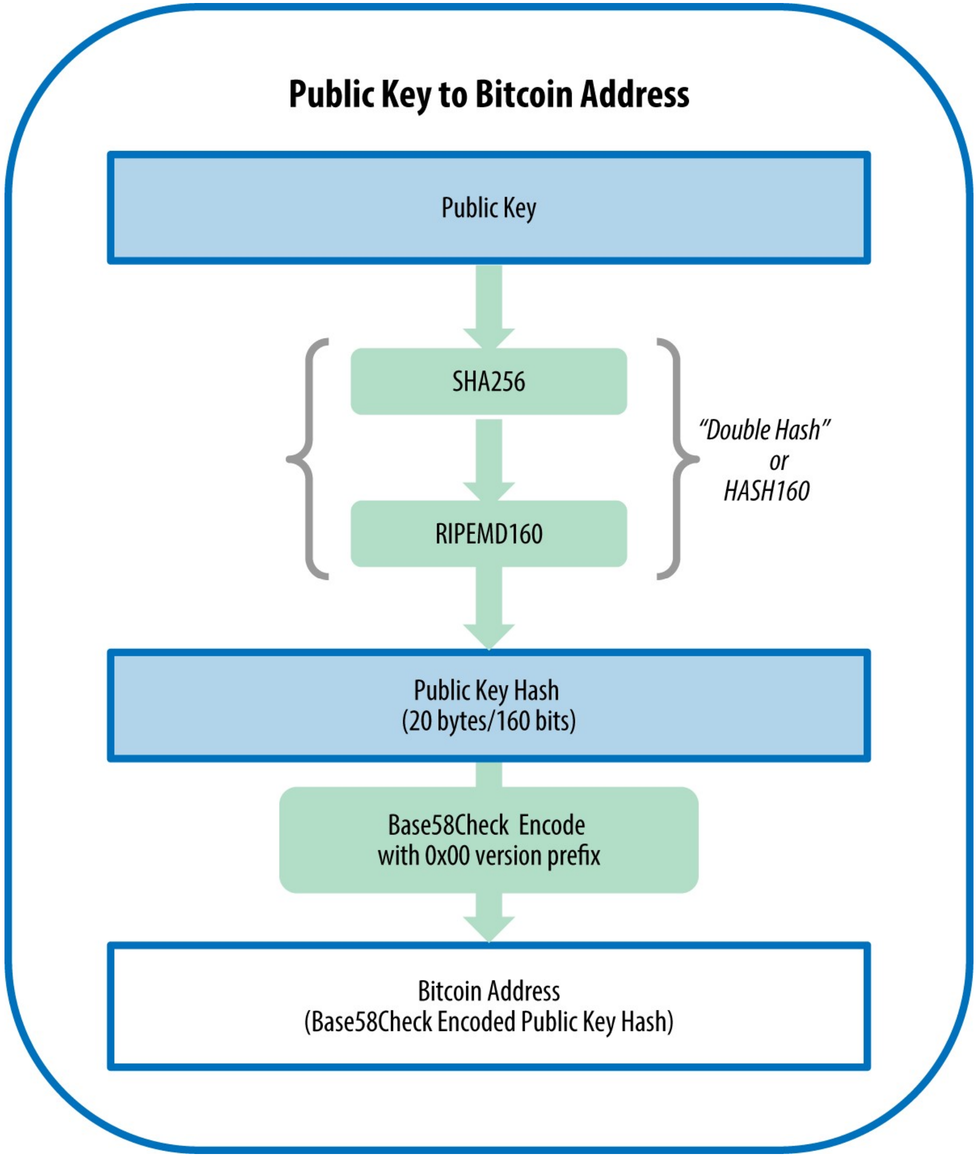
1DSrfJdB2AnWaFNgSbv3MZC2m74996JafV

or

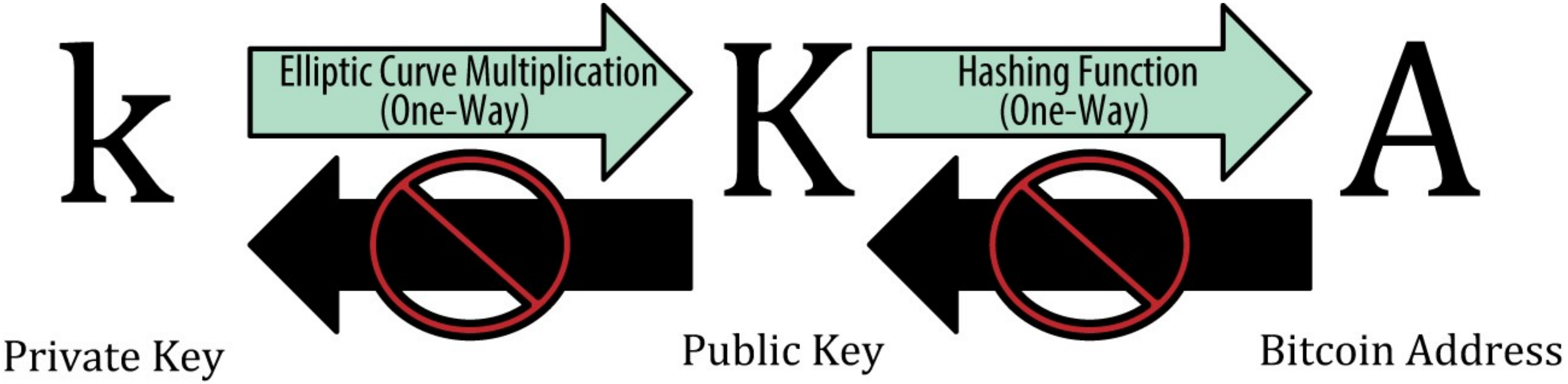
3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

- It is a hash of a public key or the hash of a script.
- Two common types of transaction pay to such addresses:
  - P2PKH (Pay-to-Public-Key-Hash)
  - P2SH (Pay-to-Script-Hash)
- The address represents the destination of a payment, and acts to redeem the encumbrance of a payment.

Public key conversion to Bitcoin address



Private and public keys and Bitcoin address



k

Elliptic Curve Multiplication (One-Way)

K

Hashing Function (One-Way)

