Blockchain Technology 3

Beni Iyaka H00181266

bi34@hw.ac.uk

MSc Software Engineering

2016 - 2017

Outline

- Overview
- Transaction
- Bitcoin Mining
- Bitcoin Payment
- Payment Protocol
- Bitcoin Payment Verification
- Conclusion
- Further Readings

Transaction
(Alice & Bob Scenario)

- Alice uses to send Bob a transaction and which Bob later uses to spend that transaction
- Both Alice and Bob will use the most common form of the standard Pay-To-Public-Key-Hash (P2PKH) transaction type
- Bob must first generate a private/public key pair before Alice can create the first transaction
- Bitcoin uses the Elliptic Curve Digital Signature Algorithm (ECDSA) with the secp256k1 curve
  - secp256k1 private keys are 256 bits of random data

Barber, S., Boyen, X., Shi, E. and Uzun, E., 2012, February. Bitter to better—how to make bitcoin a better currency. In *International Conference on Financial Cryptography and Data Security* (pp. 399-414). Springer Berlin Heidelberg.

- A copy of that data is deterministically transformed into an secp256k1 public key.

- The public key (pubkey) is then cryptographically hashed

- Bob provides the pubkey hash to Alice

- Pubkey hashes are almost always sent encoded as Bitcoin addresses, which are base58-encoded strings
  - containing an address version number, the hash, and an error-detection checksum

Barber, S., Boyen, X., Shi, E. and Uzun, E., 2012, February. Bitter to better—how to make bitcoin a better currency. In *International Conference on Financial Cryptography and Data Security* (pp. 399-414). Springer Berlin Heidelberg.

- Once Alice has the address and decodes it back into a standard hash, she can create the first transaction
  - A standard P2PKH transaction output containing instructions(are called the pubkey script or scriptPubKey)

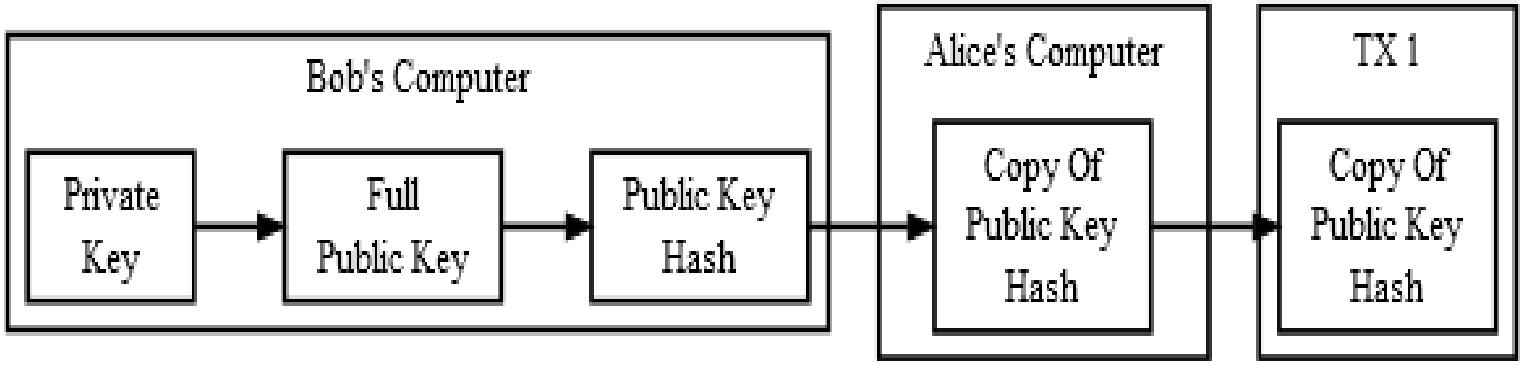
- Alice broadcasts the transaction and it is added to the block chain.
  - The network categorizes it as an Unspent Transaction Output (UTXO)

- Some time later, Bob decides to spend the UTXO, he must create an input which references the transaction Alice created by its hash, called a Transaction Identifier (txid)

Barber, S., Boyen, X., Shi, E. and Uzun, E., 2012, February. Bitter to better—how to make bitcoin a better currency. In *International Conference on Financial Cryptography and Data Security* (pp. 399-414). Springer Berlin Heidelberg.

