CRYPTOCURRENCY REGULATION PROPOSAL

Terminology

Bitcoin:	The Bitcoin cryptocurrency, or other cryptocurrency.
User:	Someone active on a cryptocurrency network.
Bank:	A regulated financial institution, or governmental institution.

Introduction

This proposal mainly addresses the risks of cryptocurrencies due to their pseudonymous nature.

In addition, it is a solution for creating more trust amongst cryptocurrency users.

Pseudonymity

Although users/transactions of a cryptocurrency network are not really anonymous (pseudonymous), the more this network grows, the more time consuming and costly it will be for a government to detect any wrongdoing.

This calls for a solution providing transparency, ideally without interfering with the network's architecture.

1. Current scenario

Anonymous addresses are being used for sending and receiving Bitcoins, leading to anonymous/pseudonymous transactions on the Bitcoin network.

As experienced lately, this could open the door to illegal activities such as money laundering, drug trafficking and other.

2. Proposed scenario

Addresses will be registered/issued by an entity that is in possession of the user's verified identity.

This entity could be a governmental institution or regulated financial institution. In this proposal we choose a bank to fulfill this task, because of its expertise in the area of security and finance.

3. How will it help fighting fraud?

Addresses will be linked to a user's profile, providing governments with transparency about transactions on the Bitcoin network. This will in turn help keep fraudulent activities to a minimum.

4. Doesn't this mean violating one of the main principles Bitcoin was founded on, namely being an independent system unaffected by any bank or government?

No, the user will still be the only one in possession of the addresses' private keys, thus retaining full control. The bank will only keep the link between the individual and the public keys/addresses.

Even if a bank would go bankrupt, its (former) customers would still have access to their funds (Bitcoins).

5. In practice: Registering/Issuing addresses

It is common for a Bitcoin user to maintain multiple addresses for increased privacy and administrative purposes. Therefore a user should be able to obtain additional addresses at any time.

This calls for an automated process, most likely in the form of a web application made available by the bank or a central authority.

Obtaining new addresses

Users will first have to authenticate to the (web) application using the credentials (username and password) received from their bank.

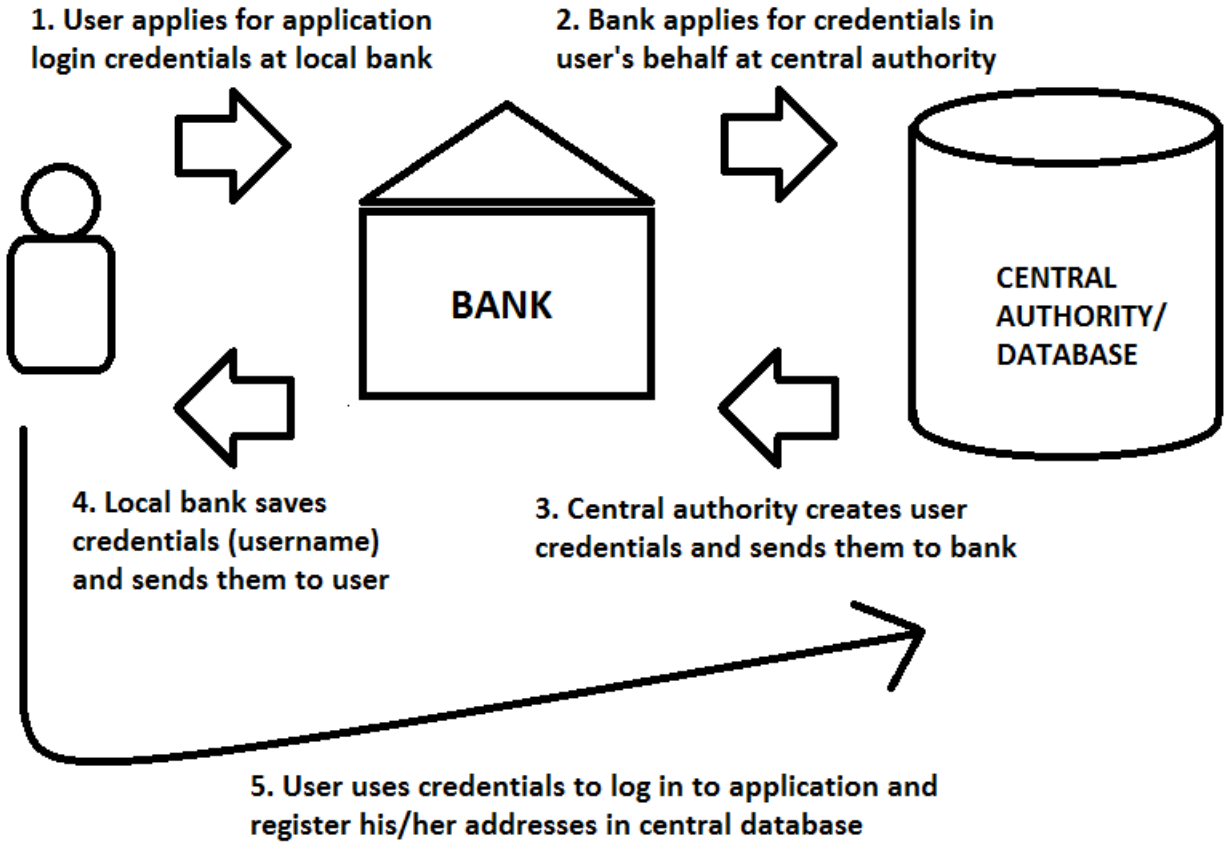
They can then choose the number of new addresses to create.

