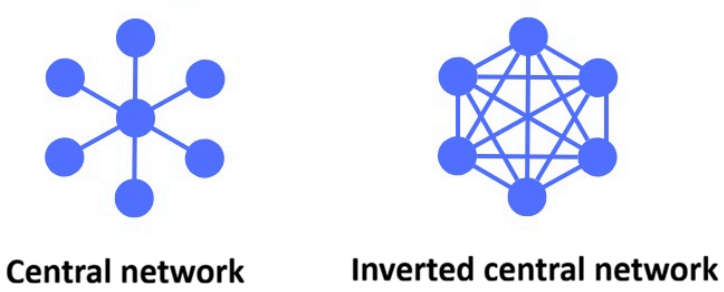
Inverse central network with payment channels and 3-party novation

Johan Nygren

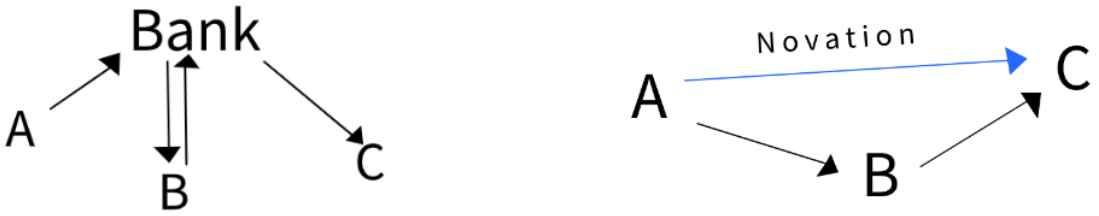
The simplest way to scale blockchain payments is by a payment channel routing network that has the architecture of an “inverted central network” and that manages the asymmetry of payments by 3-party novation. This system is the same architecture as the global banking system since the Enlightenment, but with payment channels instead of trust. It is very fast and also trustless.

Payment loops

Payments can be viewed as a loop clearing mechanism. The simplest loop clearing system is “barter”, i.e., two nodes making payments in two directions (that thus form loops), but this fails when payments become asymmetrical (i.e., one node may primarily buy from another node but not sell to them). The simplest loop clearing systems for asymmetric payments is to use a central intermediary. It makes any payment a node does with any other node behave as if it was “barter” again between the node and the central intermediary. The second simplest loop clearing system for asymmetric payments is novation. With novation, the central network can be “inverted” so that rather than a central intermediary, every node has a link to every other node. Through the mechanism of novation (that can be reduced to always only be between three nodes), debts can be rearranged so that the result is identical to the central network, accounting-wise. Novation thus finds “virtual loops”, loops that would have existed had the network instead organized via a central intermediary.



Novation is that when a node is an intermediary in terms of debt, they have both debt in and debt out, they can ask to move that debt directly between the debtor and the creditor. The result is the same as if there was a central intermediary in between the nodes, since with the central intermediary the node that was intermediary in terms of debt would have formed a loop with the central intermediary.

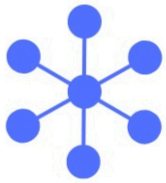


The banking system

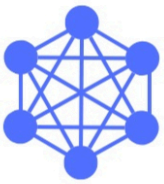
Historically payments were scaled globally by this type of inverted central network. Since it requires complete trust internally, is would typically be run by a group with complete trust internally, such as a family (the Medici or the Rothschilds, etc) or an ethnic group. But with payment channels, the “trust” becomes trustless links between the nodes. The inverted central network itself is identical to how payments were scaled globally historically, but with “collateral” on a blockchain and trustless links between nodes, it no longer needs to centralize to family or ethnic group.

The routing network

The banking network is a routing network, that is single-hop in terms of trust, and uses three-party novation to conform its accounting internally to that of a central network. Under each router is a regional bank, and the users interact with the routing network via these banks. The users have payment channels to their bank (and the bank to the users), symmetrically. This is the same architecture that scaled payments globally since the Enlightenment, but with payment channels instead of trust. Thus fast, but still trustless.



Central network



Inverted central network

Two-tier with inverted core

Payment coordination

The payment coordination is a two-phase commit with a prepare step followed by the commit step. The prepare step at any hop can be aborted at any time if both peers in the pair agree on it. To enforce cooperation to abort, a “double deposit” is used. Not just the “money-out” peer locks the amount to transfer, but also the “money-in” peer. To enforce cooperation on commit, a hash lock is used where the preimage can be published on-chain to force the transfer. The recipient releases the preimage. To enforce that the recipient releases the preimage, the prepare step at the last hop has a timeout.

The reason these simple rules work is because in a 3-hop payment, the central pair (B to C in A->B->C->D) have oversight of the full payment chain, whereas in 4-hops or more no one has oversight. The first two pairs can thus reserve money without a timeout, as there is no uncertainty about when they should abort. But as they abort manually (rather than with a timeout) they need a mechanism to enforce cooperation, and the “double deposit” provides this. And, to enforce the hash lock preimage release, a timeout is still needed but this is only at one hop (thus avoids entirely the race condition problems that come with chained timeouts).

Novation coordination

The novation uses the same coordination as payments. It first searches novation paths. Each node that is an intermediary in debt asks their money-in and money-out peers if they agree to novation.