# Blockchain for Identity Management

by

**Ori Jacobovitz**

Technical Report #16-02

December 2016

The Lynne and William Frankel Center for Computer Science Department of Computer Science, Ben-Gurion University, Beer Sheva, Israel.

# Blockchain for Identity Management

Ori Jacobovitz

December 11, 2016

## Introduction

We are living in a world that is rapidly undergoing a fundamental change, it is becoming driven by data. This transformation is about all societal systems: traffic, health, government, logistics, and defense; being more quantified and efficient, but also more transparent and accountable. This changes not only the economics of systems, but their management as well. It also blurs the lines between customer, citizen, company, and government. Everyone gets to see what is happening, and so everyone gets to have a role in shaping these new systems.
As a consequence, businesses and governments are struggling to understand what the changing landscape means and how they can participate.

In this paper, I discusses the state of the art in Blockchain technology and its applications, focusing on applications and solutions in identity management.

## Blockchain Technology

The definition of the term blockchain is far from clear. The word blockchain itself most likely traces back to Satoshi Nakamoto's original Bitcoin white paper from 2008[1].
While there is no specific mention of the word blockchain in the paper, it describes a technology component underlying the cryptocurrency as a series of data blocks that are cryptographically chained together.

In a nutshell, blockchain is nothing more than a mere distributed database that provides an unalterable public record of digital transactions.
It can be viewed as a distributed digital ledger containing a chain of blocks information, where each block is identified by a cryptographic signature. These blocks are all back-linked; that is, they refer to the signature of the previous block in the chain, and that chain can be traced all the way back to the very first block created. As such, the Blockchain contains an un-editable record of all the transactions made. The transparent and decentralized nature of the Blockchain network enables the development of a non-refutable, and unbreakable record of data, which is the fundamental feature to many applications, such as identity management.

## Identity Management

A lot of hype exists about the possibilities using blockchain technology, I will focus on identity management.

The need for blockchain based identity management is particularly noticeable in the internet age, we have faced identity management challenges since the dawn of the Internet. Prime among them: security, privacy, and usability.

While there exists somewhat imperfect systems for establishing personal identity in the real world, in the form of identity document, driver's licenses and even passports, there is no equivalent system for securing either online authentication of our personal identities or the identity of digital entities. So while governments can issue forms of physical identification, online identities and digital entities do not recognize national boundaries and digital identity authentication appears at first look to be an intractable problem without an overseeing global entity.

Blockchain technology may offer a way to circumvent this problem by delivering a secure solution without the need for a trusted, central authority. It can be used for creating an identity on the blockchain, making it easier to manage for individuals, giving them greater control over who has their personal information and how they access it.

By combining the decentralized blockchain principle with identity verification, a digital ID can be created that would act as a digital watermark which can be assigned to every online transaction. The solution can help the organizations to check the identity on every transaction in real time, hence, eliminating rate of fraud. Consumers will be able to login and verify payments without having to enter any of the traditional username and password information. Through blockchain solutions, consumers can simply use an app for authentication instead of using traditional methods, such as a username and password. The solution will store their encrypted identity, allowing them to share their data with companies and manage it on their own terms.

## Applications & Solutions

Listed below are projects, companies and movements which are focused on using blockchain for identity management.

I divided the solutions into different categories in order to make some sort of order.
Each category is sorted by importance/relevance in a descending order (According to my own view and opinion of course). This means that the first instance in each category is the most relevant while the last is the least of them all.

### Foundations and Big Projects

1. Bitnation *[53]* - A governance platform which is powered by blockchain technology.

   Seeks to establish the concept of world-citizenship through identity registration on the blockchain. Its goal is to provide the same services that governments provide, but in a decentralized and voluntary manner, unbound by geography.

   Any individual from around the world can became a citizen of Bitnation by signing on to the constitution. Bitnation has worked out an identification solution such as blockchain passport and a marriage certificate.

   The Bitnation Refugee Emergency Response (BRER) program provides an identification system called Blockchain Emergency ID (BE-ID). The BE-ID allowed a person to receive an ID recorded on the blockchain for those who cannot get other identification documents. With this ID, people were able to receive social assistance and financial services.

   The first version of the ID required users prove their existence at a certain time by taking a picture with the latest Bitcoin merkle root, or the hash of all the hashes of all the transactions in a block. Then the picture is inserted into an ID template and the documents are signed with PGP keys. Later forms of identification have been simplified, in the current Bitnation World Citizenship ID, as well as the Refugee Emergency ID.

   - The project is collaborating with the Estonian e-Residency program *2*.

2. e-Residency - A program launched by Estonia that allows non-Estonians access to Estonian services such as company formation, banking, payment processing, and taxation.

   The program gives the e-Resident a smart card which he/she can use to sign documents. The program is aimed towards location-independent entrepreneurs such as developers and writers.

   An application for e-residency can be made over the Internet, by filling in a form, supplying a scan of a national passport and a photograph, and giving the reason for applying (which does not strongly affect the outcome of the application. The blockchain

notary service allows e-residents, regardless of where they live or do business, to notarize their marriages, birth certificates, business contracts on the blockchain.

Estonian e-residents can sign in using their physical ID card and perform digital signatures on the blockchain. Bitnation provides a P2P version of e-governance. This offers foreign people to become e-residents. This does not grant the same rights as resident in the traditional sense, but offers many facilities when dealing with the country.

- Identit.ee *[61]* - A program to build blockchain identity solutions related to the Estonian e-Residency concept.

- Further Reading: *[55][56], [57], [58], [59], [60]*

3. ConsenSys *[14]* - A blockchain software technology company founded in early 2015 as a software foundry to develop decentralized software services and applications that operate on the Ethereum blockchain*[13]*.

   The company's focus is on facilitating the empowerment of people and enabling decentralized governance through the development of software tools that devolve power from the traditional command and control hierarchies.

   - The company is involved in number of different projects such as Uport*10* and Blockstack*20*

4. ID2020*[42]* - A not-profit corporation that aims to find a solution for providing a legal digital identity for every person without identification by 2020.

   According to the United Nations, there are around 1.5bn people across the world who have no way of proving who they are. To tackle the problem, the corporation is creating a hub inspired by SDG 16. Many challenges stand in the way of reaching these goals, one of which is access to online identity management services.