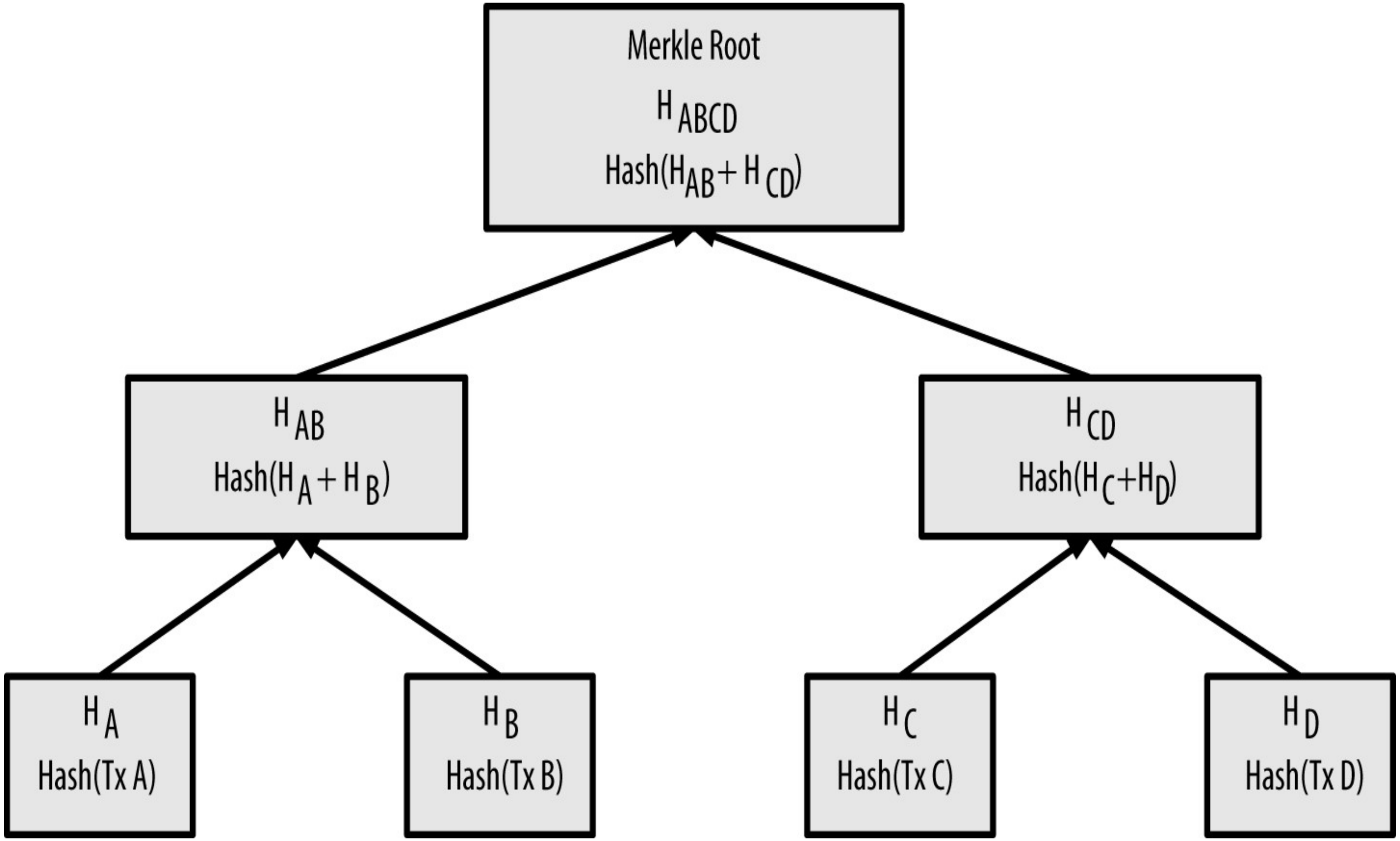
A

Private Key

Public Key

Bitcoin Address

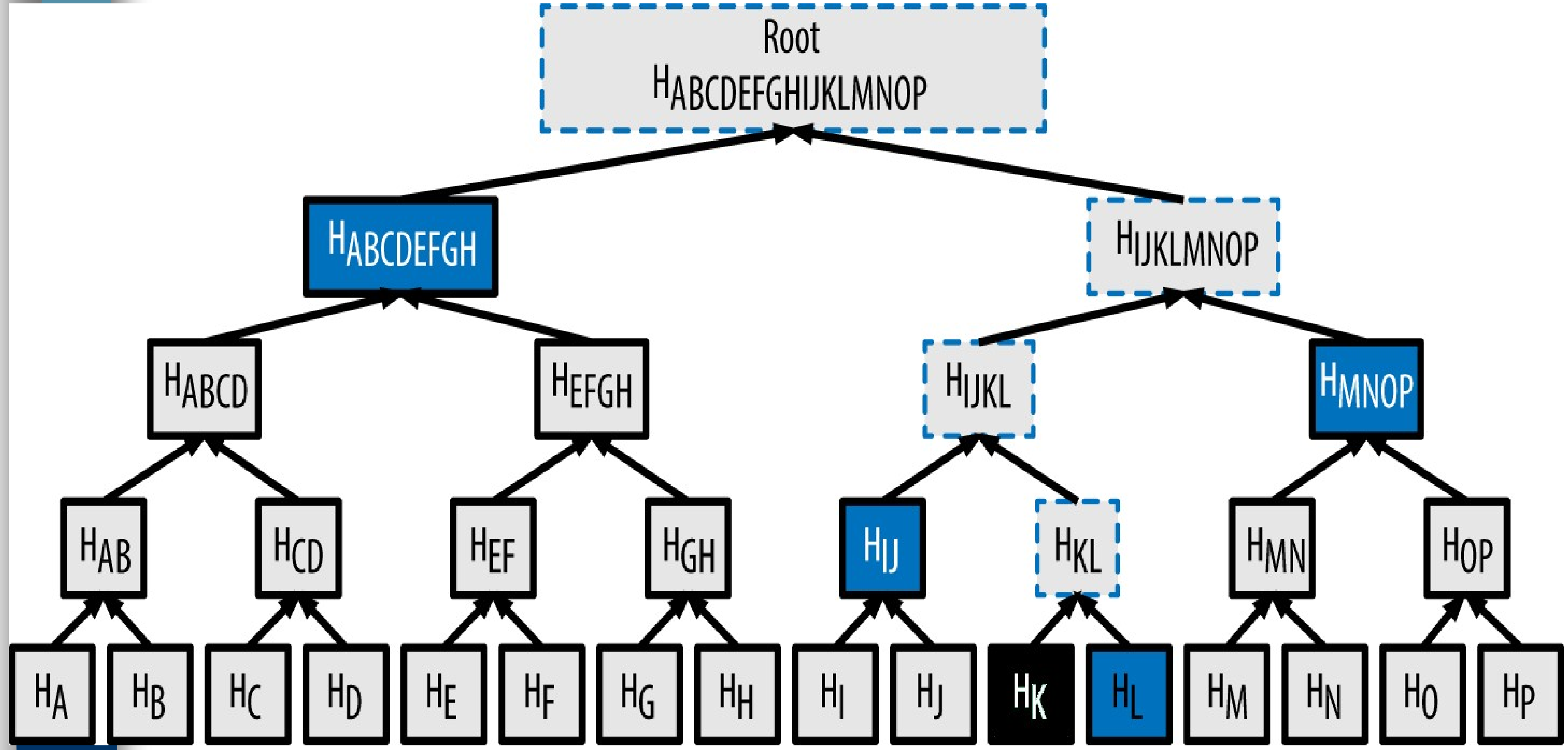
Merkle Tree



Key: TxA stands for Transaction A

Merkle path

To prove transaction K included in hash, need only provide 4 hashes (each 32 bytes long): hashes for L, IJ, MNOP & ABCDEFGH.