- Create a signature script—a collection of data parameters which satisfy the conditions Alice placed in the previous output's pubkey script.
    - Signature scripts are also called scriptSigs

Barber, S., Boyen, X., Shi, E. and Uzun, E., 2012, February. Bitter to better—how to make bitcoin a better currency. In *International Conference on Financial Cryptography and Data Security* (pp. 399-414). Springer Berlin Heidelberg.



Creating A P2PKH Public Key Hash To Receive Payment

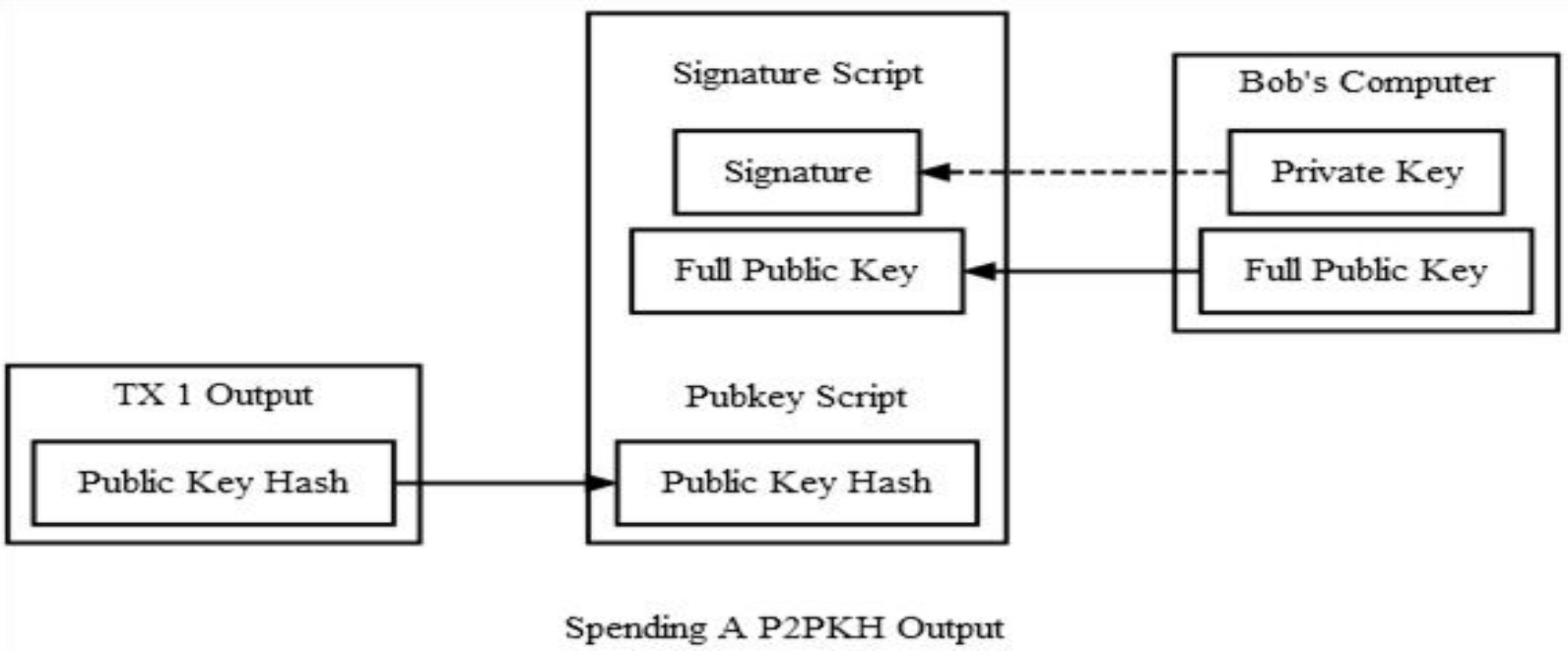
Barber, S., Boyen, X., Shi, E. and Uzun, E., 2012, February. Bitter to better—how to make bitcoin a better currency. In *International Conference on Financial Cryptography and Data Security* (pp. 399-414). Springer Berlin Heidelberg.

- Alice broadcasts the transaction and it is added to the block chain. The network categorizes it as an Unspent Transaction Output (UTXO), and Bob's wallet software displays it as a spendable balance.

- some time later, Bob decides to spend the UTXO, he must create an input which references the transaction Alice created by its hash, called a Transaction Identifier (txid)

- create a signature script—a collection of data parameters which satisfy the conditions Alice placed in the previous output's pubkey script. Signature scripts are also called scriptSigs

Barber, S., Boyen, X., Shi, E. and Uzun, E., 2012, February. Bitter to better—how to make bitcoin a better currency. In *International Conference on Financial Cryptography and Data Security* (pp. 399-414). Springer Berlin Heidelberg.



