



Quantum-safe money on a *five-second BlockDAG*.

The Internet Money whitepaper: how quantum-safe wallets, built-in tokens and a fast, GPU-mined BlockDAG fit together.

§1

ABSTRACT

Internet Money (IMN) is open-source proof-of-work money built to stay secure as quantum computers arrive. Every wallet is locked twice: with Ed25519, today's proven signature, and with SQIsign, a compact post-quantum signature. Spending needs both, so coins stay safe while either scheme holds.

Tokens, an order-book market, escrow, subscriptions and theft-resistant vaults are part of the consensus rules, not smart contracts. Anyone can issue a token and trade it without an exchange, and every node checks every rule.

Blocks arrive every five seconds on a GHOSTDAG BlockDAG, so blocks found at the same moment are kept rather than wasted. Mining uses Hallmark, a memory-hard algorithm suited to ordinary graphics cards. There is no premine, and a full node runs on a small server.

§2

WHY NOW

The signatures that protect almost every coin today, ECDSA, Schnorr and Ed25519, rest on elliptic curves. A large enough quantum computer running Shor's algorithm

could recover a private key from its public key. Coins on a chain cannot move themselves, so the safe time to change a coin's lock is before that machine exists.

The large chains are working on it: Ethereum's 2026 roadmap targets signature agility around 2029, and Bitcoin's proposals are still under discussion. A migration on a chain that already holds billions is slow, because every holder must act. Internet Money starts on the other side of that migration: its wallets are quantum-safe from the first block.

The same reasoning applies to tokens. On most chains a token is a program someone deployed, and each program is more code to trust. Internet Money makes issuing, trading and holding tokens part of the protocol, so the rules are small, fixed and checked by every node. Proof of work still matters too: quantum computers speed up hash searching only quadratically, so mining and block hashing remain sound.

§3

QUANTUM-SAFE WALLETS

Every Internet Money wallet's main address locks coins to two keys, and a spend must carry a valid signature from each. One is Ed25519, the proven standard. The other is SQIsign at NIST level I, a post-quantum signature in NIST's standardisation programme. As far as we know, Internet Money is the first blockchain to use it.

Two locks, not one. New cryptography earns trust over years. Pairing SQIsign with Ed25519 gives quantum protection today without betting coins on a single scheme: an attacker would have to break both.

Why SQIsign. On a blockchain every node stores every signature for good, so size is the cost that matters most. SQIsign has the smallest key and signature of any post-quantum scheme.

SCHEME	PUBLIC KEY	SIGNATURE	KEY + SIGNATURE	RELATIVE SIZE
SQIsign, NIST level I (Internet Money)	83 bytes	200 bytes	283 bytes	1×
Falcon-512	897 bytes	666 bytes	1,563 bytes	5.5×
ML-DSA-44	1,312 bytes	2,420 bytes	3,732 bytes	13×

A complete quantum-safe spend, both keys and both signatures, is 379 bytes.

One recovery phrase. Both keys come from a single 32-byte seed, which the wallet derives from its 12-word recovery phrase. Restoring the phrase restores the quantum-safe address, with nothing else to back up.

Fast to check. Nodes verify a block's signatures on several cores at once and remember signatures they have already verified, so a transaction seen in the mempool costs nothing again in a block. Relay limits on quantum-safe inputs per transaction and per client keep verification cheap for every node.

Malleability handled. SQIsign signatures are not strongly unforgeable, so a transaction ID excludes signature data. A re-encoded signature can never change which transaction a payment refers to.

§4

CONSENSUS

A five-second BlockDAG

Internet Money orders its blocks with GHOSTDAG, the protocol behind Kasper. Each block names several parents, so two blocks found at the same moment both join the ledger instead of one being thrown away. GHOSTDAG then puts every block in one agreed order, and the ledger applies transactions in that order.

Five seconds, deliberately. A block arrives every 5 seconds (0.2 blocks per second). Intercontinental latency of 200 to 400 ms is under a tenth of that interval, so a cluster parameter of $k = 8$ keeps over 98% of honest blocks in the blue set. The pace keeps verification light and puts a miner on home broadband on an equal footing with one in a data centre.

Small nodes. With a 100 KB block limit, optional pruning and embedded storage, a full verifying node runs on a small VPS. A shop, wallet or exchange can check its own payments rather than trust someone else's server.

Final after 12 hours. A chain that forks off more than 8,640 blue blocks (12 hours) below the tip is never adopted, whatever its work. Rented hashpower cannot rewrite old history.