Operation of the Bitcoin Blockchain

Bitcoin blockchain - Components

- Bitcoin
  - 1 satoshi = 10^-8 Bitcoin = 0.00000001 Bitcoin = smallest possible unit
  - 1 Bitcoin = 100 million satoshis
  - 1 MilliBit = 0.001 Bitcoin =100,000 satoshis

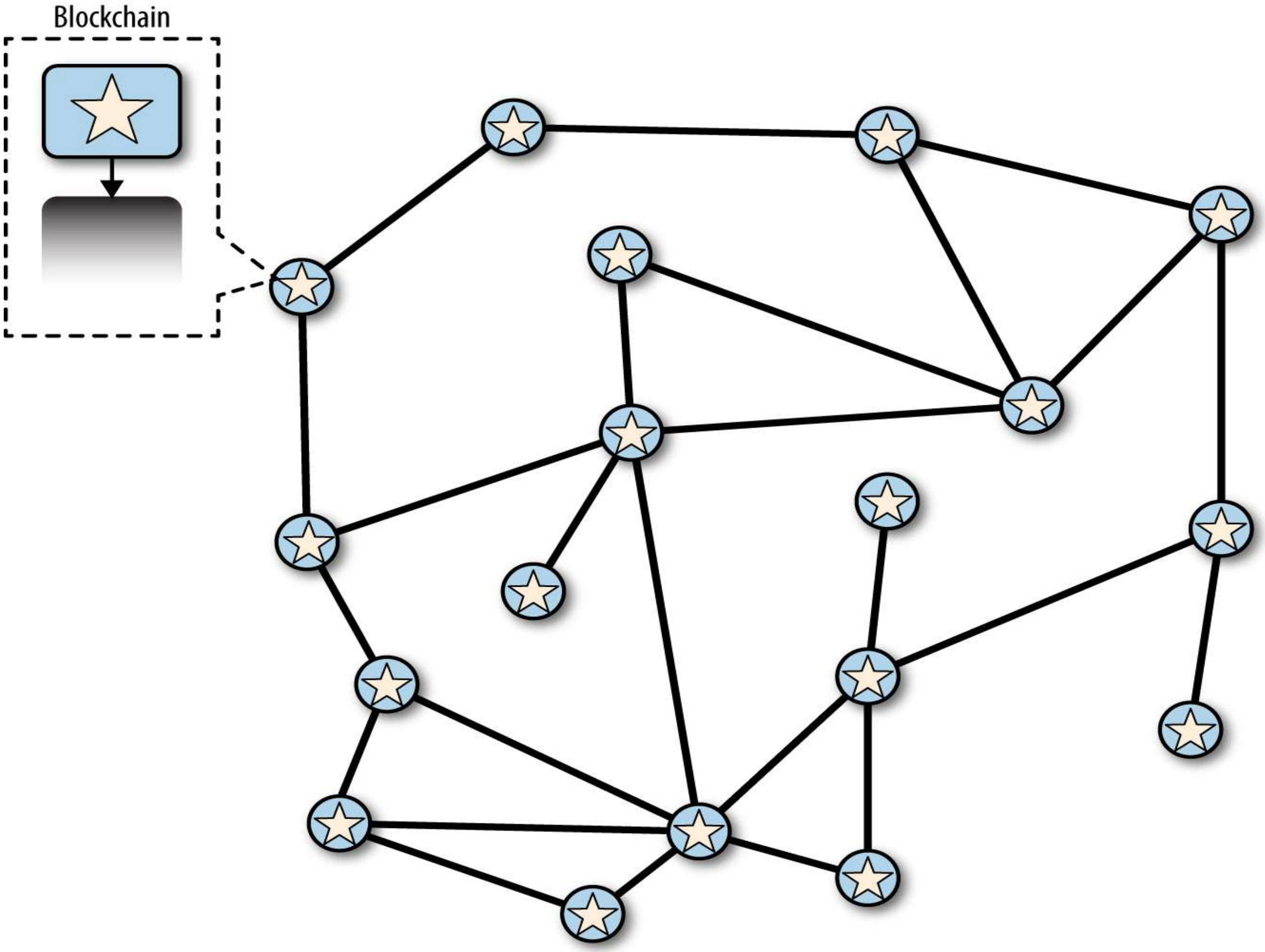
- Total number of BTC to be issued: 2,099,999,997,690,000 satoshis
  - Almost 21 million BTC
  - Will be achieved in ca. 2140 (13.4 million blocks)
  - Current number of BTC mined: 18,606,406.25 BTC

Components:

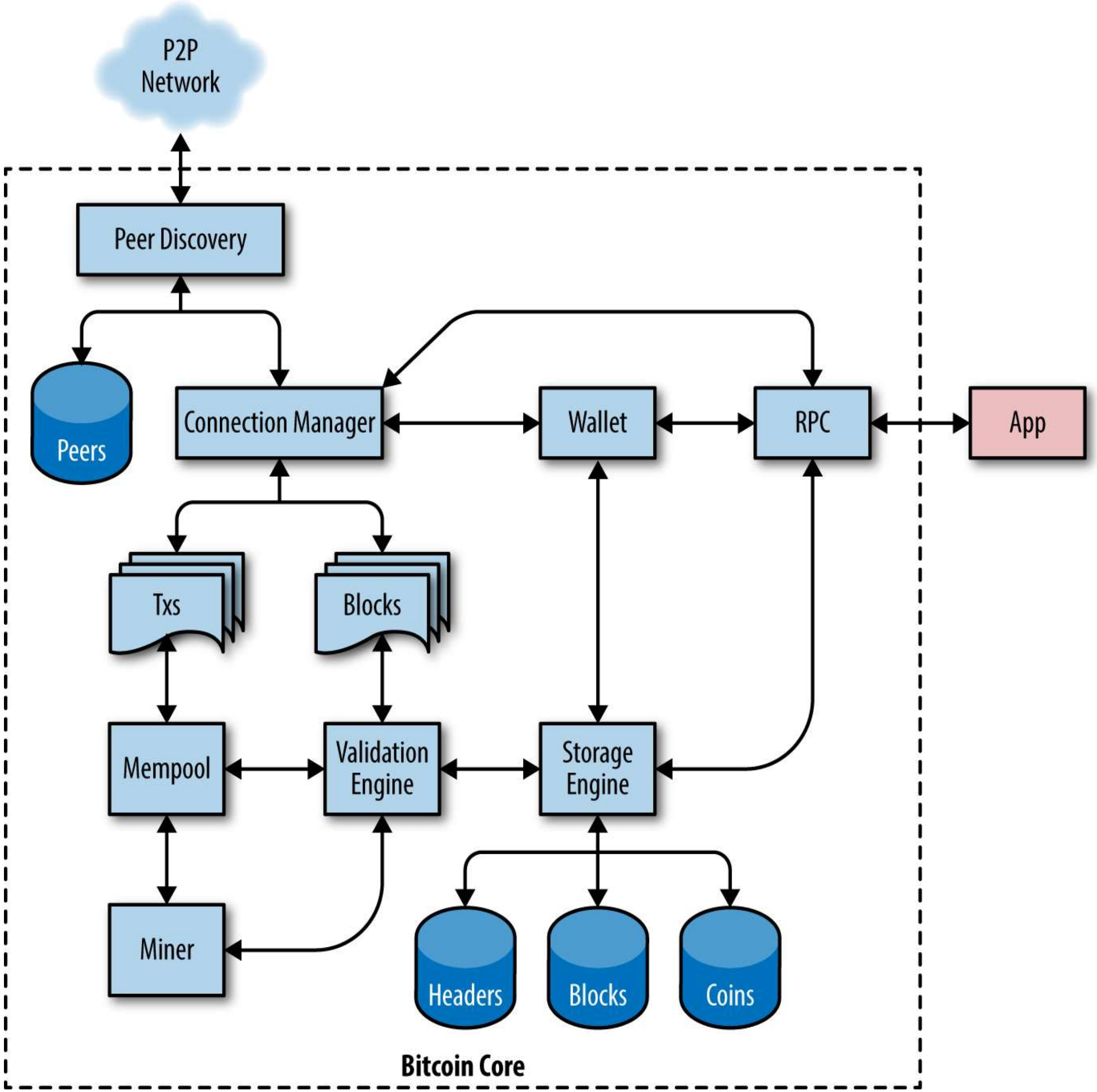
- Users with wallets
- Transactions
- Miners
- Light vs. full clients.

