Crypto in Bitcoin

Bob Cowles

CERN Academic Lecture Series
December 2, 2014

Why Crypto

Crypto gives us confidentiality and integrity

- Confidentiality – protect from unauthorized reading
- Integrity – protect from unauthorized alteration

The primary use of crypto in Bitcoin is integrity

- Protect the wallet from alteration
- Protect transactions from alteration
- Protect the blockchain from alteration
- Authenticate wallet ownership

Major crypto families

Symmetric encryption

- Single shared key

Asymmetric encryption

- Public and private key

Hashing

- One-way functions – like extended checksum

All are used in implementing digital currencies

Characteristics of good crypto

Efficient …. (or not)

Small changes in input produce large changes in output

Standardized and vetted

- Only the key is secret, not the code

Always used from a good, publicly available library

Unbroken

- Required brute force to find key

Computationally difficult to reverse

- Requires solving a “hard problem”

Symmetric Encryption

Alice and Bob want to communicate privately

Lockbox example

Alice and Bob both have a key that locks or unlocks the lock on the lockbox

In the digital case, assuming a secure algorithm, key distribution a major problem

The key management problem

What happens if we want to include Lois in the communication? But only some of the time?

The key distribution problem grows exponentially with the number of securely communicating groups

Solved by Diffe-Hellman’s key exchange solution, but requires asymmetric encryption and “real-time” exchange to establish a shared key.

Lockboxes and Padlocks

Back to Alice and Bob and the lockbox – One potential solution is two keys, one for Bob, one for Alice.

This solves (reduces) the key problem at the expense of lockboxes!

What if we use padlocks instead of built-in locks on the lockboxes? Yes? No?

What if we use “special padlocks” ?

Asymmetric Encryption

Involve mathematical problems currently hard to solve

- Factoring large numbers
- https://en.wikipedia.org/wiki/RSA_(cryptosystem)
- The elliptic curve discrete algorithm problem
- https://en.wikipedia.org/wiki/Elliptic_curve_cryptography

Each entity has two keys – one public, one private

- At one level, similar to userid and password, but different
- Lock with one key, unlock with the other

Review the Alice and Bob story

Hash

Four properties of a cryptographic hash function: it is

1. easy to compute hash for any given message
2. infeasible to generate a message with a given hash
3. infeasible to modify a message without changing hash
4. infeasible to find two different messages with same hash

