CREATE YOUR OWN

BLOCKCHAIN ID

CONCEPT BY: **CHRISTOPHER ELLIS -** PRESENTED BY **BITNATION**

CONTENT

- Preparations
- Background
- Overview
- Step 1 - Organize a meetup
- Step 2 - Meetup at a commercial venue
- Step 3 - Take photo with Merkle Root
- Step 4 - Sign with PGP Keys
- Step 5 - Sign with PGP Keys 2
- Step 6 - Design of the ID
- Step 7 - Timestamp it on the blockchain
- Step 8 - Print and laminate. Further reading.

WHAT YOU NEED TO DO THIS:

- PGP Keys - See tutorial here https://gpgtools.org
- KEYBASE.IO Profile - www.keybase.io
- Camera (a webcam or a cellphone camera is fine)
- Printer + Thick paper
- Laminator + Plastic sheet
- Scissors
- Laptop
- Internet connection
- Photoshop or similar program
- About 5-10 USD dollar in Bitcoin for the timestamp

BLOCKCHAIN ID

CONCEIVED BY **CHRISTOPHER ELLIS**

Original GitHub post: https://github.com/MrChrisJ/World-Citizenship

"*The goal of this project is to learn and layout a simple process for anyone in the world to create their own Private Passport Service that can be used to validate and prove the existence of other persons using nothing but available tools.*

We will prefer open source where available and we will draw on the cryptographic tools like Public Private Key Cryptography (PGP) and blockchain technology in the form of Bitcoin.

By doing this we aim to give people across the world the ability to grant one another Global Citizenship by virtue of their being witnessed in space and in time. This witnessing can be documented with photography and video, that content can be signed with PGP signatures, hashed and timestamped. It can then be joined with Social Network Validation services like Keybase.io before being plugged in to more dynamic reputation systems." - Christopher Ellis

WHAT IS THE ID USEFUL FOR?

- Identity for transactions (e.g. commercial transactions, signing contracts, etc) the web-of-trust component 'endorses you' to conduct transactions.

- Nobody can steal your identity to use it for fraudulent purposes (as opposed to emails or social network logins)

WHY IS THE BLOCKCHAINID IMPORTANT FOR THE WORLD?

- The reputation system rewards good behavior, and punish bad behavior. It makes people accountable, and incentivizes legitimate exchange of goods and services.

- It increases personal security, and integrity. No government or company can take away your private ID, like they can with a passport, for instance. You own your own identity.

SET UP A MEETING. Assemble a group of forward thinking soon-to-be world citizens and organize a meet up in your local town, using a service like www.meetup.com

MEETUP AT A COMMERCIAL VENUE: A group of soon-to-be World Citizens arrive at a commercial venue as advertised bringing with them their laptop and an eagerness to learn.

TAKE A PHOTO of the person(s) holding a sign of the Merkle Root (the Merkle Root shows proof-of-existence in a certain time). Group photos where individual headshots are cropped out for the IDs are preferable, considering the social validation aspect.
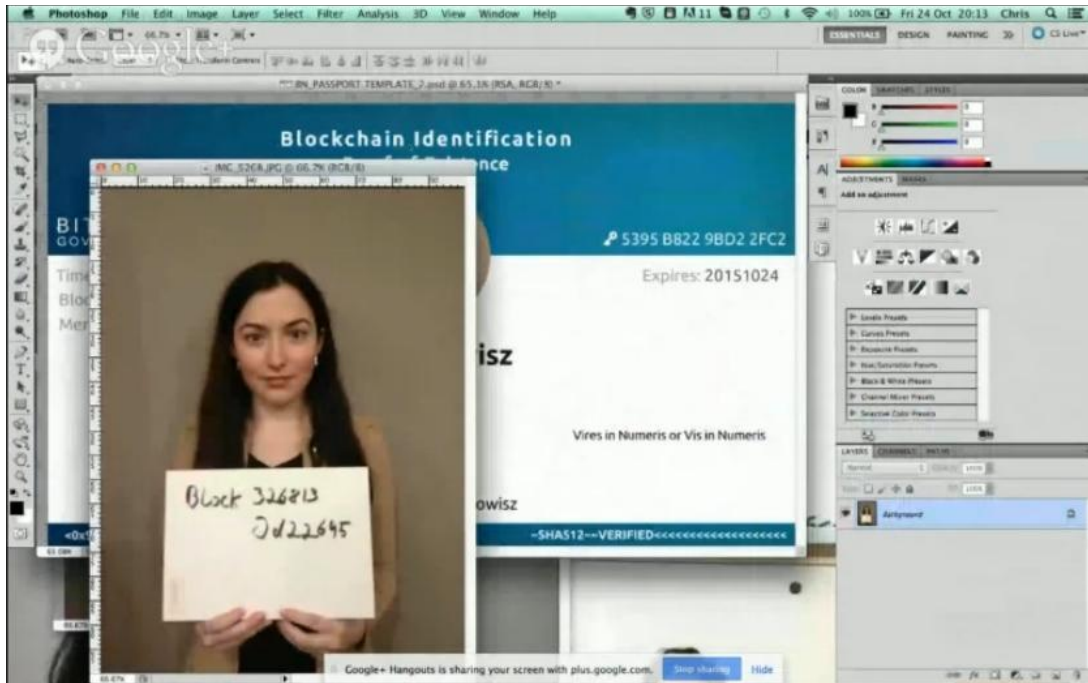
HOW TO GET THE MERKLE ROOT: Go to WWW.BLOCKCHAIN.INFO and clock on the block from the latest transaction on the blockchain, which will lead to a new page with the Merkle Root (the specific block identity).