   - Many believes blockchain has potential to solve the problems of ID2020.

   - Further Reading: *[46][47], [48], [49][2]*

5. Hyperledger (Linux foundation) *[17]* - An open source collaborative effort created to advance cross-industry blockchain technologies.

   The mission is to create an open source, technical community to benefit the ecosystem of Hyperledger Project solution providers and users, focused on blockchain and shared ledger use cases that will work across a variety of industry solutions.

6. Australia – The Australia post office, as well as the Australia's Digital Transformation Office are looking for blockchain identity management solutions.

   Australia Post handles 90 percent of all Australian passports and most of the physical IDs, It's only logical that a trusted organization like this would be able to handle digital identities of the citizens as well.

   - Further Reading: *[51], [52]*

7. PIMN (Platform Identity Management Netherlands) *[45]* – An organization in Netherlands focused on the identity management systems.

    - PIMN organized a meeting on block chain IDs in Amsterdam on April 26 2016, it was a first step and the organization shows a lot of interest at this topic.

    - PIMN also shows a particular interest with ShoCard product.

8. USA - The US Homeland Security is funding a research for identity vertification via blockchain.

    The agency says that it is seeking to "Design information security and privacy concepts on the blockchain to support identity management capabilities that increase security and productivity while decreasing costs and security risks for the Homeland Security Enterprise (HSE)."

    - Further Reading: *[50]*

**Startups and companies (focused on identity management)**

9. ShoCard[*33]* - A startup company developing an identity-platform built on blockchain. The company strives to be as easy to understand and use as showing a driver's license and simultaneously be so secure that a bank can rely on it.

    A ShoCard is a digital identity that protects consumer privacy, it is basically a tiny file that only you can manipulate. Creating a ShoCard ID can be done either through the App, or via the SDK, when you create your ShoCard, you first scan your identity document and sign it. Then, the app will generate a private and public key to seal that record. It is encrypted, hashed and sent to the blockchain where it cannot be tampered with or altered.

    The key is that the ShoCard Identity Platform is built on a public blockchain data layer, so as a company it is not storing data or keys that could be compromised.
    ShoCard uses the BlockCypher*26* Transaction API to publish identity data to other blockchains such as Bitcoin*[1]* and Ethereum*[13]*.

    ShoCard customers include SITA (an IT and communication services to the global airline industry), banks and financial services companies, including the third largest bank in Canada.

    - I tried to contact them in order to try one of their services such as a demo which is offered through the official website or an access to their API/ SDK. Unfortunately they didn't answer to any of my requests.

    - Further Reading: *[34], [35], [36], [37], [38]*

10. Uport *[11]* - A project by ConsenSys*3* focused on identity management.

    Uport is a secure system for self-sovereign identity, built on Ethereum*[13]*.

Uport represents the next generation of identity systems: the first identity system to enable self-sovereign identity, allowing the user to be in complete control of their identity and personal information. Uport identities can take many forms: individuals, devices, entities, or institutions.

- Seems very promising, it is still in the closed-beta stage (you can sign up so they would let you know whenever the open-beta is released).

- Further Reading:*[12]*

11. Ascribe GmbH*[39]* - A startup working with the blockchain to create new technological tools in the area of identity management for artists and creators.

    It describes itself as a “fundamentally new way to lock in attribution, securely share and trace where digital work spreads”.

    Ascribe leverages blockchain technology to make it possible to transfer, cosign or loan digital creations similar to physical pieces of work.
    Ascribe creates a permanent and unbreakable link between the creator and his or her creative work by allowing ownership to be forever verified and tracked.

    Ascribe partnered with Creative Commons to create a method for content creators to essentially stamp their work with proprietary information. Each work gets a unique public URL and all relevant metadata (title, creator, year, and license).

    - Ascribe offers an API which you can use to interact with their services through the blockchain.

12. I/O Digital[*40]* - A startup company building an identity-management platform based on the blockchain.

    I/O Digital provide the technology for businesses to have their own interoperable private blockchain / sidechain and the possibilities to store data in the blockchain for smart contracts, identity management, messaging and more.

    The I/O Digital project started as I/O Coin, or IOC, it is the digital currency of their blockchain and can be traded on several exchanges. With data storing capabilities, alias sending, side chain technology and decentralized (encrypted) messaging.

    I/O Digital's first venture into blockchain based identity managed was the IONS. The project's main purpose was to enable aliases on the I/O Coin blockchain but in a semi-centralized manner.

    After testing, I/O Digital decided to move forward with a more advanced system, the Decentralized I/O Name Server. Key features of the DIONS will include transferring aliases from user to user, storing identities on the blockchain and an encrypted messaging system. DIONS will utilize the I/O Digital blockchain to attach sensitive identity credentials to a specific Bitcoin or I/O Coin address.

    - They are currently developing an open API for every developer to use and it will be available soon.

13. BlockVerify[25] - A startup company developing blockchain based solutions.

    It uses blockchain technology to improve anti-counterfeit measures in different industries such as pharmaceuticals, luxury items, diamonds and electronics.

    - Still in development.
    - It seems like it is centralized in contradiction to our interest.

14. BlockAuth[26] - A startup company developing a service which enables you to own and operate your own identity registrar that allows users to submit their information for verification.

    - Still in development.
    - It seems like the company broke up into two different companies, but I can't be sure about that. One is registered under the domain blockauth.com and is part of TechEndeavors. The other is under the domain blockauth.org and is part of Neuroware. Both companies seems to work on same project as stated above since 2014 (at least).

15. UniquID[44] - A startup company which aims to provide identity and access management of connected things, as well as humans, utilizing biometric information.

    UniquID allows for the authentication of devices, cloud services, and people. It provides secure identity management, integrated with fingerprint and other biometry on personal devices. Ready to be deployed on custom hardware, servers, personal computers or smart phones and tablets.

    - At private beta stage.

16. Jolocom[20] - A startup company developing applications for everyone to own their personal digital identity, using linked data and blockchain technologies.

    - Still in development.

17. Cambridge Blockchain [21] - A startup company working on an Identity Blockchain for validating secure digital identity documents, processing electronic signatures, and recording transactions.

    - At alpha stage since 2015.

18. Cryptid[27] - A startup company developing a solution that eliminates the possibility of counterfeit identification by adding factors of identification and encryption.