Blockchain assumes a peer-to-peer (P2P) network

No node is in control.



Bitcoin core



Bitcoin Scripting Language: Script

- Called “**Script**”
  - Reverse-Polish notation stack-based execution language
  - Instead of (3+5) X 2, we write 35+2X
  - The syntax of Script is like that of the programming language Forth

- Two stack operations:
  - **Push** (adds an item to the top of the stack)
  - **Pop** (removes the item at the top of the stack)

- Items are processed left to right
  - Eg: OP_ADD
    - Pops two items from stack, adds them, and pushes sum to stack.

Script 2

- Script is deliberately simple & widely applicable
  - Not hardware dependent
  - Enables execution on devices with limited memory (eg, embedded devices)
  - Stateless
    - No state prior to execution, no state saved after execution

- Deliberately does not permit loops or complex program control features
  - This means predictable execution times
  - No infinite loops
  - Makes attacks more difficult
  - Not Turing-complete.

- Ethereum was developed to allow Turing-complete computation over a blockchain.

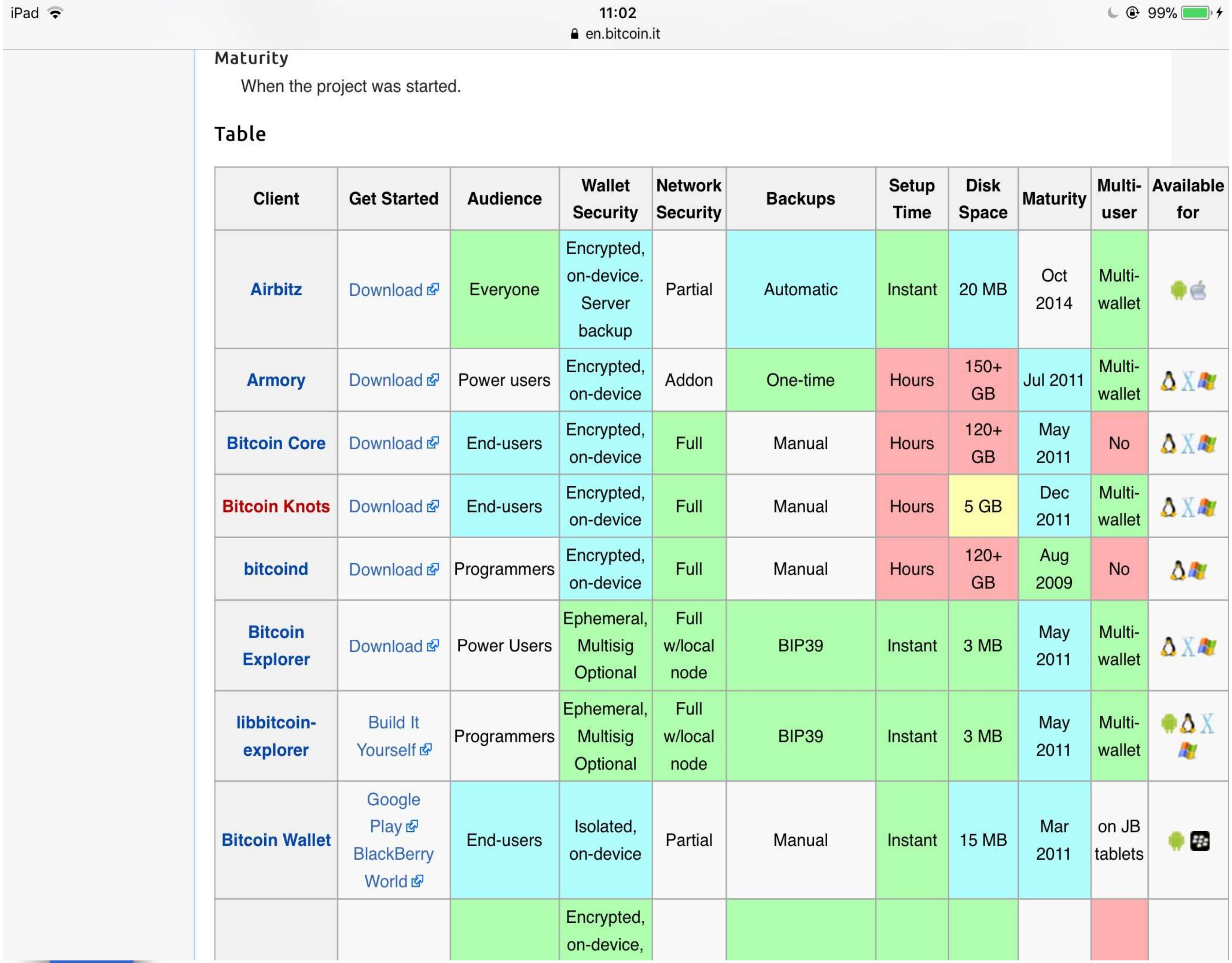
Wallets

- Wallet is the primary user interface
  - Controls access to a user’s bitcoin
  - Manages keys and addresses
  - Tracks current balance
  - Enables creation and signing of transactions.

- May be held on client machine or on an exchange

- Wallet can keep a copy of the transaction
  - Or can query the chain when needed

- Wallet also refers to the data structure used to store and manage a user’s keys and address.



Maturity

When the project was started.

Table

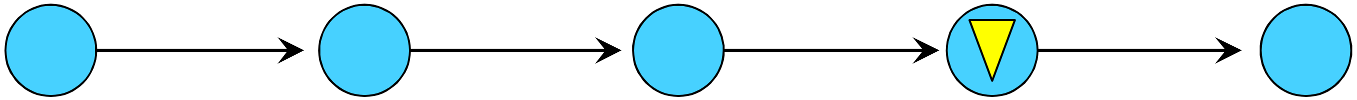
Client	Get Started	Audience	Wallet Security	Network Security	Backups	Setup Time	Disk Space	Maturity	Multi-user	Available for
Airbitz	Download	Everyone	Encrypted, on-device. Server backup	Partial	Automatic	Instant	20 MB	Oct 2014	Multi-wallet	🤖
Armory	Download	Power users	Encrypted, on-device	Addon	One-time	Hours	150+ GB	Jul 2011	Multi-wallet	🐧 X ⊞
Bitcoin Core	Download	End-users	Encrypted, on-device	Full	Manual	Hours	120+ GB	May 2011	No	🐧 X ⊞
Bitcoin Knots	Download	End-users	Encrypted, on-device	Full	Manual	Hours	5 GB	Dec 2011	Multi-wallet	🐧 X ⊞
bitcoind	Download	Programmers	Encrypted, on-device	Full	Manual	Hours	120+ GB	Aug 2009	No	🐧 ⊞
Bitcoin Explorer	Download	Power Users	Ephemeral, Multisig Optional	Full w/local node	BIP39	Instant	3 MB	May 2011	Multi-wallet	🐧 X ⊞
libbitcoin-explorer	Build It Yourself	Programmers	Ephemeral, Multisig Optional	Full w/local node	BIP39	Instant	3 MB	May 2011	Multi-wallet	🤖 🐧 X ⊞
Bitcoin Wallet	Google Play BlackBerry World	End-users	Isolated, on-device	Partial	Manual	Instant	15 MB	Mar 2011	on JB tablets	🤖 ⁂
			Encrypted, on-device,							