Spending A P2PKH Output

Barber, S., Boyen, X., Shi, E. and Uzun, E., 2012, February. Bitter to better—how to make bitcoin a better currency. In *International Conference on Financial Cryptography and Data Security* (pp. 399-414). Springer Berlin Heidelberg.

Bitcoin Wallet

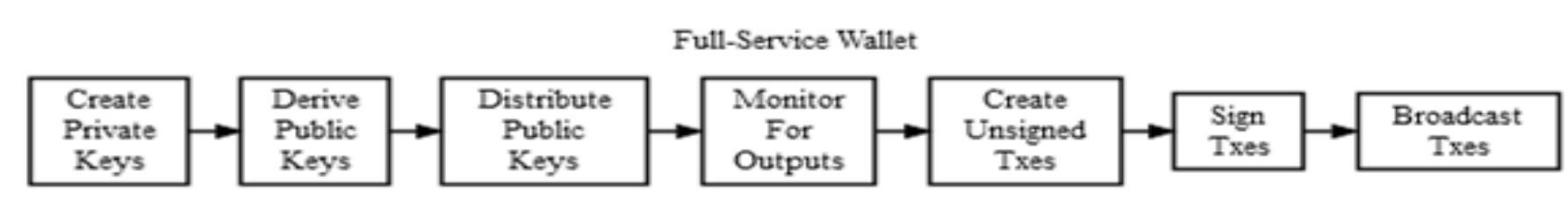
- Wallet programs create public keys to receive satoshis and use the corresponding private keys to spend those satoshis

- Wallet programs also need to interact with the peer-to-peer network to get information from the block chain and to broadcast new transactions

- three necessary, but separable, parts of a wallet system:
  - public key distribution program
  - signing program
  - networked program

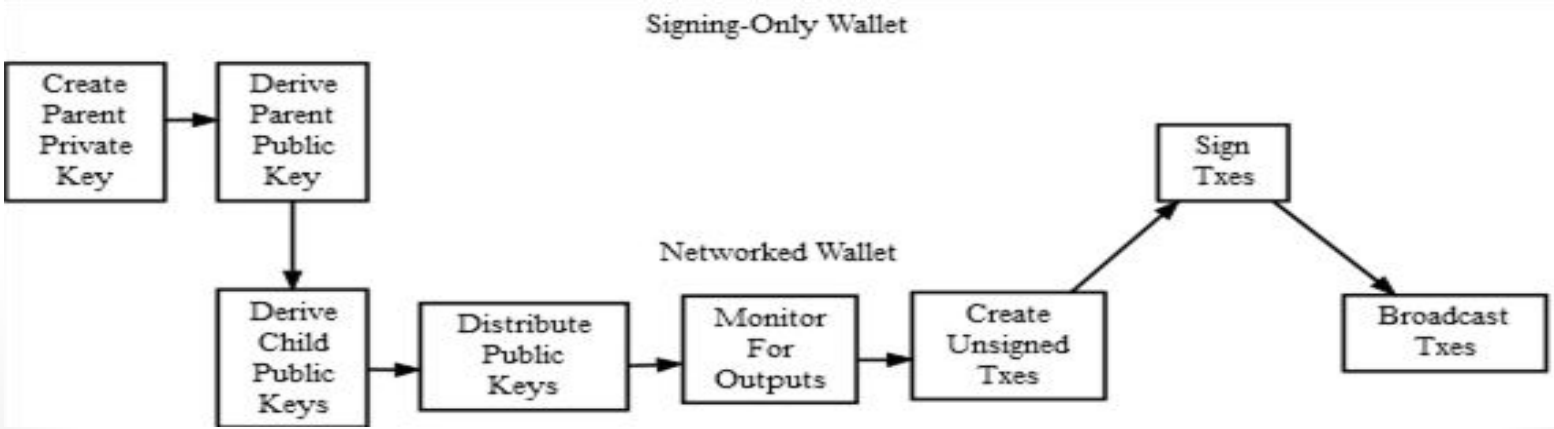
Decker, C. and Wattenhofer, R., 2013, September. Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings* (pp. 1-10). IEEE.