    Cryptid takes the data provided in the form and package it into a compact format readable by our systems and generate your Cryptid identification data. All of the data is encrypted with the provided password after which it is permanently transferred to the blockchain. The customer is then given a unique identification number that points to the

information on the block chain and can be stored on almost anything from magnetic stripes to QR codes.

- Not open-source, couldn't make the web interface to work.

19. CredyCo[28] - A cryptographic service built on top of bitcoin's blockchain.

    A document verification "software as a service" (SaaS) which uses a smart contracts and identity technology built on top of the blockchain to ensure the credibility and irrefutability of all statements.

    - It seems like the project is dead.

**Open-Source / Indie Projects**

20. Blockstack [15] – An open-source blockchain application stack - permits building decentralized, serverless apps by plugging into Blockstack's services for identity, naming, storage and authentication.

    The blockchain is utilized to maintain a cross-application identity system, securely mapping user IDs to usernames, public keys, and data storage URIs.

    Identities can be registered for people, companies, websites, software packages and more. Profiles can contain both private and public information, which is attested to by the user and can be verified by peers and select authorities.

    According to the Blockstack team, Blockstack is the largest, most popular blockchain identity system, with 50,000 registered identities.

21. NameID[30] - An OpenID service based on Namecoin[27] identifiers.

    - It seems like a very simple (working) solution.

22. CertCoin[32] - An MIT project about a NameCoin based [27] decentralized authentication system which maintains a public ledger of domains and their associated public keys.

    - All source code is available at Github[31].

23. World-Citizenship[23] – A research project on registering WebIDs on the Ethereum blockchain, to be used for Linked Data and Solid.

    - Seems dead since 2014.

24. IDCoins [24] - A research project based on a Bitcoin like cryptocurrency model whereby participants use Proofs of Identity tests in order to have certain digital identity elements linked to public key cryptographic keys.

    - Seems dead since 2014.

25. GridSingularity*[18]* - Could not find enough information (Although the name was mentioned under this topic).

**Generic Blockchain**

26. BlockCypher[*16]* - A simple API for interacting with blockchains, accessed over HTTP or HTTPS from the api.blockcypher.com domain.

    BlockCypher supports Bitcoin, Ethereum, Litecoin, Dogecoin, Bitcoin Testnet3, and BlockCypher's Test Chain.

27. Namecoin*[29]* - A blockchain that has been conceived from the start to be used for registering domain names (DNS).

    It is the first fork of the Bitcoin software.

28. Regis*[22]* - A platform that makes it easy to build, deploy, and manage decentralized registries on the Ethereum blockchain.

29. BigchainDB*[19]* - A scalable blockchain database which allows developers and enterprise to deploy blockchain proof-of-concepts, platforms and applications with a scalable blockchain database.

30. Storj*[43]* - A peer-to-peer cloud storage based on blockchain.

    The first usable blockchain technology to provide an unalterable record-keeping system.

# References


**[1]** *S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf, 2008.*

**[2]** *I. Allison, "ConsenSys and Microsoft tackle human rights abuses with blockchain-based identity system", http://www.ibtimes.co.uk/consensys-microsoft-tackle-human-rights-abuses-blockchain-based-identity-system-1562722 , 2016.*

**[3]** *K. Hsu, "Identity Management on the Blockchain", https://decentralize.today/identity-management-on-the-blockchain-3fadf5f4bb36, 2016*

**[4]** *D. Shrier, W. Wu, A. Pentland, "Blockchain & Infrastructure (Identity, Data Security)", http://cdn.resources.getsmarter.ac/wp-content/uploads/2016/05/MIT_Blockchain_Infrastructure_Report_Part_Three_May_2016.pdf, 2016.*

**[5]** *EPFL, "Managing Identities Using Blockchains and CoSi", https://infoscience.epfl.ch/record/220210/files/1_Managing_identities_bryan_ford_etc.pdf.*

**[6]** *G. Zyskind, O. Nathan, A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data", http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7163223, 2015.*

**[7]** *J. Mattila, "THE BLOCKCHAIN PHENOMENON", http://www.brie.berkeley.edu/wp-content/uploads/2015/02/Juri-Mattila-.pdf, 2016.*

**[8]** *A. Wang, "Blockchain Technology and Its Applications", http://opensiuc.lib.siu.edu/cgi/viewcontent.cgi?article=1020.*

**[9]** *Amit, "12 Companies Leveraging Blockchain for Identification and Authentication", https://letstalkpayments.com/12-companies-leveraging-blockchain-for-identification-and-authentication, 2016*

**[10]** *William, "Blockchain for Identity management", http://firstyear.id.au/blog/html/2016/07/18/block_chain_for_identity_management.html, 2016.*

**[11]** *Uport - https://uport.me*

**[12]** *C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, M. Sena, "UPORT: A PLATFORM FOR SELF-SOVEREIGN IDENTITY ", https://uport.me/library/pdf/whitepaper.pdf, 2016*

**[13]** *HH. Buerger, "Ethereum White Paper", https://github.com/ethereum/wiki/wiki/White-Paper, 2016*

**[14]** *ConsenSys - https://consensys.net*

**[15]** *Blockstack - https://blockstack.org*

**[16]** *BlockCypher - https://www.blockcypher.com*

**[17]** *Hyperledger - https://www.hyperledger.org/community/projects*

**[18]** *GridSingularity - http://gridsingularity.com*

**[19]** *BigchainDB - https://www.bigchaindb.com*

**[20]** *Jolocom - http://jolocom.com*

**[21]** *Cambridge Blockchain - http://cambridge-blockchain.com*

**[22]** *Regis - https://regis.nu*

**[23]** *World Citizenship, a POC research - https://github.com/MrChrisJ/World-Citizenship*

**[24]** *DV. Duccini, "IDCoins: A Web of Trust Blockchain for Identity and Reputation", https://github.com/IDCoin/IDCoin , 2014.*