Source: https://en.bitcoin.it/wiki/Clients

Processing of Transactions

Any node

Miners



Origination

Broadcast

Validation of transaction and propagation

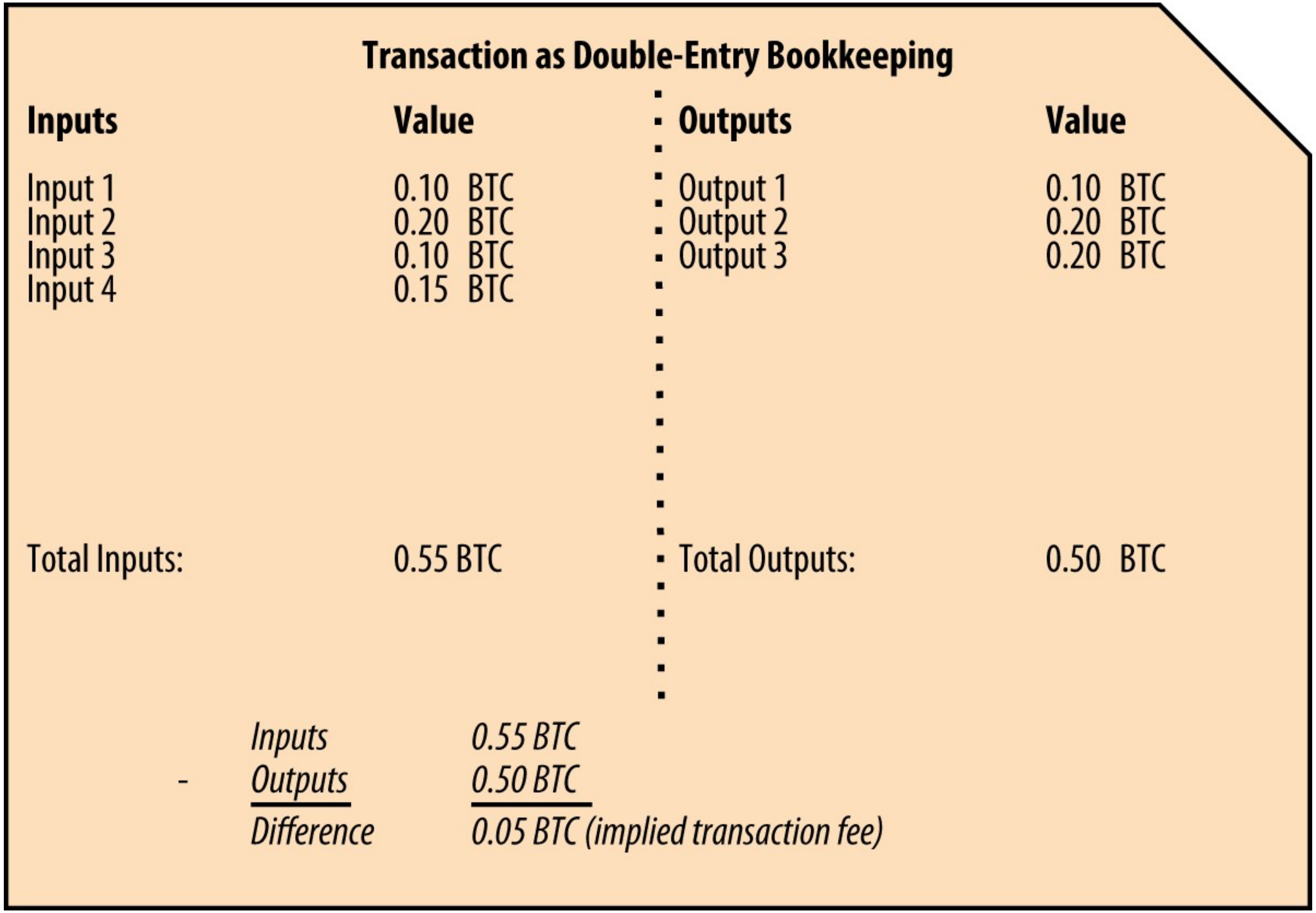
Transactions aggregated into Block and PoW

Validation of block and Confirmation

Transactions

- Transactions move value from inputs to outputs
- A transaction has at least 1 input and at least 1 output
- If the Value of Outputs < Value of Inputs
  - Implied difference between outputs and inputs is taken by the miner as a fee for processing the transaction