- Full-Service Wallets
  - The simplest wallet is a program which performs all three functions
  - almost all popular wallets can be used as full-service wallets
  - The main advantage of full-service wallets is that they are easy to use
  - The main disadvantage of full-service wallets is that they store the private keys on a device connected to the Internet



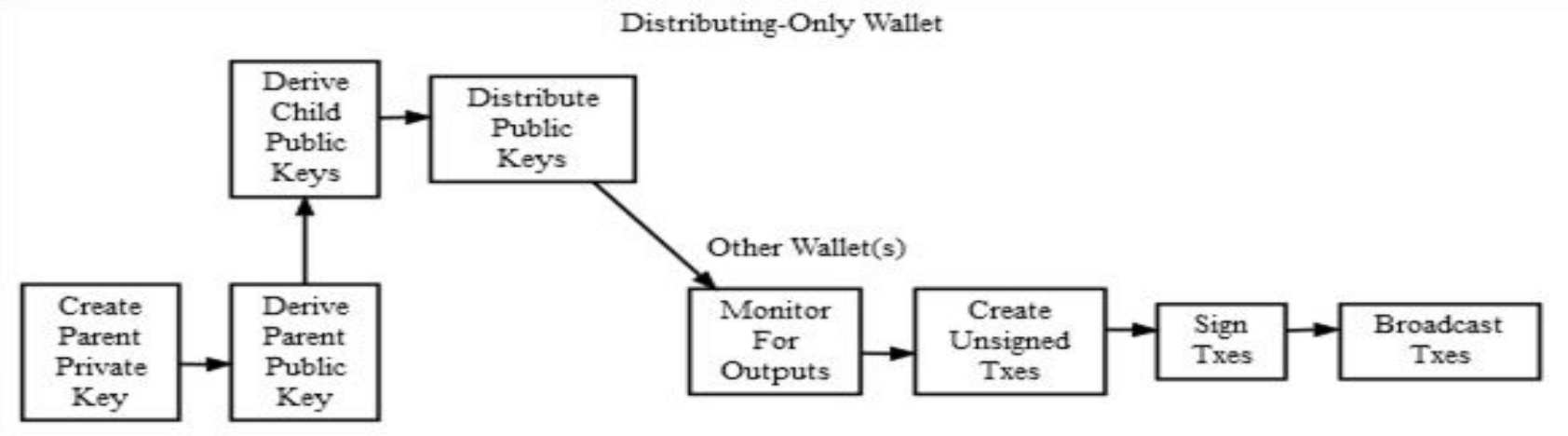
Decker, C. and Wattenhofer, R., 2013, September. Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings* (pp. 1-10). IEEE.

- Signing-Only Wallets
  - To increase security, private keys can be generated and stored by a separate wallet program operating in a more secure environment
  - These signing-only wallets work in conjunction with a networked wallet which interacts with the peer-to-peer network.



Decker, C. and Wattenhofer, R., 2013, September. Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings* (pp. 1-10). IEEE.

- Distributing-Only Wallets
  - Wallet programs which run in difficult-to-secure environments, such as webservers, can be designed to distribute public keys



Decker, C. and Wattenhofer, R., 2013, September. Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings* (pp. 1-10). IEEE.

Bitcoin Mining

- The process of finding a valid block
- (adds new blocks to the block chain)
- Nodes that mine are called miners
- Perform this steps in an endless loop:
  - Collect all broadcasted transactions and validate whether they satisfy the miner's self-defined policy

Decker, C. and Wattenhofer, R., 2013, September. Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings* (pp. 1-10). IEEE.

- The process of finding a valid block (adds new blocks to the block chain)

- Nodes that mine are called miners

- Perform this steps in an endless loop:
  - Collect all broadcasted transactions and validate whether they satisfy the miner's self-defined policy
  - Verify all transactions that are to be included in the block and it is checked whether they have been previously spent
  - Select the most recent block on the longest path in the blockchain
  - Attempt to solve the proof-of-work problem and broadcast the solution

- Miners use software that accesses their processing capacity to solve transaction-related algorithms .

- In return, they are awarded a certain number of Bitcoins per block

- Its mining hardware (an ASIC) along with a target threshold (difficulty setting).

Decker, C. and Wattenhofer, R., 2013, September. Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings* (pp. 1-10). IEEE.

- The mining hardware iterates through every possible value for the block header nonce and generates the corresponding hash
    - If a hash is found below the target threshold, the mining hardware returns the block header with the successful nonce to the mining software.
    - The mining software combines the header with the block and broadcasts to the network for addition to the block chain

Decker, C. and Wattenhofer, R., 2013, September. Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings* (pp. 1-10). IEEE.