**[25]** *BlockVerify - http://www.blockverify.io*

**[26]** *BlockAuth - http://blockauth.org, http://neuroware.io, https://blockauth.com, https://techendeavors.com*

**[27]** *CryptId - http://cryptid.xyz*

**[28]** *CredyCo - http://www.coindesk.com/trustatom-raises-100k-blockchain-based-due-diligence-service*

**[29]** *Namecoin - https://namecoin.org*

**[30]** *NameID - https://nameid.org*

**[31]** *CertCoin Github - https://github.com/cfromknecht/certcoin*

**[32]** *C. Fromknecht, "CertCoin: A NameCoin Based Decentralized Authentication System", https://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf, 2014*

**[33]** *ShoCard - https://shocard.com*

**[34]** *ShoCard , "Blockchain revolutionizing identity management", https://shocard.com/cpt_news/blockchain-revolutionizing-identity-management, 2016*

**[35]** *ShoCard, "Identity Management on the Blockchain", https://shocard.com/cpt_news/identity-management-on-the-blockchain, 2016*

**[36]** *ShoCard, "ShoCard and SITA want to store your ID details on the blockchain to authenticate travelers", https://shocard.com/cpt_news/shocard-and-sita-want-to-store-yourid-details-on-the-blockchain-to-authenticate-travelers, 2016*

**[37]** *ShoCard, "How it Works", https://shocard.com/how-it-works/, 2016*

**[38]** *R. Dillet, "ShoCard Is A Digital Identity Card On The Blockchain", https://techcrunch.com/2015/05/05/shocard-is-a-digital-identity-card-on-the-blockchain/, 2015*

**[39]** *Ascribe GmbH - https://www.ascribe.io*

**[40]** *I/O Digital - http://www.iodigital.io*

**[41]** *B. Cooper, "Blockchain tech powers identity management", http://www.virtualcurrencytoday.com/articles/blockchain-tech-powers-identity-management, 2015*

**[42]** *ID2020 - http://id2020.org*

**[43]** *storj - https://storj.io*

**[44]** *UniquID - http://uniquid.com*

**[45]** *PIMN (Platform Identity Management Nederland) - http://www.pimn.nl*

**[46]** *L. Parker "ID2020, held at the United Nations, features 'lots and lots of Blockchain'", http://bravenewcoin.com/news/id2020-held-at-the-united-nations-features-lots-and-lots-of-blockchain, 2016*

**[47]** *L. Aru, "ID2020: How Blockchain Could Be Used To Solve Global Identity Crisis", https://cointelegraph.com/news/id2020-how-blockchain-could-be-used-to-solve-global-identity-crisis, 2016*

**[48]** *J. Schwartz, "Microsoft Among Those Pitching Blockchain at U.N. Summit To End Identity Crisis", https://redmondmag.com/blogs/the-schwartz-report/2016/05/microsoft-among-those-pitching-blockchain.aspx, 2016*

**[49]** *G. Prisco, "Microsoft Building Open Blockchain-Based Identity System With Blockstack, ConsenSys", https://bitcoinmagazine.com/articles/microsoft-building-open-blockchain-based-identity-system-with-blockstack-consensys-1464968713, 2016*

**[50]** *Department of Homeland Security, "Applicability of Blockchain Technology to Privacy Respecting Identity Management", https://www.sbir.gov/sbirsearch/detail/867797, 2015*

**[51]** *L. Parker, "Amid declining revenue Australia Post considers using a blockchain for identity management", http://bravenewcoin.com/news/amid-declining-revenue-australia-post-considers-using-a-blockchain-for-identity-management, 2016*

**[52]** *W. Zhang, "Blockchain identity management", http://bravenewcoin.com/news/blockchain-identity-management, 2016*

**[53]** *Bitnation - https://bitnation.co*

**[54]** *Bitnation on Wikipedia - https://en.wikipedia.org/wiki/Bitnation*

**[55]** *G. Prisco, "Estonian Government Partners with Bitnation to Offer Blockchain Notarization Services to e-Residents", https://bitcoinmagazine.com/articles/estonian-government-partners-with-bitnation-to-offer-blockchain-notarization-services-to-e-residents-1448915243, 2015*

**[56]** *B. Homes, "e-Estonia initiative progresses with blockchain partnerships", http://bravenewcoin.com/news/e-estonia-initiative-progresses-with-blockchain-partnerships, 2016*

**[57]** *A. Alender, "What is Estonian e-Residency and how to take advantage of it?", https://www.leapin.eu/articles/e-residency, 2016*

**[58]** *Future of Identity - http://www.futureofidentity.org*

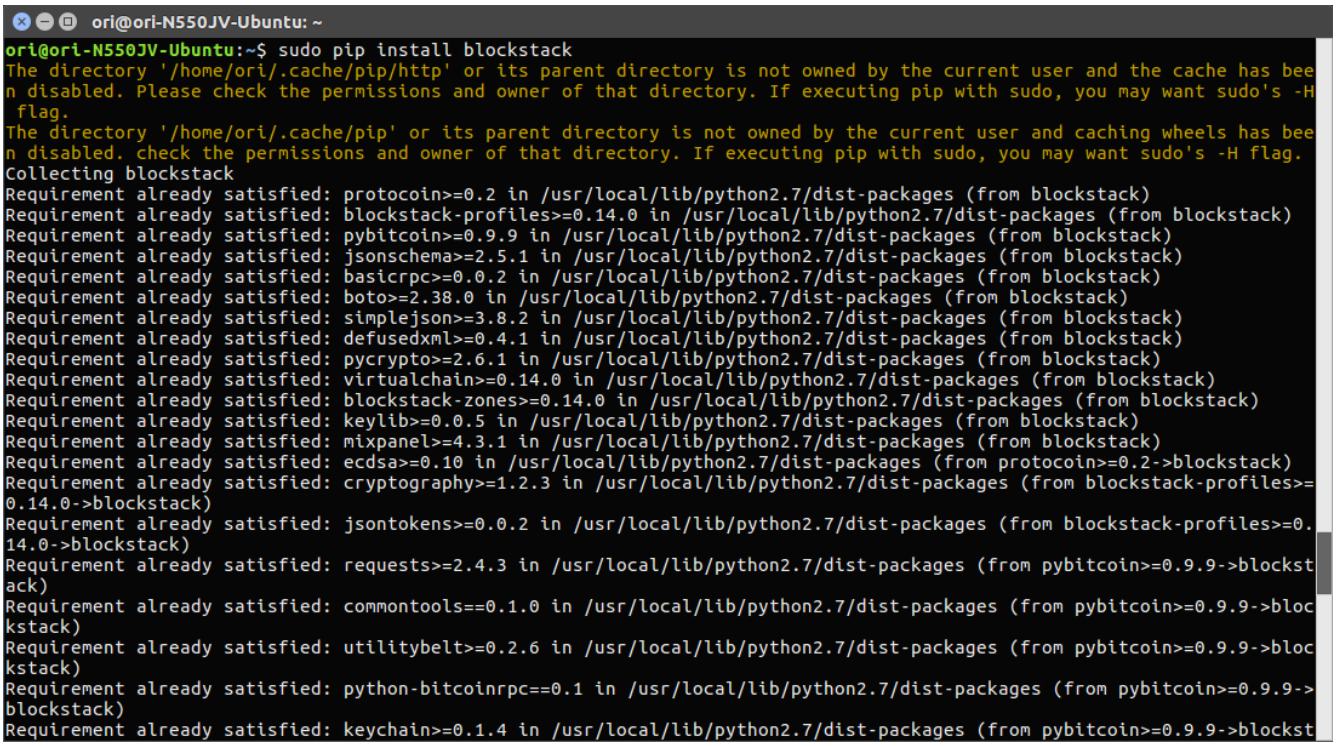
**[59]** *R. Jones, "Becoming a virtual Estonian", http://www.bbc.com/news/technology-36276673, 2016*

