

Flame: The Future of bitcoin

Confidential electronic cash and smart contracts, built on top of Bitcoin

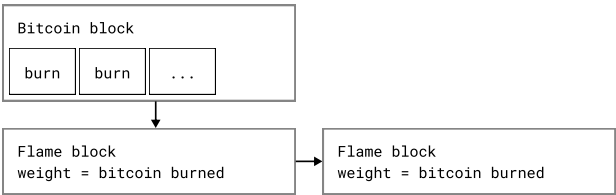
The world today

About two-thirds of crypto’s value sits in Bitcoin: the most trusted asset, but slow to confirm, with no on-chain privacy and little programmability. The other third sits in altcoins that add features at a price – centrally controlled tokens.

What Flame does

Flame is a new decentralized network that extends Bitcoin instead of competing with it. It adds confidential payments, smart contracts and fast payment confirmation, without changing a single Bitcoin rule.

1. Secured by burning bitcoins

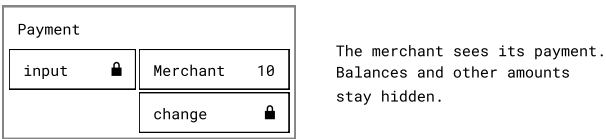


Instead of mining with electricity, participants (“minters”) burn bitcoins to vouch for the network’s history. The cost is real and irreversible, so rewriting history is expensive. Minters earn newly issued flames.

2. Fair by design

No premine. No allocation for founders, team or investors. Every flame is issued through the same open process, burning bitcoins, and everyone takes part on equal terms. Total supply is capped at 21 million flames.

3. Confidential by default



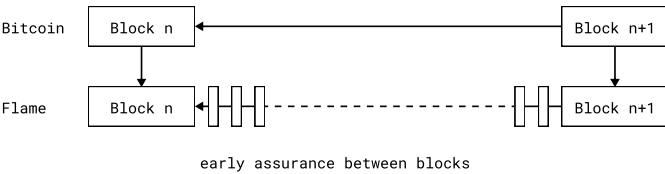
Amounts and balances are hidden from the public, while the network can still verify that no money is created or spent twice. Transaction graphs stay visible, which keeps double-spending prevention efficient.

Bitcoin	2/3	Altcoins	1/3
---------	-----	----------	-----

Store of value Functionality

	Bitcoin	Altcoins (fragmented)	Flame
1. Decentralization	+	-	+
2. Fair launch	+	-	+
3. Confidentiality	-	+	+
4. Speed	-	+	+
5. Programmability	-	+	+

4. Light and fast



Users keep their own proofs of ownership, so the network stays small and scalable. Merchants get early payment assurance before the next Bitcoin block arrives; final confirmation follows from Bitcoin.

Users can decide how much time they want to wait depending on transaction volume.

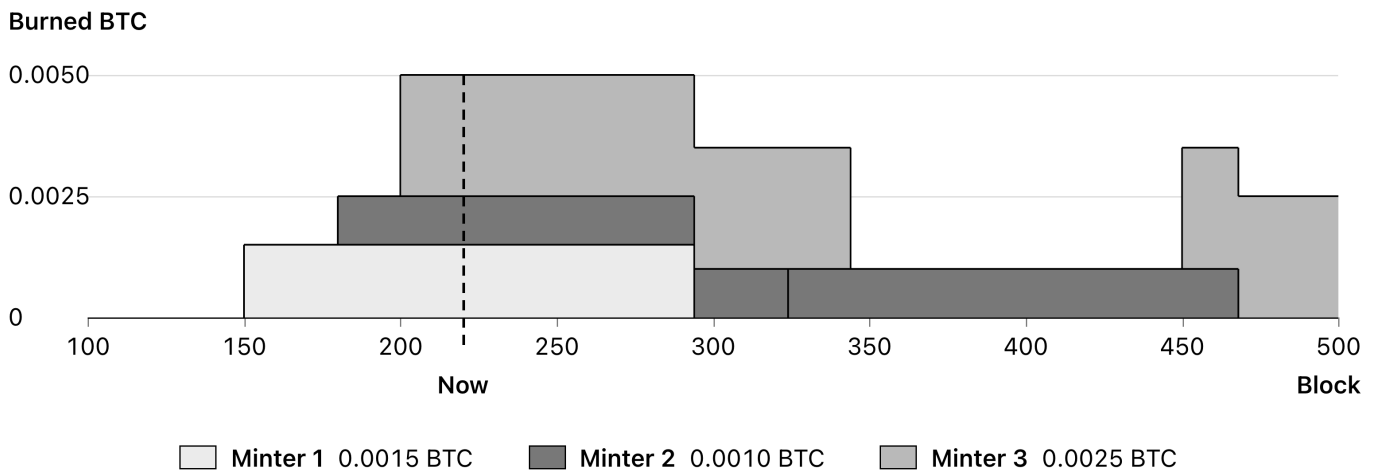
Time to approve tx in a Flame block	~ 2 sec
Time to approve tx in a Bitcoin block	~ 10 min
Time to get more approvals (6 blocks)	~ 1 hour

5. Programmable money

FlameVM lets developers build escrows, shared wallets, exchanges and lending, including rules that work on hidden values, such as checking a price limit without revealing it. Escrow multisig payment channel stablecoin custom token DEX vesting salary system dead man’s switch treasury and more

A few points about minting

1. Minters endorse (vote for) every block with their bitcoin.
2. Initially, each block distributes 50 flames among all minters, in proportion to their bitcoin stake. This amount halves every four years, as in Bitcoin, and total supply is capped at 21 million flames.
3. Every mint is a commitment of at least the next 144 blocks (about 24 hours).
4. The whole amount of bitcoin is burned upfront and spread evenly across the blocks of the period (144, or more if a longer period is chosen).
5. The number of minters and their stakes in each block determine the satoshis-per-flame rate for that block.
6. Each minter pays a Bitcoin transaction fee of about \$1 per block (estimated), which may affect minting strategy. Delegated minting will be allowed by the network rules once the work is finalized and minting has launched (January 2027 estimated).



Minting simulation model. For illustrative purposes only.

Why Bitcoin benefits

As block rewards keep halving, Bitcoin's security will depend more on fees. Every Flame endorsement is a Bitcoin transaction that pays for block space. Burned bitcoins are permanently removed from circulation, which changes the supply. All without touching Bitcoin's issuance.

Status

Minting starts January 2027 (estimated). Work in progress.

Creator & Architect: Oleg Andreev

Previously co-author of TxVM and ZkVM at Chain and Interstellar, the predecessors of FlameVM.

For further questions

Dasha Mukhina, head of common sense, dmukhina@andreevco.com.