Bitcoin Payment

- Payment processing encompasses the steps senders and receivers perform to make and accept payments in exchange for products or services

- The Payment Protocol is described in depth in BIP70, BIP71, and BIP72

Grinberg, R., 2012. Bitcoin: An innovative alternative digital currency. *Hastings Sci. & Tech. LJ*, *4*, p.159.

- New payment protocol adds many important features :

  - Supports X.509 certificates and SSL encryption to verify receivers' identity and help prevent man-in-the-middle attacks.

  - Allows spenders to submit transactions directly to receivers without going through the peer-to-peer network
    - Bluetooth-based payments

  - Instead of a meaningless address (mjSk1Ny9spzU2fouzYgLqGUD8U41iR35QN), Common Name (CN) description from the receiver's X.509 certificate (www.bitcoin.org)

Grinberg, R., 2012. Bitcoin: An innovative alternative digital currency. *Hastings Sci. & Tech. LJ*, *4*, p.159.

Payment Protocol

- Charlie, the client, is shopping on a website run by Bob
- Charlie adds a few items to his shopping cart and clicks the "Checkout With Bitcoin" button.
- Bob's server automatically adds the following information to its invoice database:
  - The details of Charlie's order, including items ordered and shipping address.
  - An order total in satoshis
  - An expiration time when that total will no longer be acceptable.
  - A pubkey script to which Charlie should send payment.
- After adding all that information to the database, Bob's server displays a bitcoin: URI for Charlie to click to pay

- Charlie clicks on the bitcoin: URI in his browser
- His browser's URI handler sends the URI to his wallet program
- Wallet sends an HTTP GET to that URL looking for a PaymentRequest message
- The PaymentRequest message returned may include private information, such as Charlie's mailing address
- The unique public key created for the payment request can be used to create a unique identifier

- After receiving the HTTP GET to the URL, Bob's webserver takes the unique identifier from the URL and looks up the corresponding details in the database.

- creates a PaymentDetails message with information:

  - The amount of the order in satoshis and the pubkey script to be paid
  - A memo containing the list of items ordered
  - The time the PaymentDetails message was created plus the time it expires
  - A URL to which Charlie's wallet should send its completed transaction

Grinberg, R., 2012. Bitcoin: An innovative alternative digital currency. *Hastings Sci. & Tech. LJ*, *4*, p.159.

- That PaymentDetails message is put inside a PaymentRequest message.

- Bob's server sign the entire Request with the server's X.509 SSL certificate.

- Bob's server sends the payment request to Charlie's wallet in the reply to the HTTP GET

- Charlie's wallet receives the PaymentRequest message, checks its signature, and then displays the details to Charlie

- Charlie agrees to pay, the wallet constructs a payment to the pubkey script Bob's server provided

- Constructs a Payment message and sends it to the URL provided in the PaymentDetails message as an HTTP POST which contains:

  - The signed transaction in which Charlie pays Bob
  - An optional memo Charlie can send to Bob
  - A refund address (pubkey script) which Bob can pay if he needs to return some or all of Charlie's satoshis

