Decentralized & Encrypted Notary Blockchain Service
For a pre-stated CBDC.

User Identity protection and system integrity problem state solution by
DEV.Joaquin Rodriugo Avendaño de la Selva.

SHORT DESCRIPTION

Sharing and recording information in a DLT or Blockchain network has many applications. Before any specific detail about what kind of information can be shared to be recorded, let's keep in mind that; a person-to-person network was designed to share files for them to be available to download and stored in a local memory/vault.
This is different from sharing the information of what the files contain, like the type of information shared in a bank network.

For example:

A and B can share the information attached from a movie file or share the file that contains the movie.
When they only shared the information attached, neither of them can actually play the movie. Which is different from sharing the file that contains the movie to be played.

And when a Bank A shares with a Bank B the information of the amount of currency that one of his clients/users is transferring from bank A to bank B. The file they share does not contain the currency that's being transferred, just the information for bank B to make the deposit of the currency that's in the file info.

By acknowledging this difference of process; to be applied in a DLT. We can think of a bank transfer or payment like sharing the information attached to what the movie files contain. And a CBDC transfer or payment as sharing the movie file to be stored in a local vault.

At this point the first thing to take in consideration is that a file that contains a movie once is shared and downloaded; is that, the file can be changed and multiplied.
To prevent this; experience in p2p networks has shown that stating a file in a decentralized network with a shared protocol for modifications where files in the network can not be modified without the consent of 51% of the participants in the network prevents the multiplication of files if that is not a permitted function. Also a decentralized network has shown to provide the best security protocol to protect the information attached to the shared file by applying a p2p or block to block encryption for it.

Therefore if a CBDC is emitted. The best network protocol to protect user Identity and maintain the integrity of the system while monitoring to validate.Is the one that applies an encrypted decentralized network with central banks included as a node to valided in the network and particular institutions or software service providers included as notaries to provide access to managing tools for the attach data and the files related to CBDC.

To provide an efficient solution to invalided a not defined or illegal operation in the network service . A CBDC must be pre-stated in two groups or sets of exceptions:

1.- In which cases a vault is permitted to receive a transaction or payment. For this group the service is being applied to the file shared in the network.

2.- Once the transaction is complete which tax regulation or retention is applicable for it.For this group the service is being applied to the attached information to the file that's being shared in the network.

Applying a pre-stated file for a CBDC in an encrypted and decentralized network has more than just identity security and system integrity application benefits. Emitting a pre-stated CBDC will provide an automated network for local authorities and citizens to inform and approve of any of the specific commercial activities that generate their incomes or to inform and validate their transactions of payments.
This means a full collaboration between central banks to define and emit a pre-stared CBDC for services providers to produce efficient, accessible and escalable tools to manage a CBDC.

Description of the service.

When a system for transactions or payments for some fiat currency is at work. The system tasks to complete the transaction have some information or data correlated to it.

A.-The person or entity that is sending an amount of currency as a payment for a product or service.

B.-The person or entity that receives an amount of currency as a payment for a product or service.

And the process to be completed can be described within tree steps or states.

State 1
A owns x_1 amount of y_1 currency.
B owns a payment agreement or contract with A for an x_2 amount of a y_1 currency.

Note that x_2 does not need to be a one-time event; that will depend on the contract A accepted with B, this implies that the contract needs to be addressed for a specific period of time given with a date and a specific number of events for the task in the system to proceed.

State 2

A transferred x_2 amount to be B. And A completes a partial or full compromise in the contract with B.
Thus the system has to actualize to A owns(x_1 - x_2) amount of y_1 currency.
B received x_2 amount from A.
And delivered A from the compromise in the contract for what was previously agreed for that date.
Thus the system has to be actualized to; B owns x_2 amount of y_1 currency that received from A as payment or transaction. And A completed what's on the contract With B for the date the task was completed.

State 3
B transfers a note to A as a receipt for the x_2 amount of the y_1 currency.
Thus the system has to be actualized to; A owns a receipt note from B. And B completed what's on the contract With A for the date the task was completed.

This process takes place for every payment or transaction made with a computer system. And can contain personal and public information or data.

And in most cases this information needs to be recorded for administrative purposes or legal compromises. And the system managing is obligated to complete the task for both parties and guarantee that the personal information of the participants it's not being shared without previous consent.

For the computer system that's managing transactions and taking legal responsibility for its obligations. These are, complete the task for parties A and B, keep a record, and give guarantees that personal information it's not being shared with previous consent.
The most trustable procol is an encrypted and decentralized one.
For the following reasons or motives:

1.- With decentralized protocol for sharing or sending data the systems participants or nodes can´t monopolise tasks or data from parties or systems users.The system integrity can be guaranteed because in a decentralized system protocol the nodes that participate to complete the task share the compute process and information in the network.
This type of network is known as a DLT, blockchain or blockchain inspired network.
Which adds an extra function for any node. If the task can not be completed with its own process, the process can be shared with any other node that can complete the task on the date previously agreed to take place; and when needed, to make a record of all states that took place while completing the file and file information shared or transferred.

2.-With a decentralized and encrypted protocol or blockchain system for the secureness of the personal data that's being shared or transferred it's theoretically impossible to break through its records without previous consent.

This protocol has already been tested with the cryptocurrency named bitcoin.
However, the protocol guarantees the system integrity; parties' or users' experience has shown the need for a third party or notary to participate as a service provider for the

following administrative and legal reasons. And by implementing a pre-stated CBDC for the benefits explained in the short description. The process to complete can include the following specific tasks for states to be validated or to be invalidated.

To define an efficient, accessible and manageable pre-state, it will be needed to add the following tasks to complete for states 1 to 3 from a transaction or payment.

Pre- state 1 = State 1 + Service task

State 1
A owns x_1 amount of y_1 currency.
B owns a payment agreement or contract with A for an x_2 amount of a y_1 currency.

Since partie A and B have the simultaneous legal responsibility to inform the local authorities from which activity belongs their owned amount of currency to be applied to complete a payment or transaction ; the service provider may include a smart contract template to complete the task, this smart contact can be defined by a central bank with the specific exceptions to validated or invalidated state 1, depending on the local regulations. Hopefully at this point the “pre-stated CBDC” concept is clear. There for.

Service task
Will be to share the encrypted information attached to state 1 with the local authorities for them to validate. And to attach the validation to the owner's file or CBDC.

Therefore;

Pre- state 2 = State 2 + Service task and **Pre- state 3 = State 3 + Service task**

Applying this specific task protocol with the blockchain inspired network provided by the Corda system will be a manable task to add and to be included in the benefits in the framework for service providers, users or CBDC owners and local authorities.