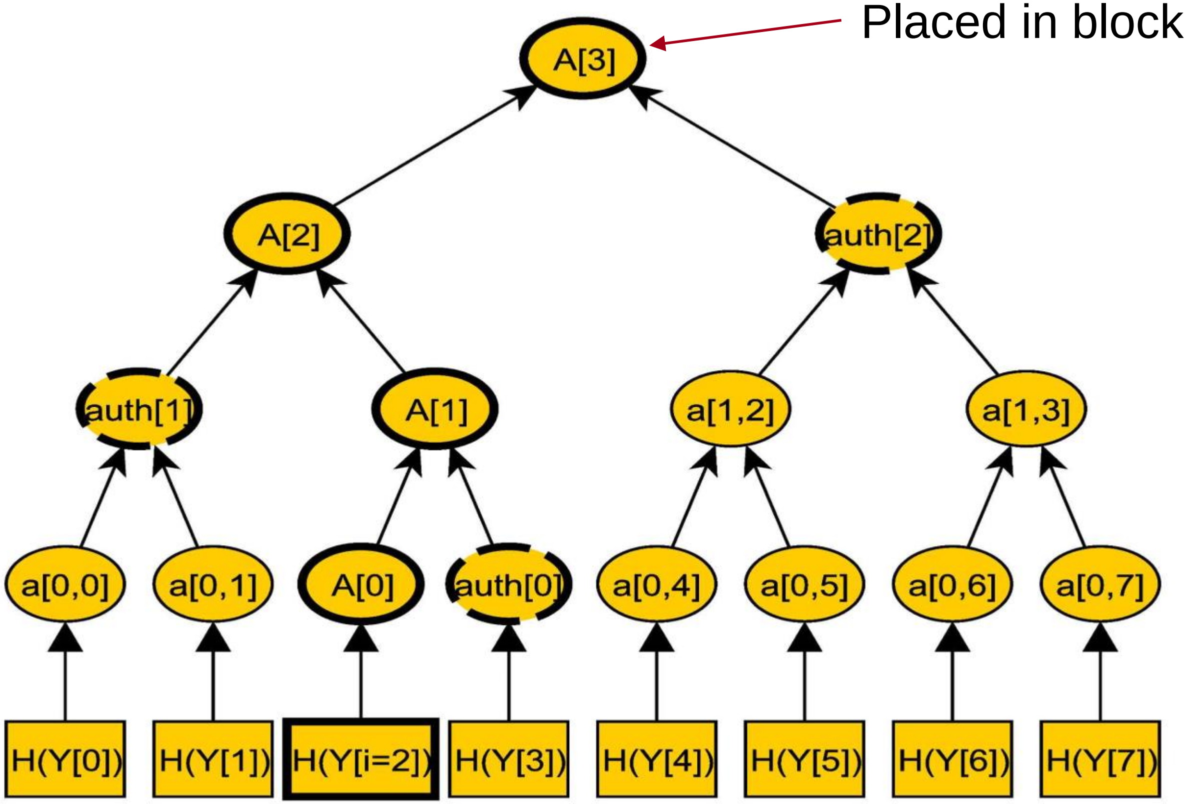
Used to

Ensure a message hasn’t changed

Verify passwords

Merkle Trees

Technique to generate a hash for a large number of messages and then be able to easily verify a particular message is included in the hash