**[60]** *E-Estonia - https://e-estonia.com/e-residents/about*

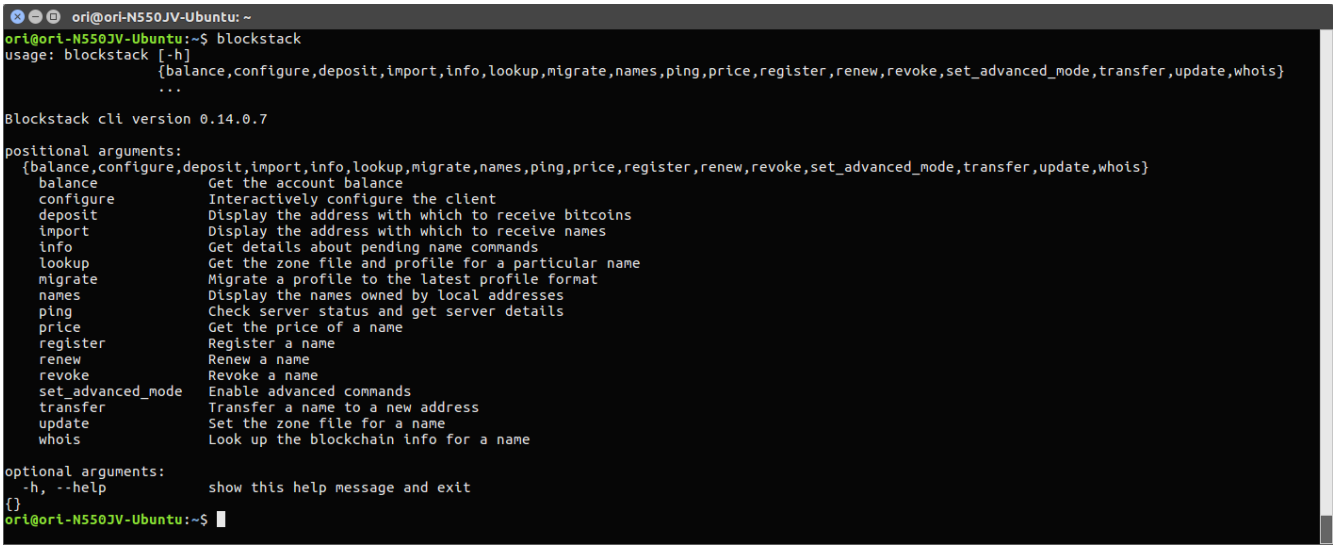
**[61]** *Identit - http://www.identit.ee*

# BlockStack

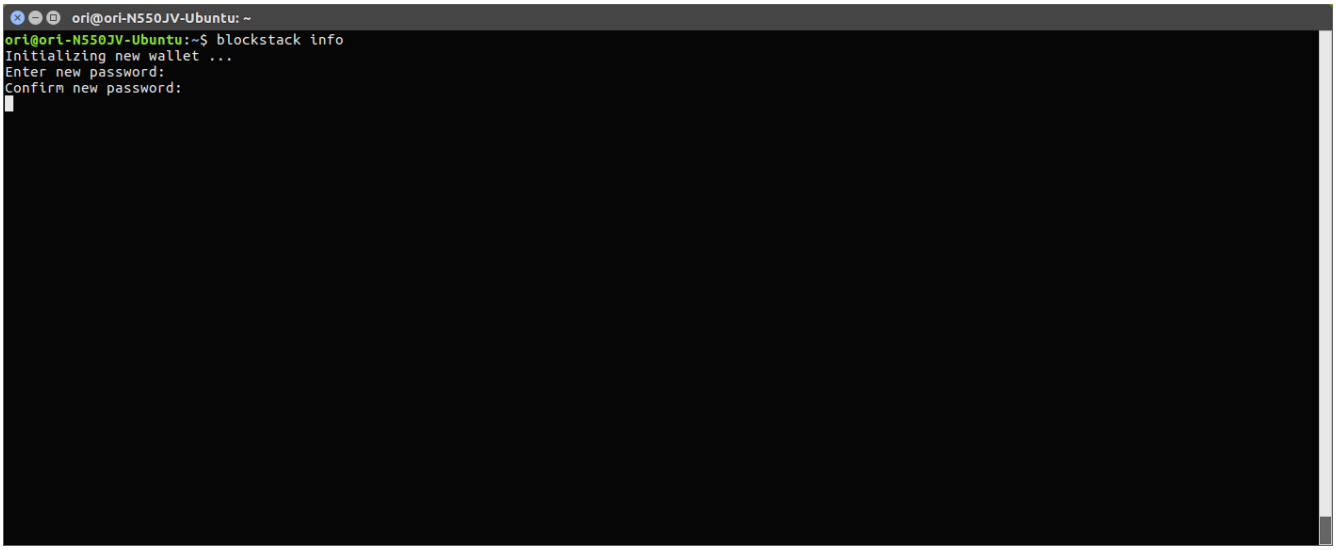
First, install blockstack using pip:

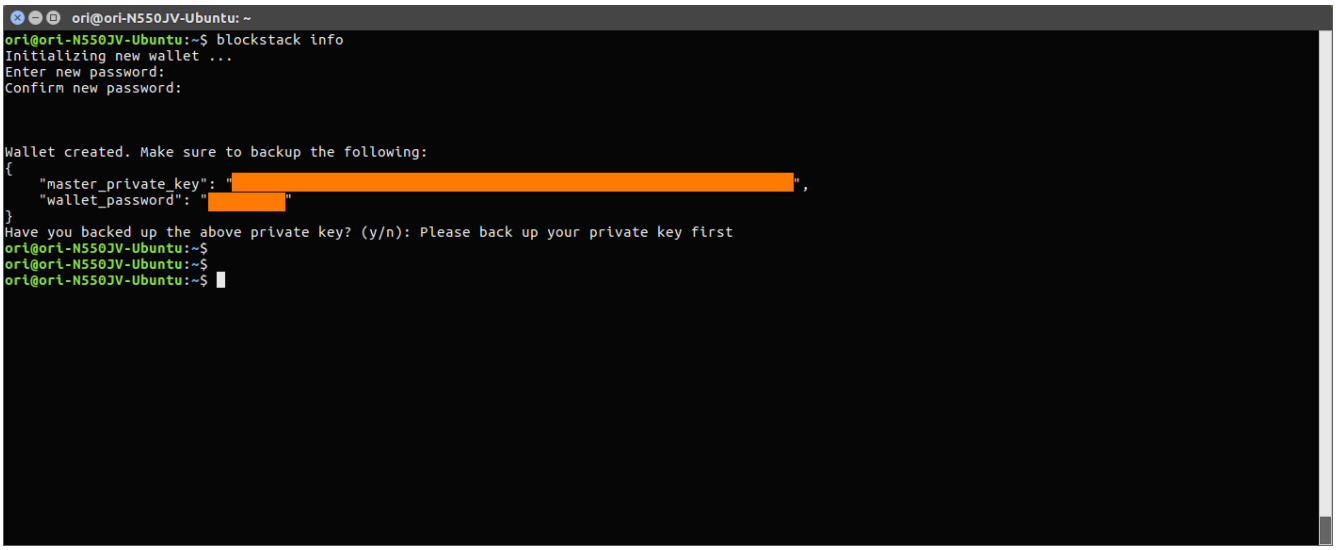



Make sure it was installed correctly:

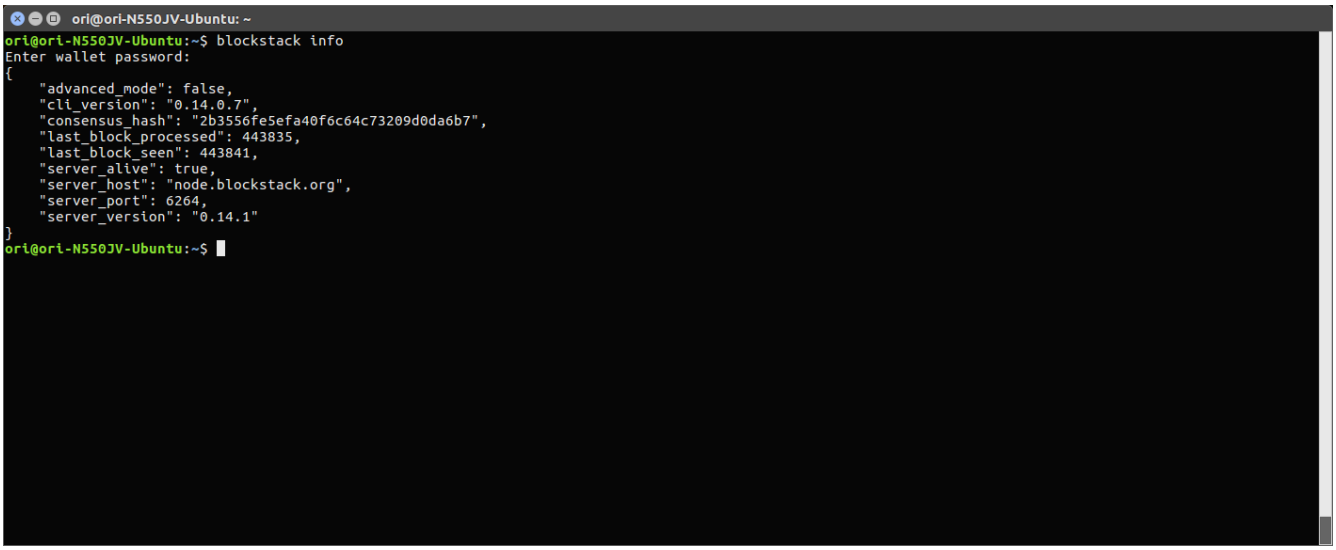


Initialize your account and supply a password:

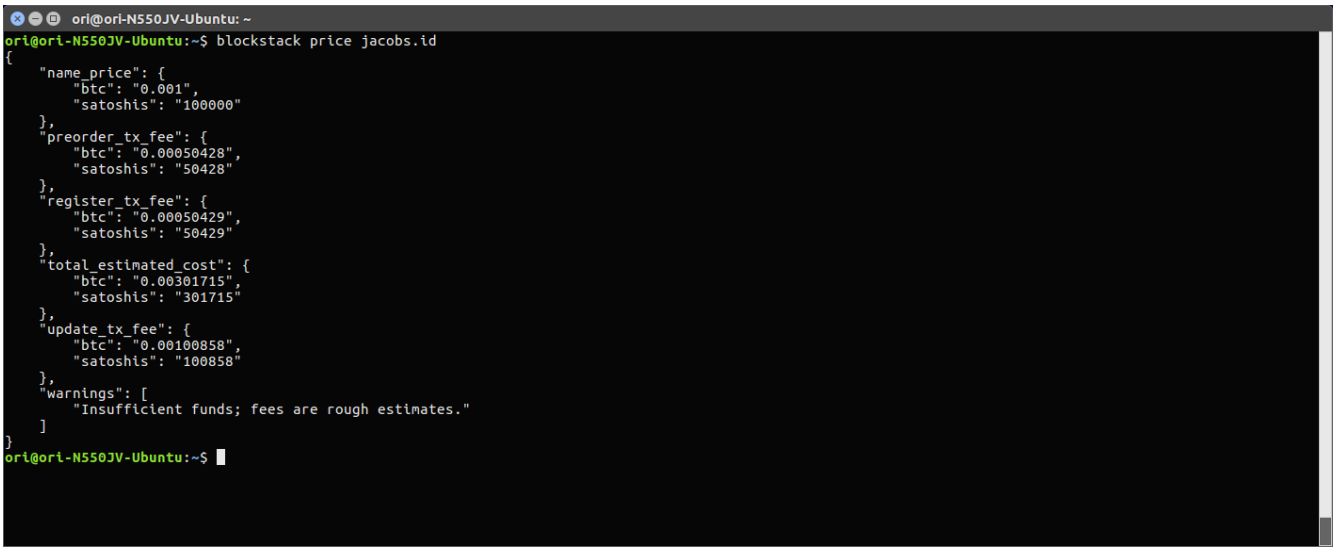


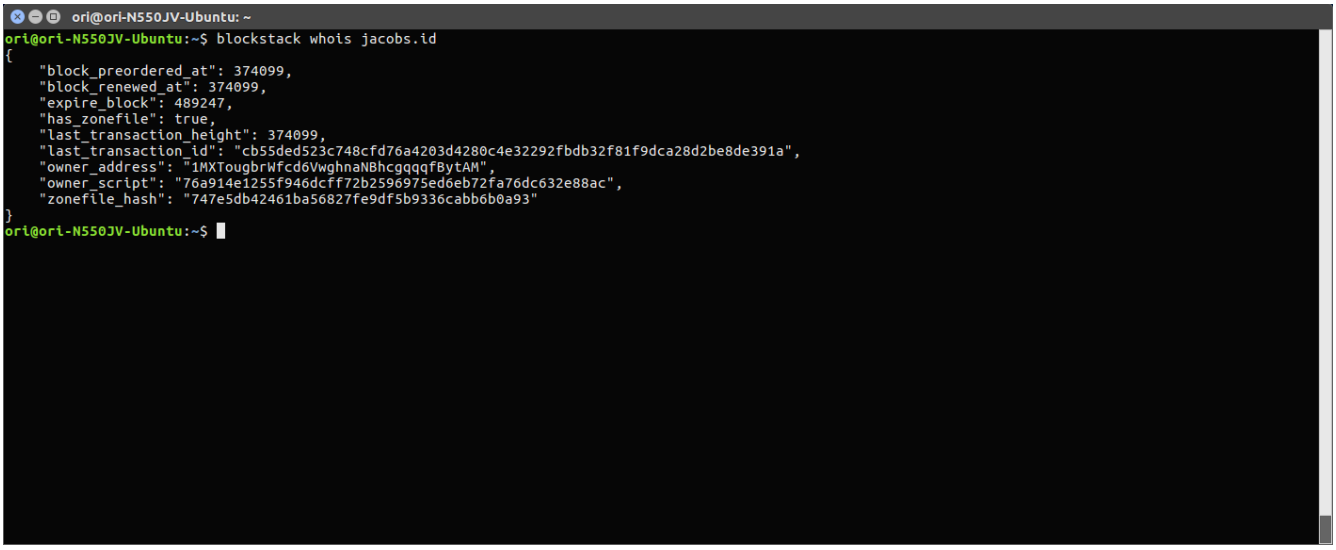
You can view your current information:



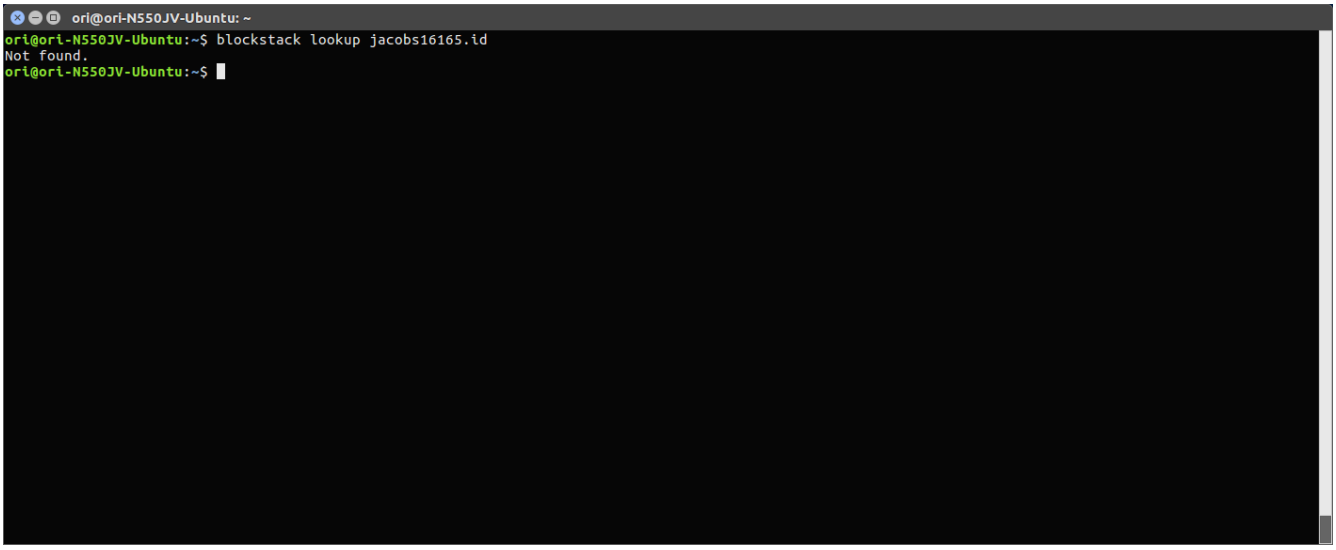

Estimate a price for a new name ID (In Bitcoin currency):



