ELENCO LINK

SCRAPING DARK WEB 27/10

- https://blog.scrapinghub.com/2015/02/24/memex/

1. Se ne occupa Alessio

BITLODINE 30/10

- https://github.com/mikispag/bitiodine
- https://miki.it/pdf/BitIodine_presentation.pdf
- https://web.archive.org/web/20160503034434/https://bitiodine.net/
- https://www.ifca.ai/fc14/papers/fc14_submission_11.pdf
- https://www.politesi.polimi.it/bitstream/10589/88482/3/thesis.pdf

1. utilizzato come punto di partenza quindi ben conosciuto

DA INVESTIGARE 02/11

- http://bitcoin.stackexchange.com/questions/7447/is-it-possible-to-figure-out-whether-two-addresses-are-in-the-same-wallet

1. dice di raggruppare con il criterio degli indirizzi di input, non più vero dopo l'avvento di servizi come coinjoin

- http://stackoverflow.com/questions/25343204/determine-if-a-bitcoin-wallet-address-is-valid

1. Parla dei sistemi di validazione di un indirizzo bitcoin, dal 2014 (data del post) a oggi ne sono stati fatti moltissimi. ALESSIO

NOVETTA MIXING SERVICES 03/11

- https://www.novetta.com/wp-content/uploads/2015/10/NovettaBiometrics_BitcoinCryptocurrency_WP-W_9182015.pdf

1. Parla delle mixnet, da vedere quando le tratteremo

VARIE 05/11

- https://www.elliptic.co
  (Cliccare su "?",tipi di nodi bitcoin in particolare quelli rossi! (appuntarseli)
  ci servirebbe elenco di tutti i nodi gia' identificati/conosciuti)

1. All'interno sono presenti alcuni nodi bitcoin che potrebbero essere utili, tuttavia non presenta né API né indirizzi bitcoin ma soltanto i nomi

- tipi nodi bitcoin: http://www.bitcoinlinks.net/exchanges

1. Lista di (alcuni?) exchange conosciuti, sono presenti le home page di questi siti perciò potrebbe essere utile prenderli tutti e scraparli ALESSIO

- deanonimizzazione: https://arxiv.org/pdf/1107.4524.pdf

1. Ancora devo leggerlo

CAMPI DEL DB E COME PARSARE LA BLOCKCHAIN 10/11

- https://bitcoin.org/en/developer-reference#raw-transaction-format
- http://codesuppository.blogspot.it/2014/01/how-to-parse-bitcoin-blockchain.html

1. Abbiamo già deciso e quasi finito questo passaggio

VISUALIZZAZIONE PATTERN DINAMICI DELLE TRANSAZIONI 12/11

- http://online.liebertpub.com/doi/pdf/10.1089/big.2015.0056

1. Parla di come visualizzare dinamicamente la blockchain e le transazioni, la visualizzazione non bisogna farla noi

TOOL DI VISUALIZZAZIONE 14/11

- http://mrvar.fdv.uni-lj.si/pajek/italian/Italian.pdf
- https://casmodeling.springeropen.com/articles/10.1186/s40294-016-0017-8

1. Tool di visualizzazione proposto dal prof, da valutare insieme.

VARIE 15/11

- https://github.com/UniCreditDnA/blockchain-paper/raw/master/Blockchain.Technology.and.Applications.from.a.Financial.Perspective.pdf

1. Altro articolo molto generale che parla della blockchain e si concentra sull'ambito economico, poco utile

PUBBLICAZIONI DA GUARDARE E CITARE 16/11

pubblicazioni da citare sicuramente e da guardare

- Traversing Bitcoin's P2P network: Insights into the structure of a decentralised currency
- Quantitative analysis of the full Bitcoin transaction graph
- Evaluating user privacy in Bitcoin
- An analysis of anonymity in bitcoin using P2P network traffic

- An analysis of anonymity in the bitcoin system
- Exploring the Bitcoin network
- CoinShuffle: Practical decentralized coin mixing for bitcoin
- Identifying Bitcoin users by transaction behavior
- A graph-based investigation of bitcoin transactions
- Analyzing the bitcoin network: The First Four Years

1. queste devo guardarle tutte

SCRAPER DEEP WEB 19/11

- https://scrapy.org

1. Web spider consigliato dal prof santini, Alessio ha già fatto il suo perciò magari utile per la bibliografia

TRANSAZIONI 24/11

- http://bitcoin.stackexchange.com/questions/25767/why-is-it-possible-to-have-multiples-addresses-in-an-output-of-a-transaction

1. Utile per capire il campo addresses, c'è un esempio con 2 addresses ma provato sul software da dove prendiamo i dati ne restituisce uno alla volta, UTILE, DA VERIFICARE CON NODO PALUELLO

- http://bitcoin.stackexchange.com/questions/3718/what-are-multi-signature-transactions

- https://bitcoinmagazine.com/articles/multisig-future-bitcoin-1394686504
- https://en.bitcoin.it/wiki/Multisignature

1. Tutti e due ne parlano, "Multisignature (multisig) refers to requiring more than one key to authorize a Bitcoin transaction."

GREEN ADDRESS 27/11

- https://en.bitcoin.it/wiki/Green_address

1. **Green addresses** was a proposed use of special trusted ECDSA keypairs that to indicate the origin of funds to a recipient. Assuming the recipient trusts the operator of the keypair to not attempt a double spend, the recipient may treat the funds as confirmed the moment they arrive. **This proposal is generally considered a bad idea and not advisable to implement.**

   Queste righe riassumono cos'è, non utile.