Placed in block header

https://upload.wikimedia.org/wikipedia/commons/9/93/MerkleTree2.jpg

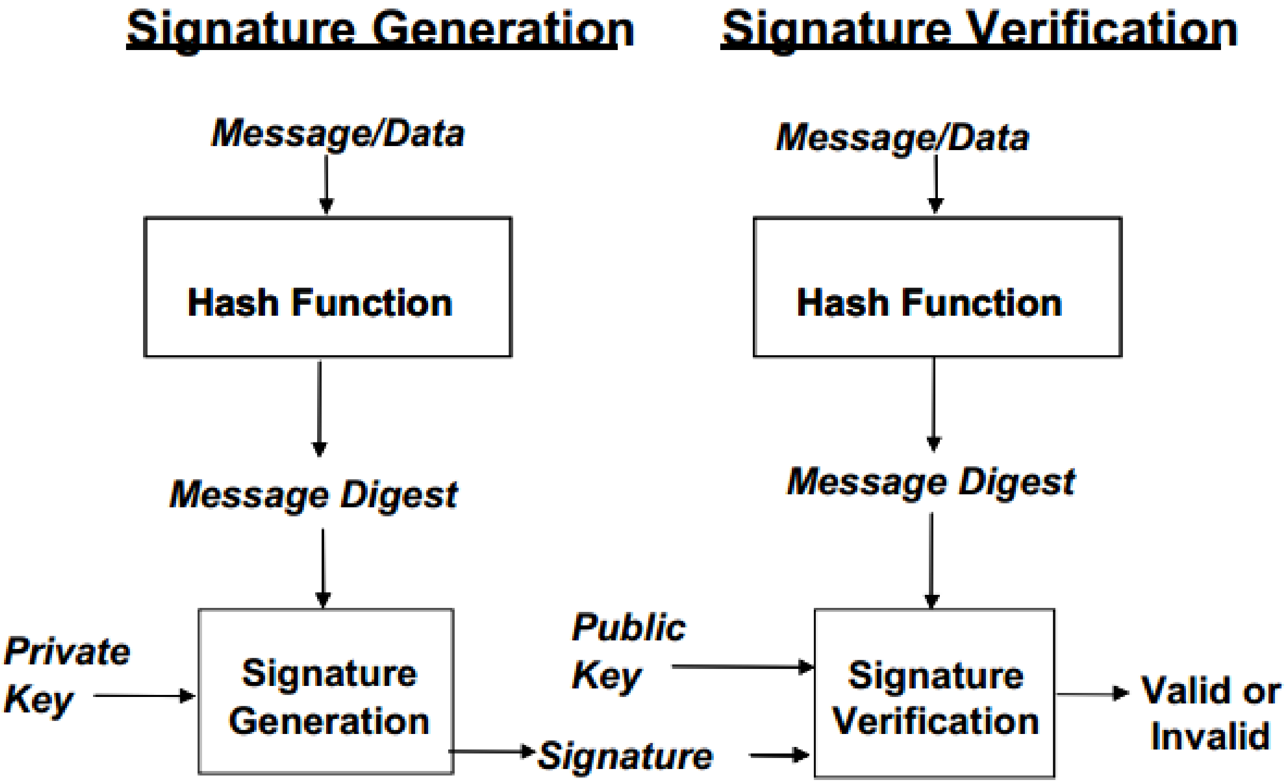
Digital Signatures

A valid digital signature gives a recipient reason to believe … the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity).

In the asymmetric encryption case, if we encrypt with our private key that proves it came from us. Inefficient!

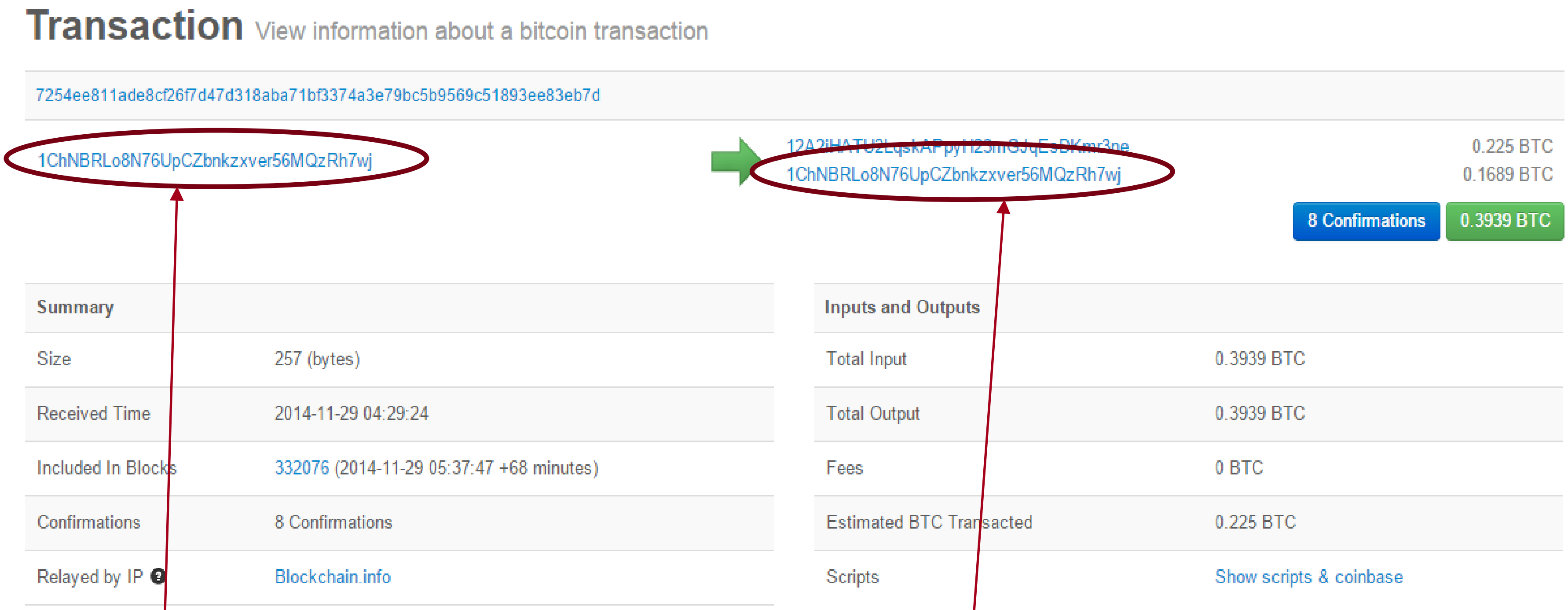
Instead, a Digital Signature Algorithm (DSA) is used and incorporated cryptographic hashes