After confirmation, the (web) application will generate the requested addresses and will save the addresses (or public keys) together with the user's profile.

The newly created addresses and corresponding private keys will thereafter be securely presented or sent to the user, who can immediately start using them within the Bitcoin network.

Note that keeping the private keys secure will still be the user's responsibility. The application should not keep a copy of the private keys.

Figure 1: Registering addresses



6. In practice: Tracing user transactions

If, in case of suspicion of fraud, a government would need a list of transactions an individual has made within the Bitcoin network, the Bitcoin block chain can be queried for all transactions containing the registered addresses of that individual.

How to trace the other party of the transaction?

Countrywide

If the other party has to follow the same regulations (lives in the same country), the address will also be registered within the system[1] and can be looked up (reversely).

[1] Note that it would be more convenient for this to have a central system (countrywide) for keeping records (as shown in figure 1), instead of each bank maintaining their separate system.

Globally

A. Implementing a globally accessible central system

When using a central system that is accessible by any country, Bitcoin users across the world would have their addresses registered within the same system. Consequently it will be possible to trace both parties of any transaction.

As this solution may not always be desirable for a government because of privacy and security reasons, further options will be explored.

B. Implementing a link between an address and the issuer using the block chain

If the transaction's counterparty is from another country, and thus not registered within the system, a way to trace the foreign address is by firstly finding out its issuing country. A government can then cooperate with the foreign issuer to complete the trace.

To be able to determine the issuer of an address, a link between the address and its issuer is needed.

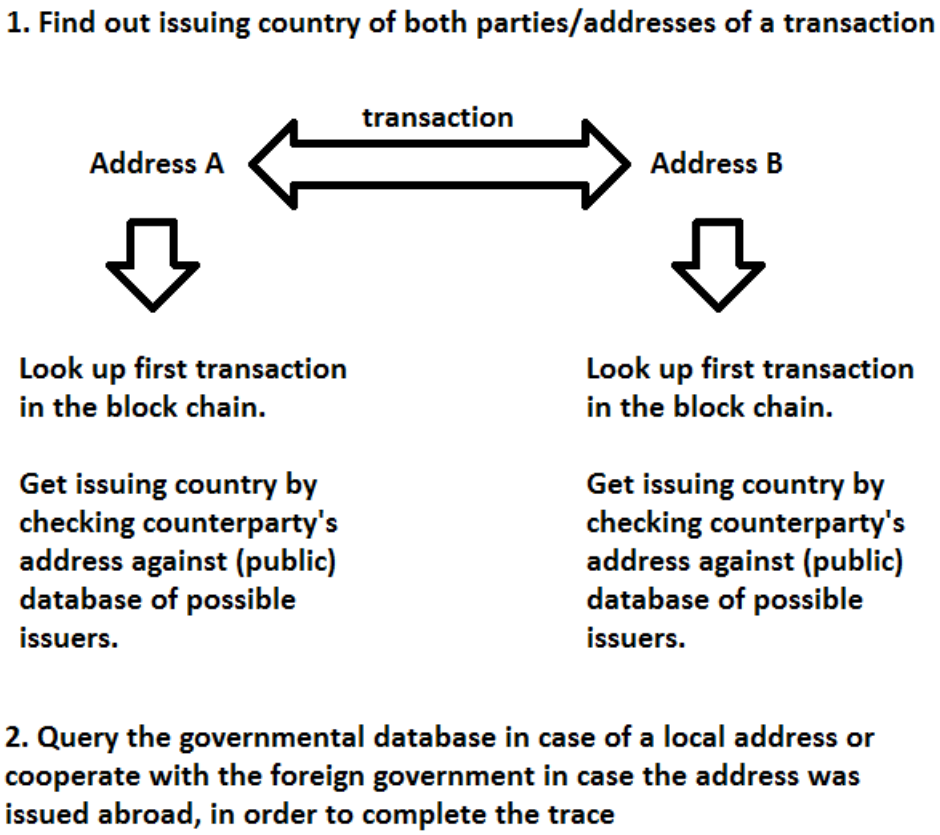
An implementation of such a link can be as follows.