New blocks are being created roughly every 10 minutes, and it's impossible to know the unique number in advance.

DESIGN THE ID: Insert headshot of the person from the photo/ group photo (save the full photo for the record). The ID can be branded as BitNation, World Crypto Network or something of the organiser's choice. It may be useful to prepare ID designs for different people ahead of the meeting with basic information like names on it, to speed up the process.

Include the following:

Name

Photo

Time stamp (see following pages)

Merkel root

Keybase.io address

Public key

Expiration date (expiration date should be

one year after the event, so people need to renew

it every year to make sure it stays valid in the

social context.

Blockchain Identification
Proof-of-Existance

BITNATION
GOVERNANCE 2.0

🔑 5395 B822 9BD2 2FC2

Time Stamp: 20141024 1800 UTC
Block: 326789
Merkle Root: 7146aa4bc51c453e
5d1f79e845dcc82e
5ee1071ea825f8eb
ba4b4f0dc71e5674

Expires: 20151024

Jenna Lowitz

Vires in Numeris or Vis in Numeris

keybase.io/janina_lowisz

<0x9BD22FC2<<RSA<<2048/4096<<AES256<   ~SHA512~~VERIFIED<<<<<<<<<<<<<<<<<

SIGN WITH YOUR PGP KEYS: Use the hosts PGP key, as well as your own, to publicly sign the completed image of the ID (JPEG or PNG file).

Sign through right-clicking on the image, and an option "sign" should appear. Click sign, and then a new signed document should be generated.

If someone at the meetup doesn't have a private key, they can go to a private room with their laptop and generate a new PGP Key.
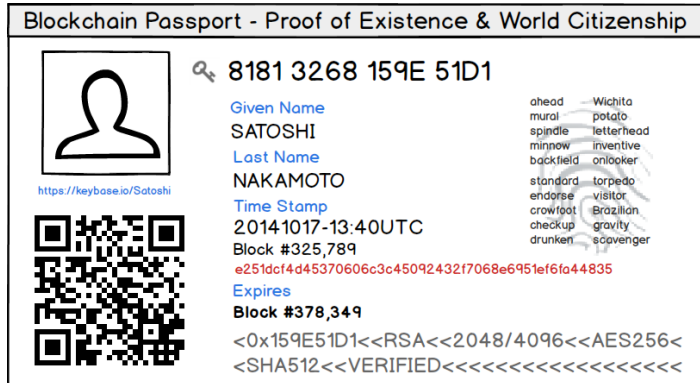
KEY-SIGNING 2: The new world citizen then has their PGP Key signed by others in attendance. A SHA256 digest of the key is then placed along with the key's ID into the Bitcoin blockchain using an address that is preferably owned by the venue hosting the event. If the person do not want to put their key on the blockchain, they can simply store the hash.

- By including the Merkle Root of the latest block we prove we have knowledge of an event that cannot have taken place any time prior the latest block being published.
- By signing the Passport with a PGP key we bind the state of the document to it's cryptographic signature preventing us from changing its contents without detection.
- By stamping the digest of the resulting passport and its signature in to the blockchain following these steps we prove that it existed in this state at no time later than the block in which it was published.
- By using the venue's address with a public IP address we prove that it exists in this space.

TIMESTAMP THE ID ON THE BLOCKCHAIN: You can use proofofexcistence.com to timestamp your documents. There are other websites offering the same service, however proofofexistance.com is the most userfriendly one.

The 3 different documents which needs to be timestamped are:

1. The JPEG file of the ID
2. The full image of the person(s) holding the Merkel Root
3. The signature of the host of the event (further signatures can be added later on)

You drag the documents from your desktop, and put them into the window on proofofexistance.com - which generates a hash, with an address.

You send your bitcoins to that address, to communicate to the blockchain that you have made an entry into the blockchain.
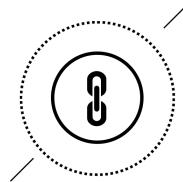
After the transaction, a link will appear with the transaction ID on the blockchain itself.

Print the design, laminate the print-out, and cut it so it fits your design nicely.

CONGRATULATIONS, YOU'RE NOW A WORLD CITIZEN!

Blockchains, Not Borders!

www.bitnation.co