DSA



http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

Bitcoin Transaction   http://blockchain.info



Transaction View information about a bitcoin transaction

7254ee811ade8cf26f7d47d318aba71bf3374a3e79bc5b9569c51893ee83eb7d

1ChNBRLo8N76UpCZbnkzxver56MQzRh7wj

12A2iHATU2LqskAPpyH23mGJqEsDKmr3ne	0.225 BTC
1ChNBRLo8N76UpCZbnkzxver56MQzRh7wj	0.1689 BTC

8 Confirmations   0.3939 BTC

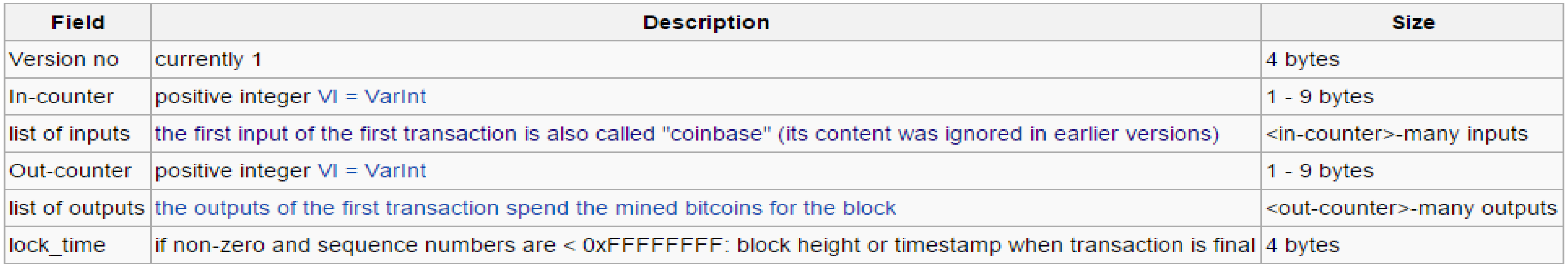
Summary	
Size	257 (bytes)
Received Time	2014-11-29 04:29:24
Included In Blocks	332076 (2014-11-29 05:37:47 +68 minutes)
Confirmations	8 Confirmations
Relayed by IP ❷	Blockchain.info

Inputs and Outputs	
Total Input	0.3939 BTC
Total Output	0.3939 BTC
Fees	0 BTC
Estimated BTC Transacted	0.225 BTC
Scripts	Show scripts & coinbase

“Previous-sent-to”, not “From” address
Sender supplied public key and signature
Includes “change back” to sender – similar to cash
First transaction is the “coinbase” transaction

