

Flame

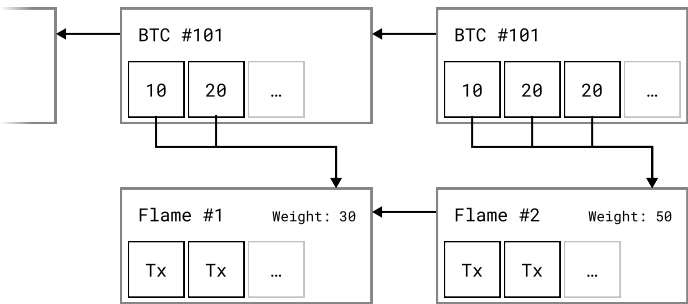
runflame.org

Decentralized electronic cash with confidentiality and smart contracts

Flame is a Bitcoin-based electronic cash network that combines confidentiality, programmability and fast payment verification. Minters continuously burn bitcoin to support valid transaction histories and earn newly issued flames. A unified virtual machine brings confidential transfers, programmable contracts and persistent actors into one network.

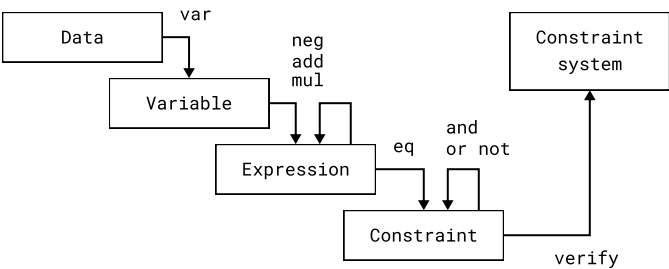


Proof-of-burn consensus



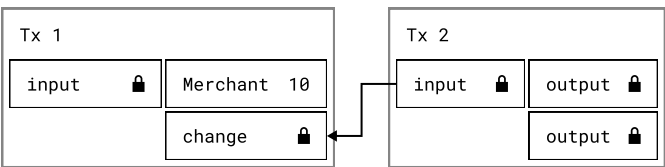
Minters burn bitcoin and publish endorsements that give Flame blocks weight. Nodes choose among valid histories using logarithmic block weights, favoring sustained support and discounting late endorsements; newly issued flames reward minters in proportion to their contributions.

FlameVM: programmable constraints



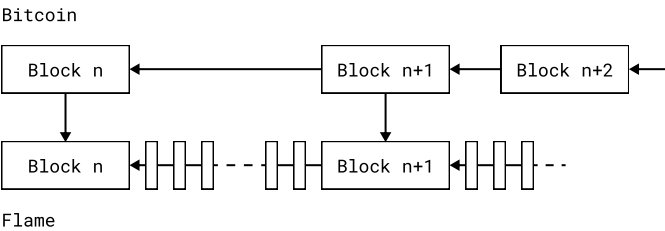
FlameVM combines arithmetic expressions and logical conditions over hidden values into a single Bulletproof within each external transaction. Contracts can verify confidential prices, limits and other rules without revealing the underlying values.

Confidentiality



Amounts remain hidden from the network: the merchant sees its payment, but not the sender's balance, change or later transfer amounts. Cryptographic commitments conceal values while nodes verify transactions; the transaction graph remains public.

Fast payment verification



Minters use BFT pre-agreement to produce intermediate blocks between Bitcoin blocks, offering early payment assurance. This is not finality: smaller payments may accept the additional risk, while stronger assurance requires Bitcoin-recorded endorsements and subsequent Flame confirmations.