VARIE 27/11

- http://bitzuma.com/posts/five-ways-to-lose-money-with-bitcoin-change-addresses/

1. Single-Address Wallets use a single address to receive both payments and change. Additional addresses may added when a receiving address is manually added, or a private key is imported. Examples include Blockchain.info and MultiBit.

- Random Address Pool Wallets use a fixed-size pool of randomly-generated addresses. Change is sent to the next available empty address, causing the creation of a new empty address to take its place. The best-known example is Bitcoin-Qt.
- Deterministic Address Pool Wallets contain a practically infinite pool of deterministically-generated addresses. A subset of this pool contains addresses reserved for receiving change. Examples include Electrum and Armory.
- Hybrid Wallets use multiple strategies, depending on context. MultiBit, Mycelium, and Electrum are examples.

  Questa era la cosa utile di questo articolo, tipi di wallet

- https://bitcointalk.org/index.php?topic=279249.0

1. Questo articolo parla di coinjoin, il sistema che prende input da più utenti per preservare la privacy

- https://medium.com/@octskyward/merge-avoidance-7f95a386692f#.flyfka8l0

1. Anche questo parla di coinjoin

- http://bitcoin.stackexchange.com/questions/20701/what-is-a-stealth-address

1. With a stealth address, you ask payers to generate a unique address in such a way that you (using some additional data which is attached to the transaction) can deduce the corresponding private key. So although you publish a single "stealth address" on your website, the block chain sees all your incoming payments as going to separate addresses and has no way to correlate them. (Of course, any individual payer knows their payment went to you, and can trace how you spend it, but they don't learn anything about other people's payments to you.)

- https://bitcoinmagazine.com/articles/is-bitcoin-anonymous-a-complete-beginner-s-guide-1447875283

1. Parla in generale della privacy nei bitcoin, come si clusterizzava con gli indirizzi di input e come hanno risolto questo problema con coinjoin

- https://99bitcoins.com/know-more-top-seven-ways-your-identity-can-be-linked-to-your-bitcoin-address/

1. Parla dei modi consigliati per non far collegare un indirizzo bitcoin al proprio nome

- http://anonymity-in-bitcoin.blogspot.it/2011/07/bitcoin-is-not-anonymous.html

1. Lo devo ancora guardare

SITO DOVE POTER SCRAPARE 27/11

- http://bitcoinfoundation.org/member/

1. non sono presenti indirizzi bitcoin all'interno di questo sito

ALTRA COSA 27/11

- https://en.bitcoin.it/wiki/Colored_Coins

1. Da leggere

- https://letstalkpayments.com/11-blockchain-api-providers-that-are-allowing-developers-to-build-next-generation-applications/

1. Lista di api provider riguardanti i bitcoin, da vedere

- ARTICOLO SHAMIR: http://dcg.ethz.ch/lectures/fs14/seminar/paper/Christian/22.pdf

1. Da guardare

- https://curiosity-driven.org/low-level-bitcoin

1. Parla del parser della blockchain, già fatto

questi citano il papero di shamir
aggiungete il prec e queati alla bibliografia
guardate se riuscite a scaricarli

- https://www.scopus.com/record/display.uri?origin=citedby&eid=2-s2.0-84991773817&citeCnt=13&noHighlight=false&sort=plf-f&src=s&st1=Quantitative+Analysis+of+the+Full+Bitcoin+Transaction+Graph&st2=&sid=6DCC18E60C1DED74AEF3FFCF99B3AE0C.wsnAw8kcdt7IPYLO0V48gA%3a170&sot=b&sdt=b&sl=74&s=TITLE-ABS-KEY%28Quantitative+Analysis+of+the+Full+Bitcoin+Transaction+Graph%29&relpos=0
- https://www.scopus.com/record/display.uri?origin=citedby&eid=2-s2.0-84962106697&citeCnt=13&noHighlight=false&sort=plf-f&src=s&st1=Quantitative+Analysis+of+the+Full+Bitcoin+Transaction+Graph&st2=&sid=6DCC18E60C1DED74AEF3FFCF99B3AE0C.wsnAw8kcdt7IPYLO0V48gA%3a170&sot=b&sdt=b&sl=74&s=TITLE-ABS-KEY%28Quantitative+Analysis+of+the+Full+Bitcoin+Transaction+Graph%29&relpos=2
- https://www.scopus.com/record/display.uri?origin=citedby&eid=2-s2.0-84991773817&citeCnt=13&noHighlight=false&sort=plf-f&src=s&st1=Quantitative+Analysis+of+the+Full+Bitcoin+Transaction+Graph&st2=&sid=6DCC18E60C1DED74AEF3FFCF99B3AE0C.wsnAw8kcdt7IPYLO0V48gA%3a170&sot=b&sdt=b&sl=74&s=TITLE-ABS-KEY%28Quantitative+Analysis+of+the+Full+Bitcoin+Transaction+Graph%29&relpos=0

- https://www.scopus.com/record/display.uri?eid=2-s2.0-84961321922&origin=resultslist&sort=plf-f&cite=2-s2.0-84883268487&src=s&imp=t&sid=6DCC18E60C1DED74AEF3FFCF99B3AE0C.wsnAw8kcdt7IPYLO0V48gA%3a330&sot=cite&sdt=a&sl=0&relpos=8&citeCnt=0&searchTerm=

1. Tutti da guardare