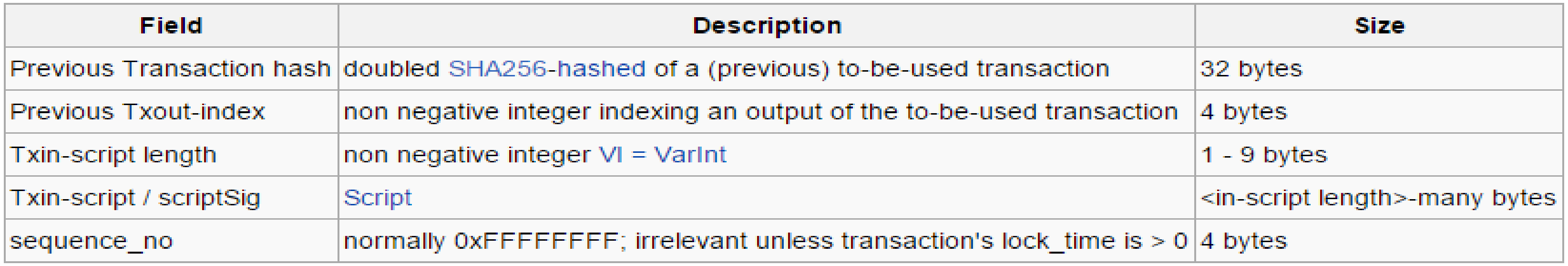
Transaction Format

General format   https://en.bitcoin.it/wiki/Transaction



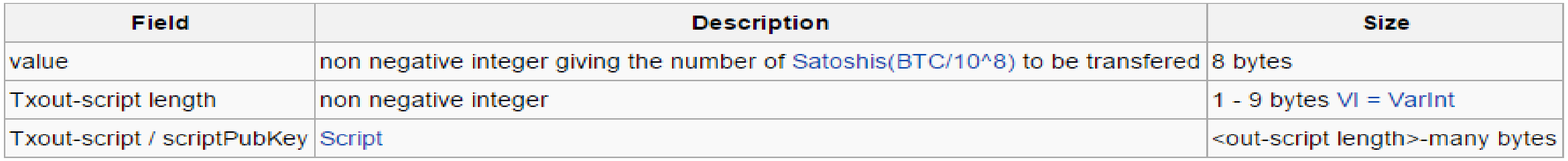
Field	Description	Size
Version no	currently 1	4 bytes
In-counter	positive integer VI = VarInt	1 - 9 bytes
list of inputs	the first input of the first transaction is also called "coinbase" (its content was ignored in earlier versions)	<in-counter>-many inputs
Out-counter	positive integer VI = VarInt	1 - 9 bytes
list of outputs	the outputs of the first transaction spend the mined bitcoins for the block	<out-counter>-many outputs
lock_time	if non-zero and sequence numbers are < 0xFFFFFFFF: block height or timestamp when transaction is final	4 bytes

Transaction Input



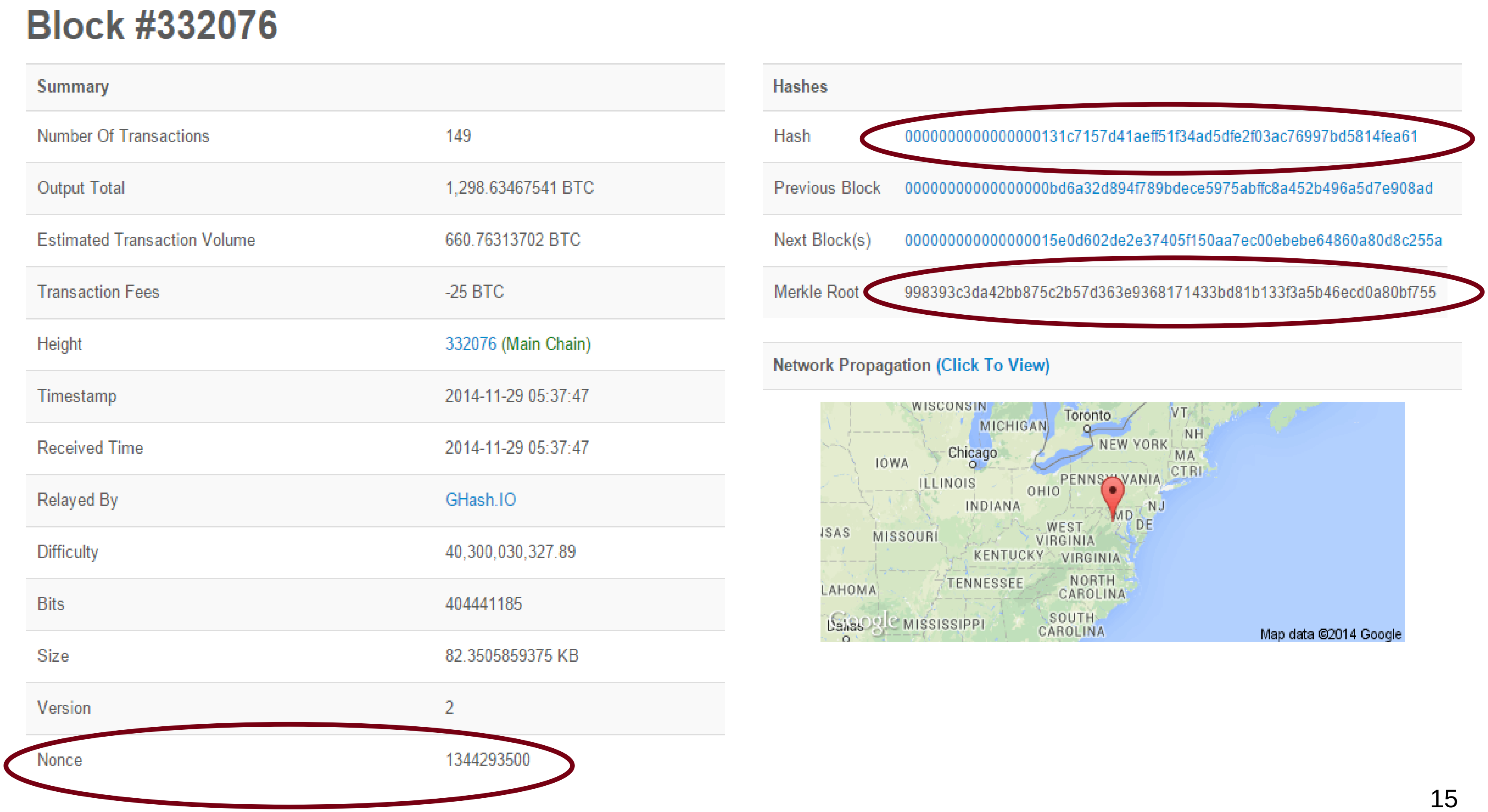
Field	Description	Size
Previous Transaction hash	doubled SHA256-hashed of a (previous) to-be-used transaction	32 bytes
Previous Txout-index	non negative integer indexing an output of the to-be-used transaction	4 bytes
Txin-script length	non negative integer VI = VarInt	1 - 9 bytes
Txin-script / scriptSig	Script	<in-script length>-many bytes
sequence_no	normally 0xFFFFFFFF; irrelevant unless transaction's lock_time is > 0	4 bytes