Transactions as inputs and outputs

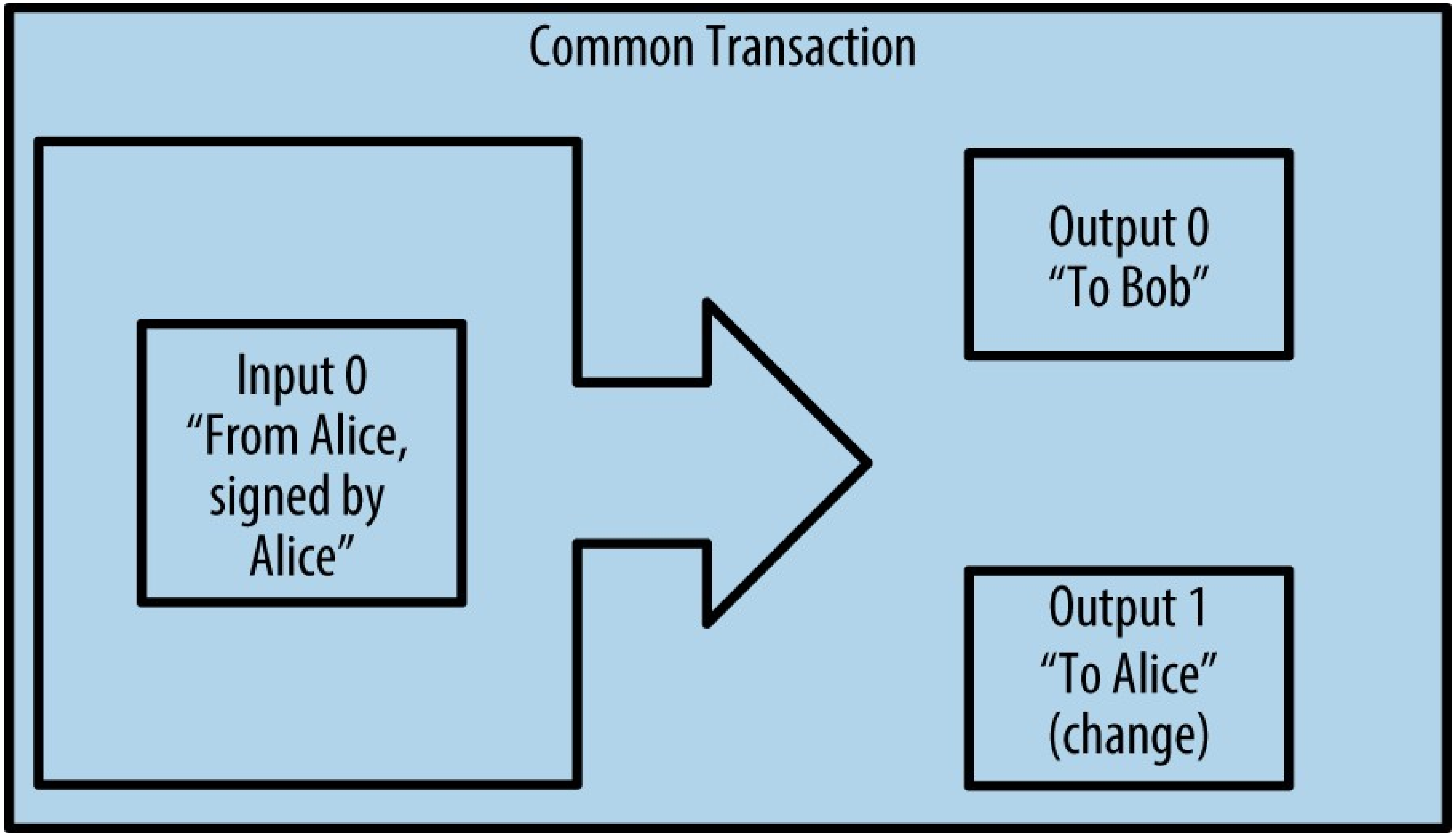


Transaction as Double-Entry Bookkeeping

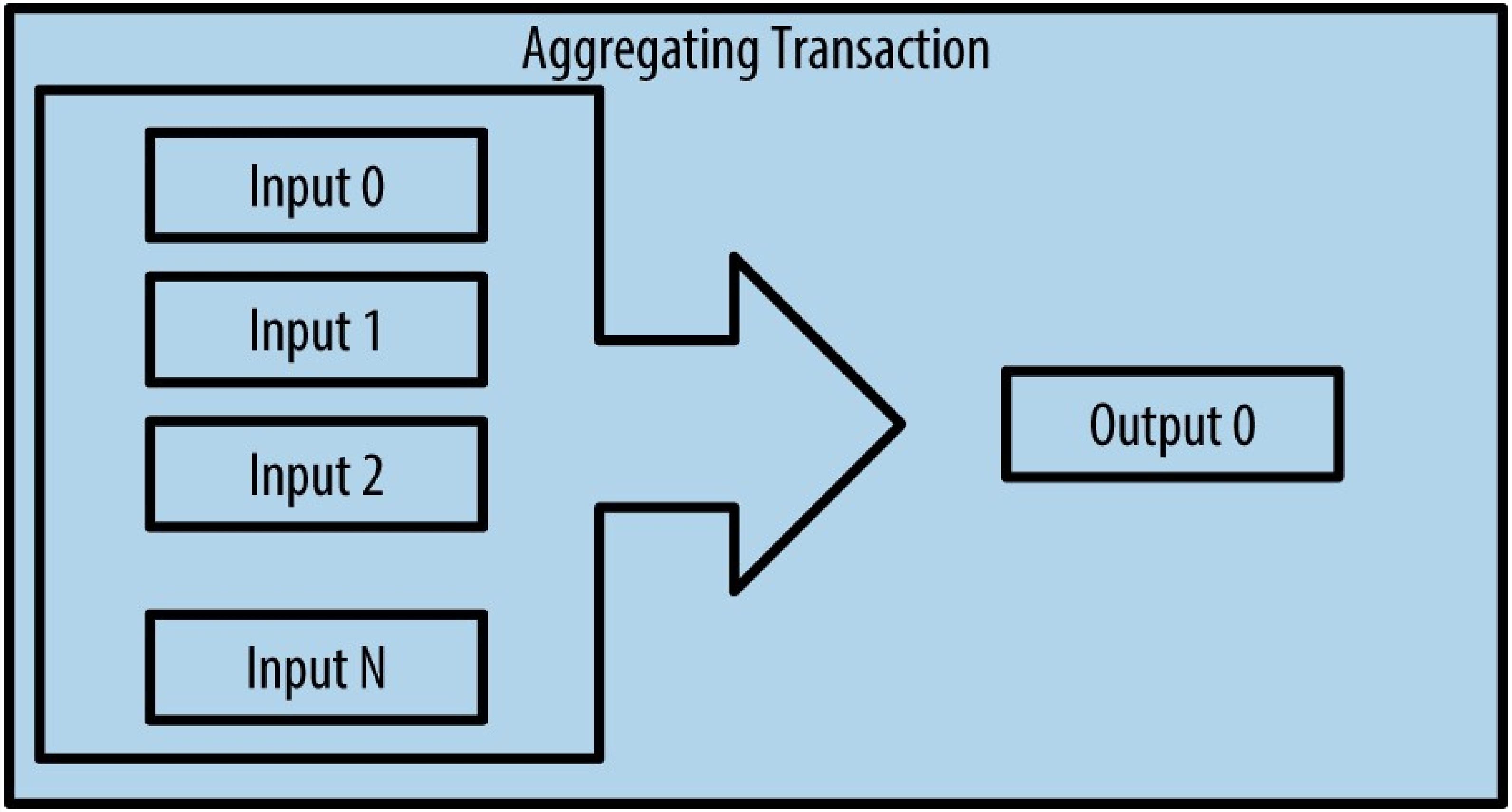
Inputs	**Value**	**Outputs**	**Value**
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC

	Inputs	*0.55 BTC*
-	*Outputs*	*0.50 BTC*
	Difference	*0.05 BTC (implied transaction fee)*

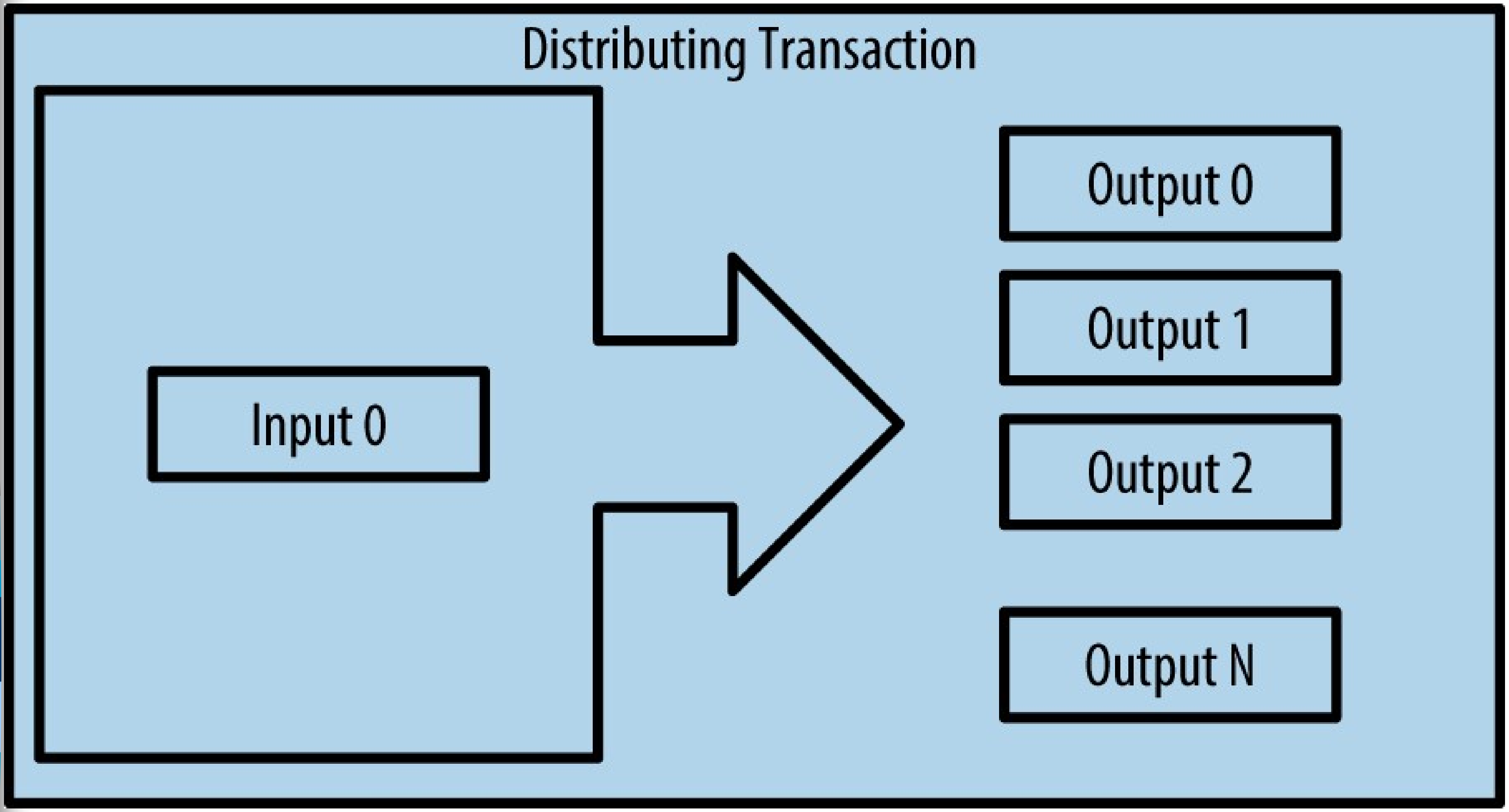
Common transaction: one to one plus change