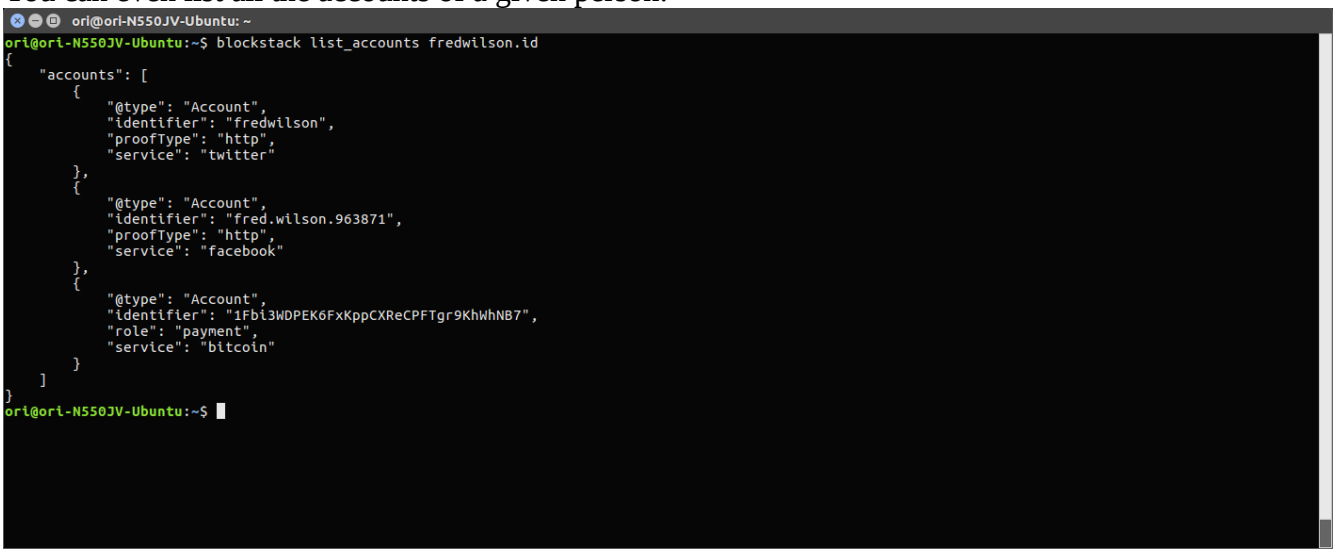
Lookup for identities using whois and lookup



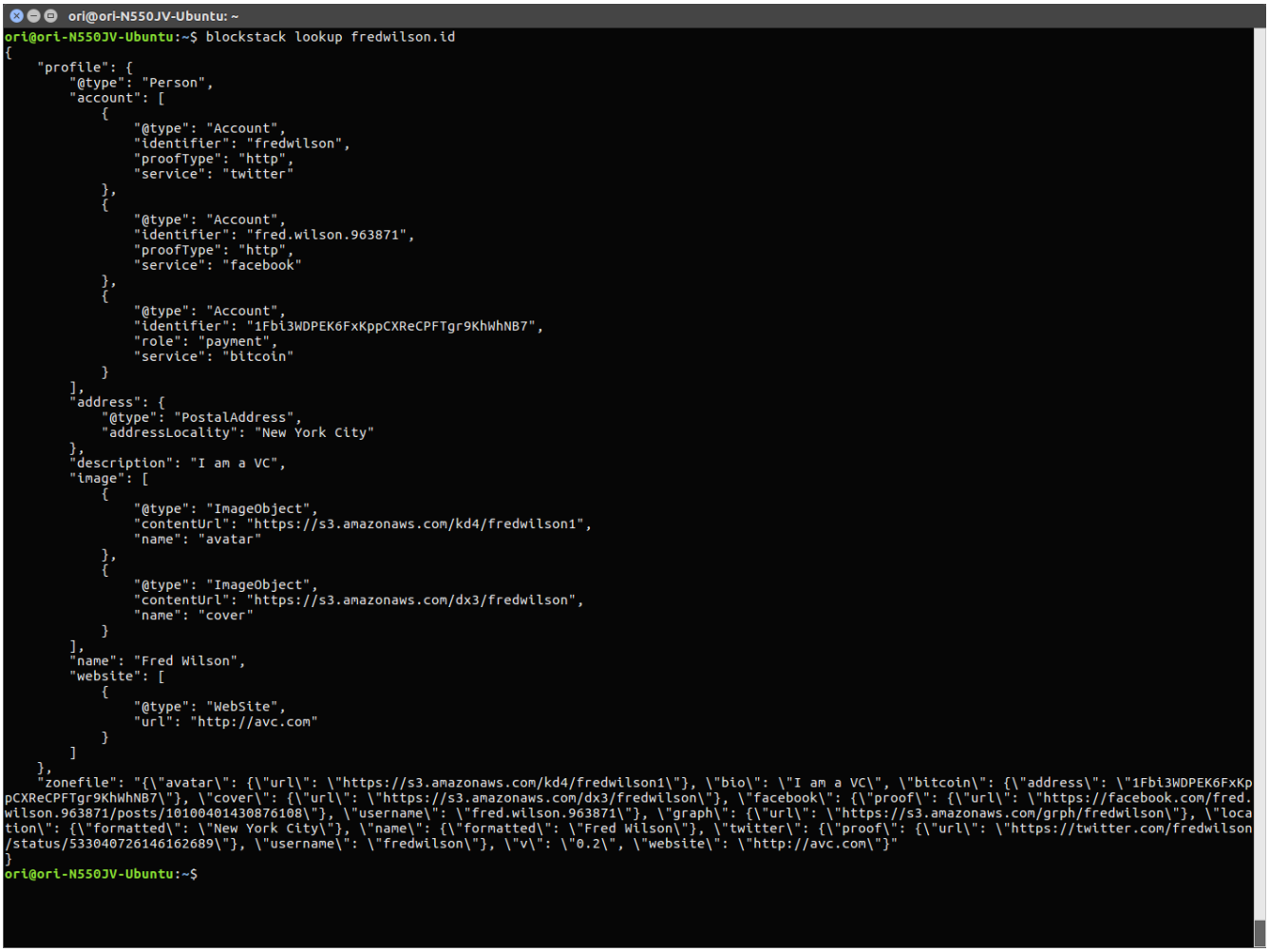




You can even list all the accounts of a given person:




Add another identities to your account (Including Facebook, Twitter, Microsoft and more..):



In addition, you can start your own blockstack server and add your machine to the public blockchain.