Transaction Output



Field	Description	Size
value	non negative integer giving the number of Satoshis(BTC/10^8) to be transfered	8 bytes
Txout-script length	non negative integer	1 - 9 bytes VI = VarInt
Txout-script / scriptPubKey	Script	<out-script length>-many bytes

Blockchain Block Header Information



Block #332076

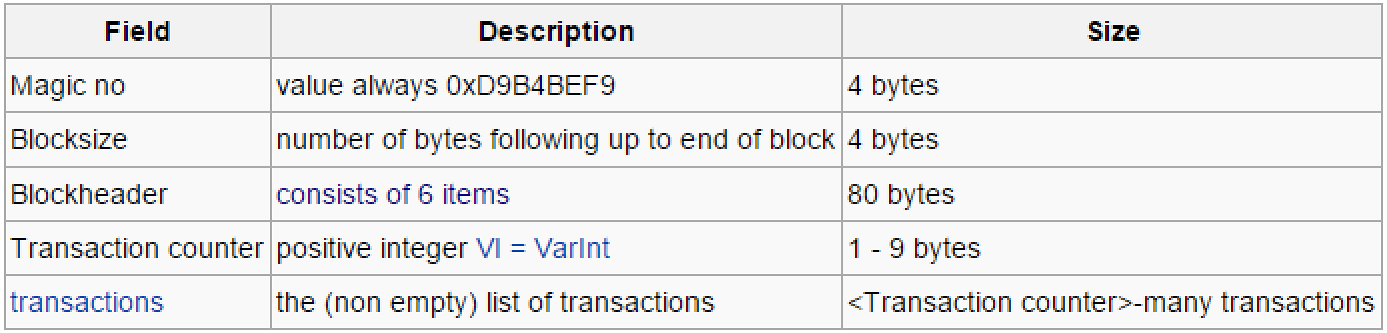
Summary	
Number Of Transactions	149
Output Total	1,298.63467541 BTC
Estimated Transaction Volume	660.76313702 BTC
Transaction Fees	.25 BTC
Height	332076 (Main Chain)
Timestamp	2014-11-29 05:37:47
Received Time	2014-11-29 05:37:47
Relayed By	GHash.IO
Difficulty	40,300,030,327.89
Bits	404441185
Size	82.3505859375 KB
Version	2
Nonce	1344293500