Transaction aggregating funds: Many to one



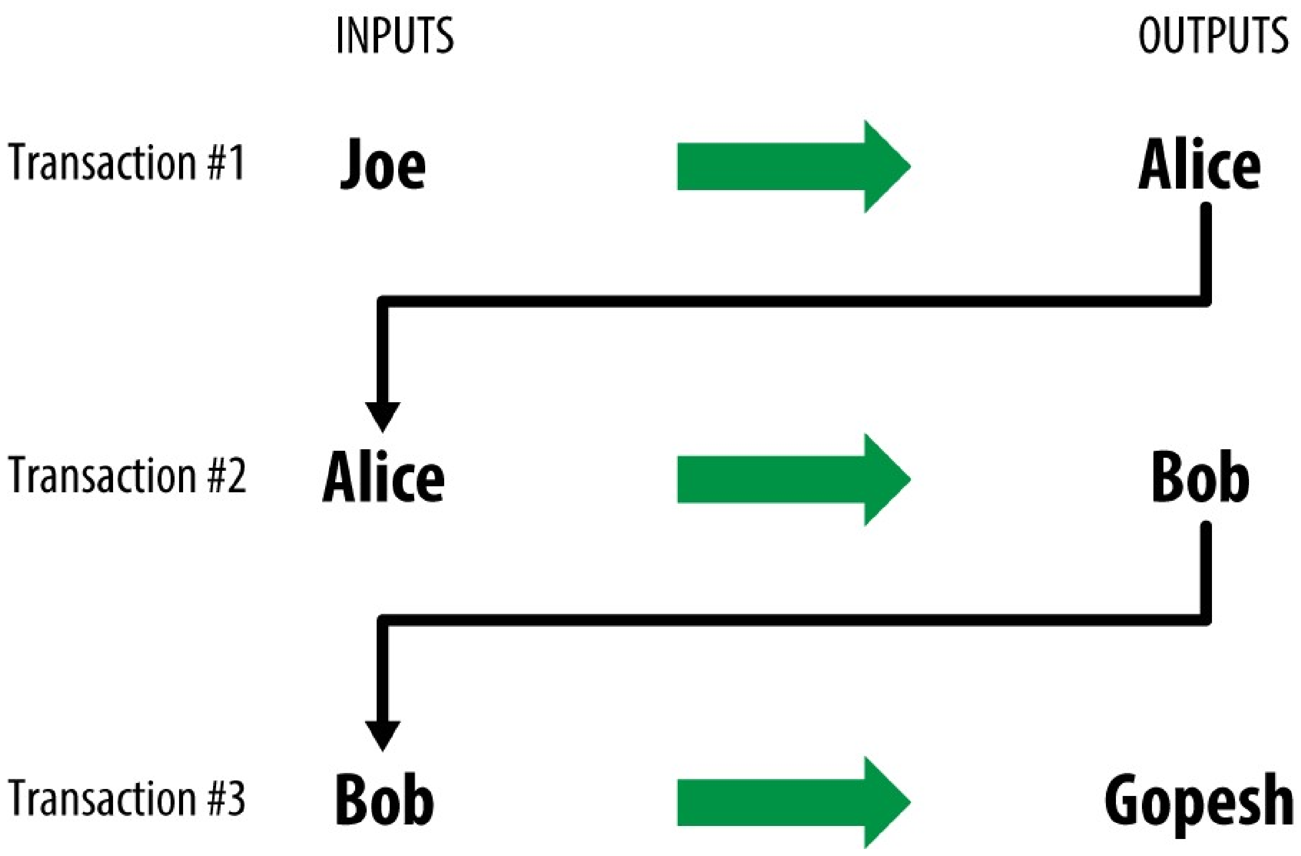
Transaction distributing funds: one to many