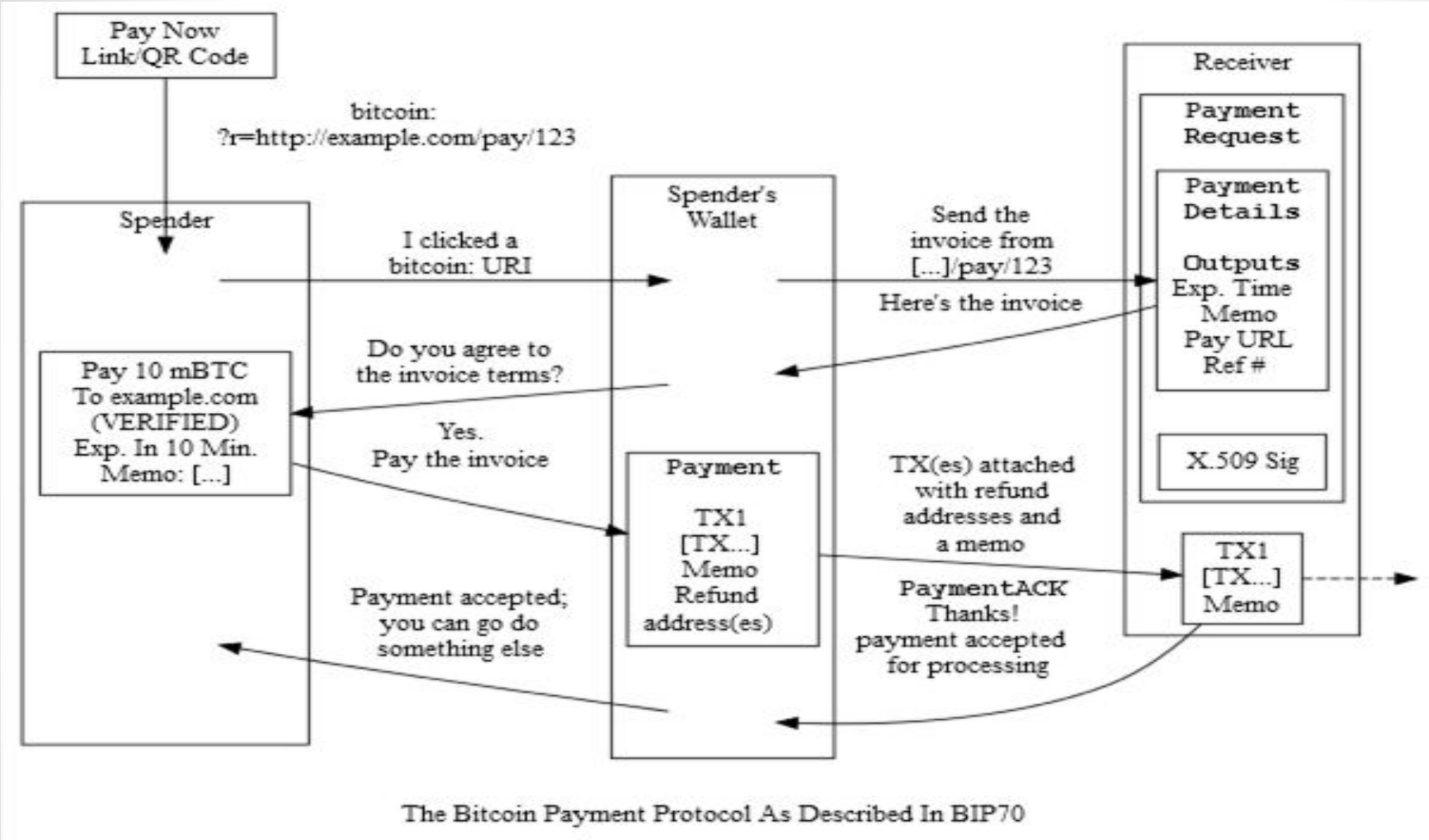
- Bob's server receives the Payment message, verifies the transaction, then broadcasts the transaction to the network.
- Replies to the HTTP POSTed Payment message with a PaymentACK message
- Charlie's wallet sees the PaymentACK and tells Charlie that the payment has been sent

Grinberg, R., 2012. Bitcoin: An innovative alternative digital currency. *Hastings Sci. & Tech. LJ*, *4*, p.159.