Hashes	
Hash	0000000000000000131c7157d41aeff51f34ad5dfe2f03ac76997bd5814fea61
Previous Block	00000000000000000bd6a32d894f789bdece5975abffc8a452b496a5d7e908ad
Next Block(s)	0000000000000000015e0d602de2e37405f150aa7ec00ebebe64860a80d8c255a
Merkle Root	998393c3da42bb875c2b57d363e9368171433bd81b133f3a5b46ecd0a80bf755

Network Propagation (Click To View)

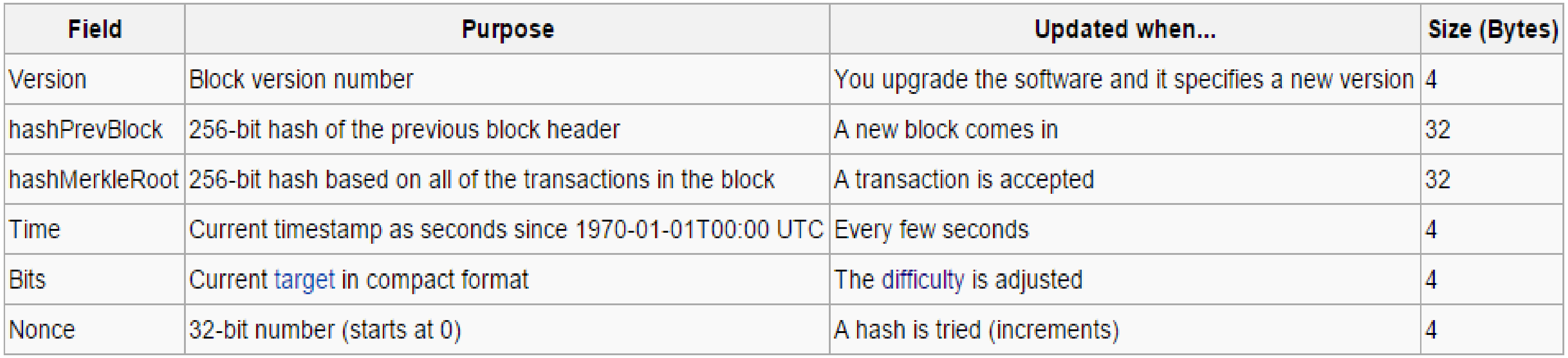
Block Hashing

Block format https://en.bitcoin.it/wiki/Blocks



Field	Description	Size
Magic no	value always 0xD9B4BEF9	4 bytes
Blocksize	number of bytes following up to end of block	4 bytes
Blockheader	consists of 6 items	80 bytes
Transaction counter	positive integer VI = VarInt	1 - 9 bytes
transactions	the (non empty) list of transactions	<Transaction counter>-many transactions

Block header https://en.bitcoin.it/wiki/Block_hashing_algorithm



Field	Purpose	Updated when...	Size (Bytes)
Version	Block version number	You upgrade the software and it specifies a new version	4
hashPrevBlock	256-bit hash of the previous block header	A new block comes in	32
hashMerkleRoot	256-bit hash based on all of the transactions in the block	A transaction is accepted	32
Time	Current timestamp as seconds since 1970-01-01T00:00 UTC	Every few seconds	4
Bits	Current target in compact format	The difficulty is adjusted	4
Nonce	32-bit number (starts at 0)	A hash is tried (increments)	4

Bitcoin Wallet

Money is added to account in the wallet associated with the Bitcoin address (one-time use)

The address includes a hash of a public key; the associated private key is used to lock the funds in the account

The wallet should be encrypted to protect the private keys
https://en.bitcoin.it/wiki/Securing_your_wallet

In some cases, backups must be done frequently to capture all the keys in the wallet

Wallet Types

Paper (hardcopy)

Hardware

Software (Bitcoin-QT or bitcoind)

- encrypt, backup, erase

Online or Mobile

- use for ready cash

Explore

http://blockchain.info

To be continued …

That’s all for today … come back tomorrow for an overview of Bitcoin and other possibilities …

The blockchain is disruptive technology and the possibilities are endless.

Questions?

Many answers can be found at http://bitcoin.org

Mastering Bitcoin http://shop.oreilly.com/product/0636920032281.do