Before sending a newly created address to the user, the (web) application will create an initial transaction on the block chain using the new address and a predefined issuer's address (comparable to a BIC/SWIFT code). This can be achieved by sending a token or small amount of value[2] (0.00000001 BTC) to the new address.

The issuer can then be found by looking up the first transaction of an address in the block chain.

[2] The amount of value can be reclaimed immediately or afterwards.

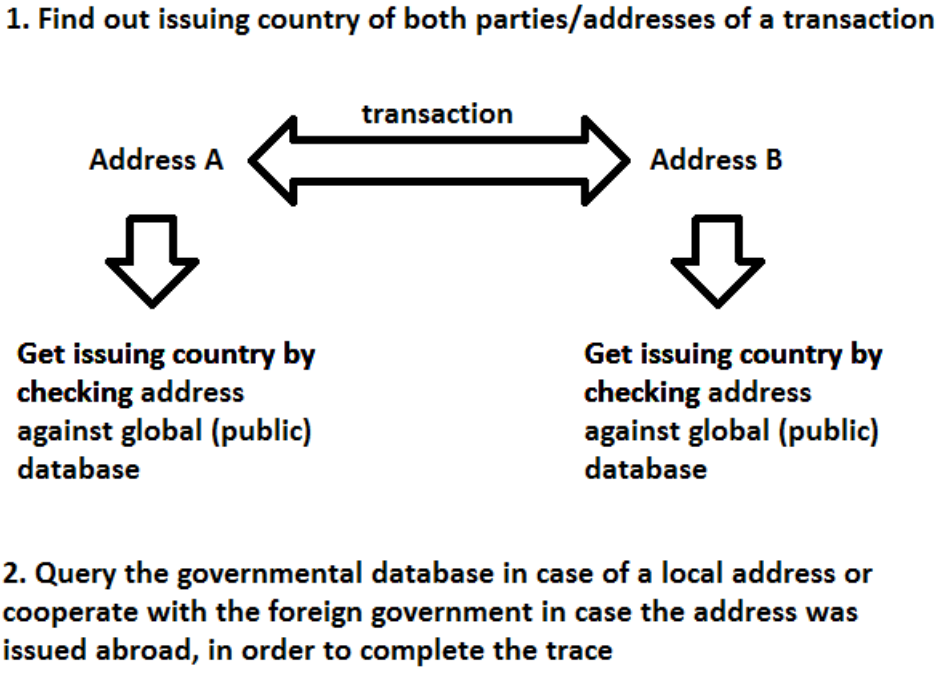
Figure 2a: Tracing user transactions



C. Implementing a link between an address and the issuer using a global database

Another way to implement a link between an address and its issuer is by using a global database where a link is being kept between any registered address and its country of issue.

Figure 2b: Tracing user transactions



7. Will users' privacy be affected?

Users will still retain their anonymity on the Bitcoin network. Depending on the implementation, another user can at most learn about the issuer (country of issue) of a particular address.

8. How will it create more trust amongst users?

A user or business will be able to check whether the counterparty's address is a registered address by checking if a link between the address and any issuer exists (as explained in 6B and 6C).

For a business, this can also contribute to the KYC (Know Your Customer) process.

9. What about current (unregistered) addresses?

Funds from unregistered addresses can be transferred to registered addresses.

Another possibility is to allow registration of current (unregistered) addresses, by means of proving ownership of the address (which can be achieved by signing a specific message).

Dario Di Pardo