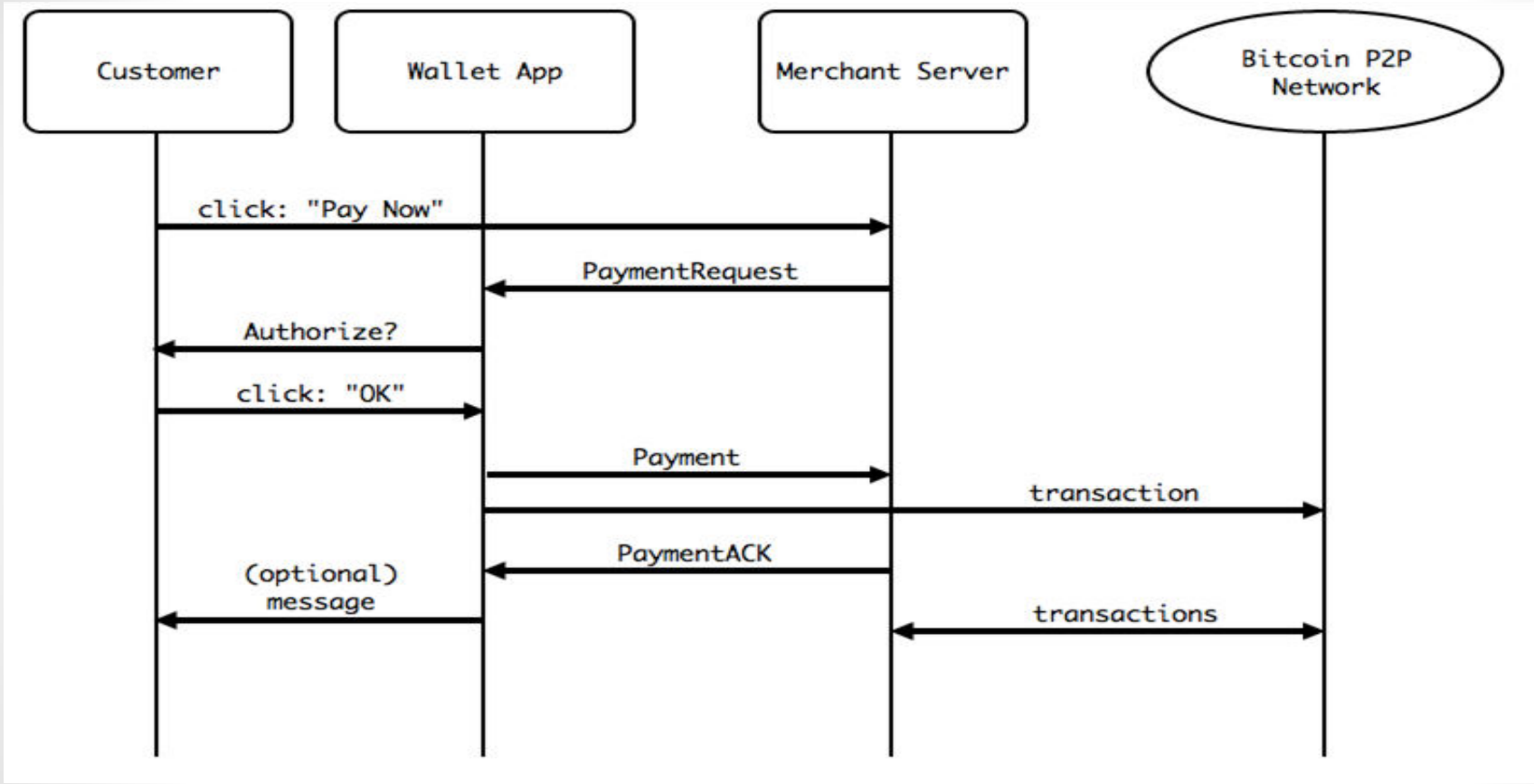
- The PaymentACK doesn't mean that Bob has verified Charlie's payment

- After Bob's server verifies from the block chain that Charlie's transaction has been suitably confirmed, it authorizes shipping Charlie's order

Grinberg, R., 2012. Bitcoin: An innovative alternative digital currency. *Hastings Sci. & Tech. LJ*, *4*, p.159.