Metaphor – Mixing buckets of water

Images: West Roane County Fire Department

A sequence of transactions



INPUTS

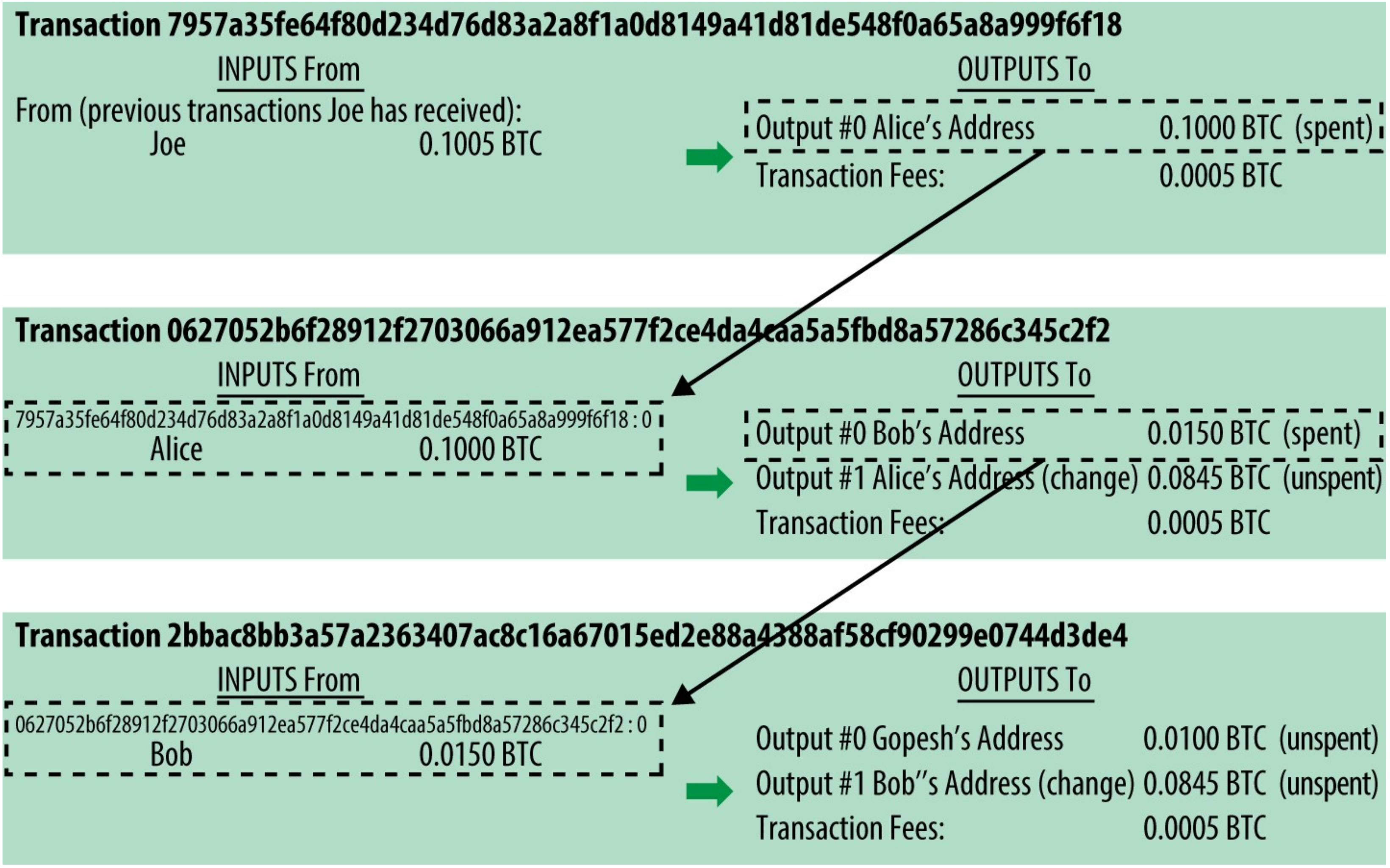
OUTPUTS

Transaction #1 Joe Alice

Transaction #2 Alice Bob

Transaction #3 Bob Gopesh

A chain of transactions: Joe to Alice to Bob to Gopesh



Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18

INPUTS From

From (previous transactions Joe has received):
Joe 0.1005 BTC

OUTPUTS To

Output #0 Alice's Address 0.1000 BTC (spent)
Transaction Fees: 0.0005 BTC

Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

INPUTS From

7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0
Alice 0.1000 BTC

OUTPUTS To

Output #0 Bob's Address 0.0150 BTC (spent)
Output #1 Alice's Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC

Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4

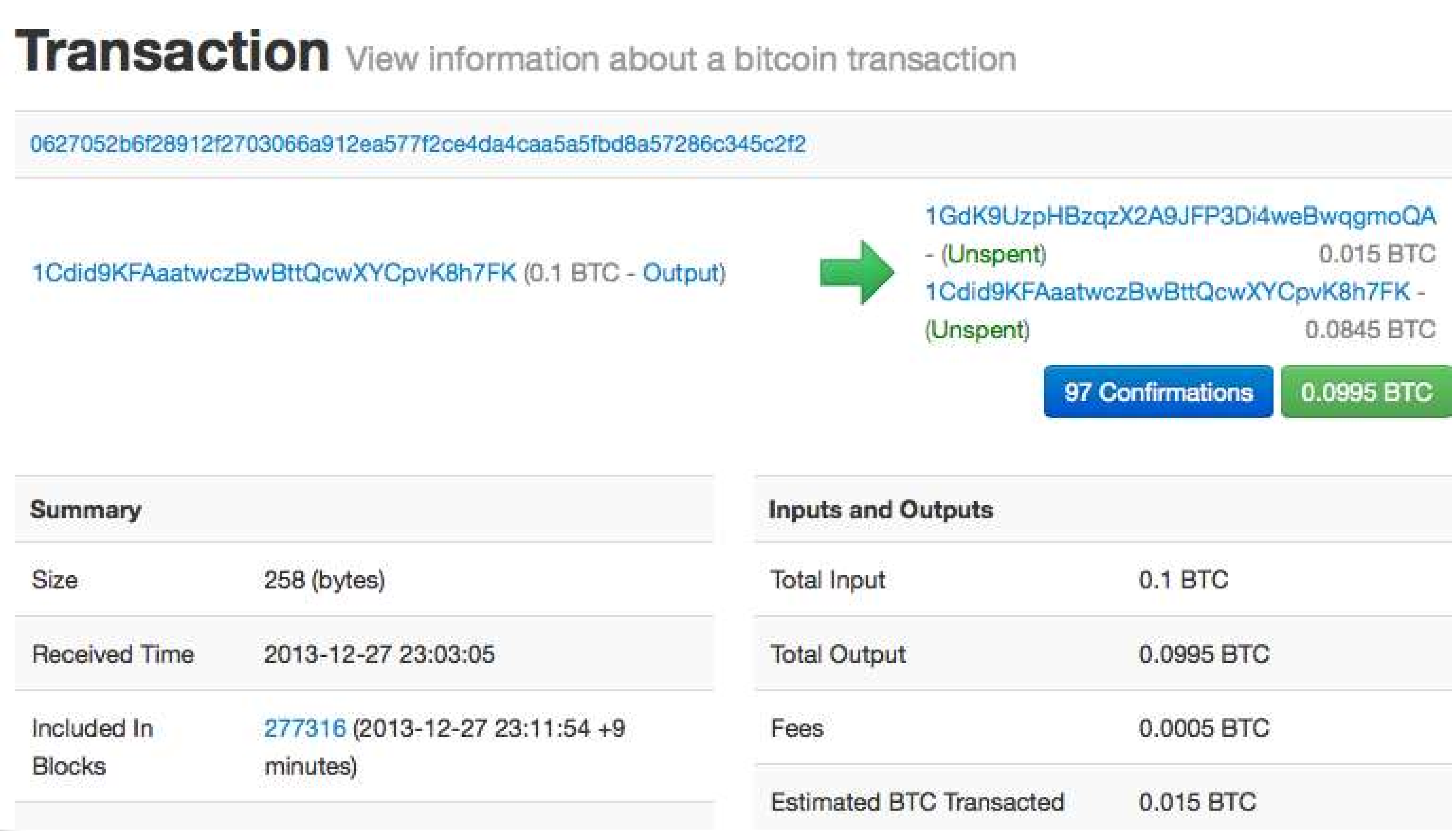
INPUTS From

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0
Bob 0.0150 BTC

OUTPUTS To

Output #0 Gopesh's Address 0.0100 BTC (unspent)
Output #1 Bob''s Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC

Transactions – block explorer view



Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Output)

→

1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (Unspent) 0.015 BTC

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (Unspent) 0.0845 BTC

97 Confirmations

0.0995 BTC

Summary	
Size	258 (bytes)
Received Time	2013-12-27 23:03:05
Included In Blocks	277316 (2013-12-27 23:11:54 +9 minutes)

Inputs and Outputs	
Total Input	0.1 BTC
Total Output	0.0995 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.015 BTC

Thank you!

peter.mcburney@kcl.ac.uk