The Bitcoin Payment Protocol As Described In BIP70



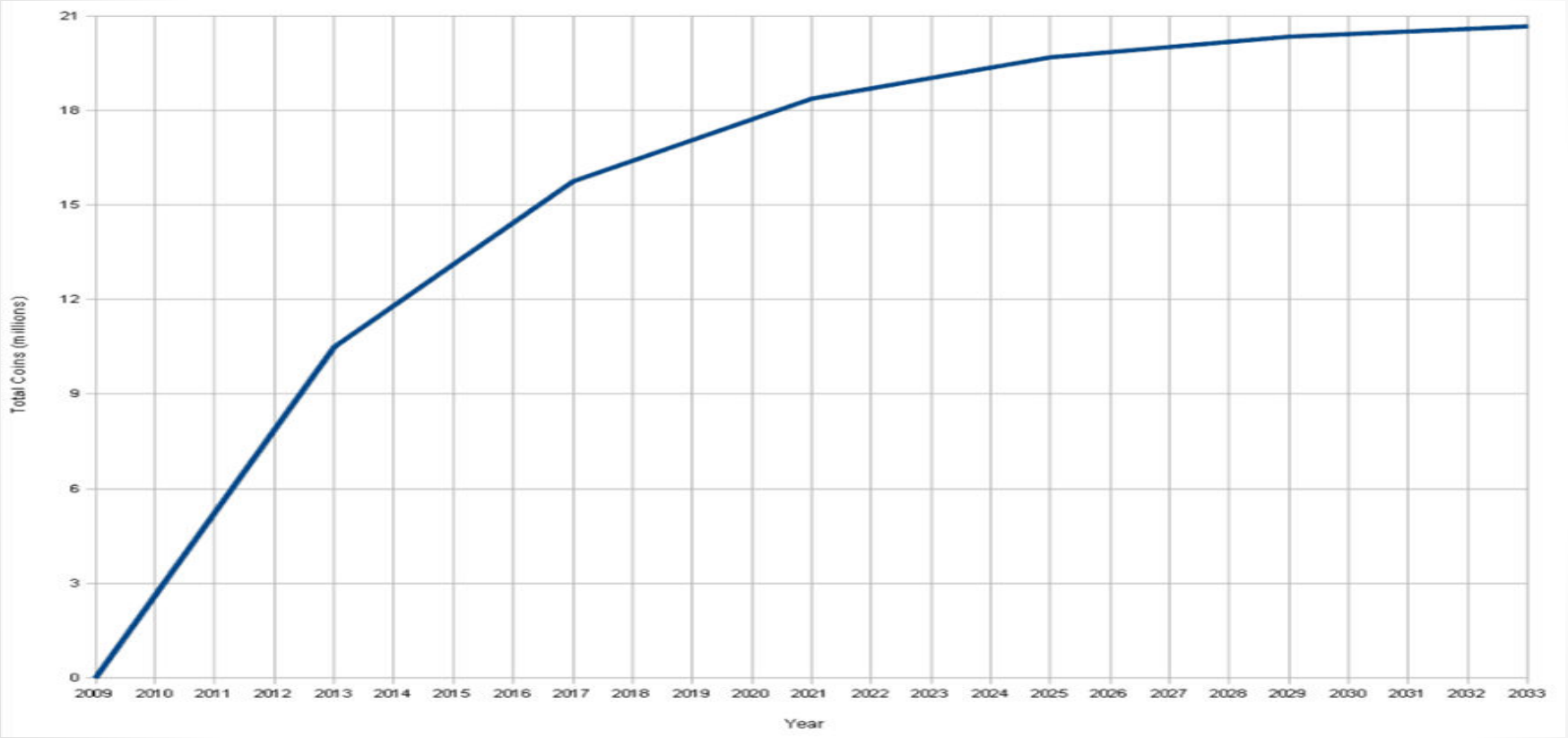
Grinberg, R., 2012. Bitcoin: An innovative alternative digital currency. *Hastings Sci. & Tech. LJ*, *4*, p.159.

Bitcoin Payment Verification

- 0 confirmations (unconfirmed transactions)
  - The transaction has been broadcast but is still not included in any block
  - should generally not be trusted without risk analysis
  - Miners usually confirm the first transaction they receive, fraudsters may be able to manipulate the network into including their version of a transaction.
- 1 confirmation
  - The transaction is included in the latest block and double-spend risk decreases dramatically
  - Transactions which pay sufficient transaction fees need 10 minutes on average to receive one confirmation
  - The most recent block gets replaced fairly often by accident, so a double spend is still a real possibility

- 2 confirmations
  - The most recent block was chained to the block which includes the transaction
  - As of March 2014, two block replacements were exceedingly rare, and a two block replacement attack was impractical without expensive mining equipment.
- 6 confirmations
  - The network has spent about an hour working to protect the transaction against double spends and the transaction is buried under six blocks
  - Even a reasonably lucky attacker would require a large percentage of the total network hashing power to replace six blocks

Bitcoin over time



Grinberg, R., 2012. Bitcoin: An innovative alternative digital currency. *Hastings Sci. & Tech. LJ*, *4*, p.159.

Conclusion

- It is useful to understand blockchains in the context of bitcoin, but you should not assume that all blockchain ecosystems need bitcoin mechanisms such as tokens, proof of work mining, longest chain rule, etc.

- Bitcoin is the first attempt at maintaining a decentralised, public ledger with no formal control or governance.

- Ethereum is the next iteration of a blockchain with smart contracts.

- There are significant challenges involved.

- On the other hand, private or internal distributed ledgers and blockchains can be deployed to solve other sets of problems.

- As ever, there are tradeoffs and pros and cons to each solution, and you need to consider these individually for each individual use case.

Further readings

https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/

https://bitsonblocks.net/2016/05/09/confused-by-blockchains-revolution-vs-evolution/

https://bitsonblocks.net/2015/12/01/the-pros-and-cons-of-internal-blockchains/

Further readings

https://bitsonblocks.net/2015/09/28/a-gentle-introduction-to-digital-tokens/

https://bitsonblocks.net/2015/09/21/a-gentle-introduction-to-bitcoin-mining/

https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/