Responsive difficulty. Difficulty is recomputed for every block from the last step of the selected chain, with a 100-second half-life chosen by simulation. It catches up with a fifty-fold jump in hashrate in about two minutes and recovers from a fifty-fold

drop in about ten. A miner that switches on only while difficulty is low earns within 2% of a steady miner per hash.

§5

PROOF OF WORK

Hallmark

Hallmark is FishHash, the memory-hard algorithm designed for Iron Fish, with a seed unique to each Internet Money network. The seed is derived from the network's genesis block, so no other FishHash chain's dataset can be reused here. Internet Money's implementation is tested byte for byte against Iron Fish's.

Each hash makes 96 random reads across a 4.6 GB dataset. Graphics cards are built for exactly that kind of memory access, which keeps mining open to anyone with a gaming PC; a card with 6 GB or more is enough. No FishHash ASIC is publicly known.

Nodes do not need the dataset to verify a block. They compute the 96 items a block's hash reads from a 75 MB light cache, so verification stays cheap. The seed never changes, so there are no epochs and the dataset is built once.

Miners connect to a node directly or through the Stratum bridge used by common mining software, and a reference OpenCL GPU miner and pool are included.

§6

BUILT INTO THE COIN

Internet Money has no virtual machine and no smart contracts. Instead, a fixed set of contracts people actually use is written into the consensus rules, each as a small address type every node checks. Each is a few dozen lines of rules rather than an open-ended program, which keeps the code small enough to review and leaves no contract for an attacker to deploy.

FEATURE

WHAT IT DOES

Native tokens

Issue a token with a name, ticker and decimals; send it like IMN. Supply is conserved by consensus, a mint authority allows more to be minted, and giving it up fixes the supply for good.

FEATURE

WHAT IT DOES

Built-in market	An offer states its price in the clear. Anyone can take all or part of it in one transaction without a signature from the maker, and the maker is always paid. Nodes list open offers as an order book.
Escrow with a referee	Buyer, seller and arbiter keys, with a deadline. Each role may pay only certain parties, so escrowed coins can never go anywhere else.
Subscriptions	A merchant collects a fixed amount once per period, never more; the customer can cancel at any time.
Savings vaults	Every withdrawal waits a delay the owner chooses. During it, a backup key can pull the coins back, so a stolen everyday key cannot empty the vault.
Shared wallets	Multi-signature addresses that need m of up to 16 keys.
Swaps with other chains	Hash locks using SHA-256, which Ethereum-style chains also verify, so IMN and a token on another chain change hands both or neither. Swap offers list IMN for sale against tokens elsewhere.

Within one transaction, an output can settle only one contract, so a single payment can never satisfy two of them at once. Tokens can be held in escrow, vaults, shared wallets and hash locks, and traded on the market like IMN.

§7

PAYMENTS

A payment can name the invoice it settles. The invoice number travels in the transaction and is covered by the payer's signature, so nobody can relabel the payment and a shop knows exactly which order was paid. A payment request is a plain link: `imn:q...?amount=12.5&invoice=INV-1042`.

A node reports each invoice at three levels, and the receiver chooses which to wait for by the value at stake:

LEVEL	MEANING	TYPICAL TIME
Seen	The node has the payment	under a second
Included	Accepted into the ledger	about 5 seconds
Final	At least 60 confirmations, with no network alert	about 5 minutes

Fees are under a cent. When a wallet names the node that served a payment, half the fee goes to that node, which rewards running one. A JavaScript developer kit, a checkout window with locally drawn QR codes, and a WooCommerce plugin come ready to use.

§8

ECONOMICS

Every coin is mined. Genesis creates nothing, there is no premine and no sale, and the schedule is fixed in the consensus rules. The block reward starts at 5 IMN, halves every four years four times, then stays at 0.3125 IMN per block for good, so miners are always paid to secure the network.

YEARS	REWARD PER BLOCK	MINED IN PERIOD	SUPPLY AT END	INFLATION AT START
0–4	5 IMN	126,144,000	126,144,000	—
4–8	2.5 IMN	63,072,000	189,216,000	12.5%
8–12	1.25 IMN	31,536,000	220,752,000	4.2%
12–16	0.625 IMN	15,768,000	236,520,000	1.8%
16 onward	0.3125 IMN	1,971,000 a year	no cap	0.83%, falling

Maintenance fund. For the first three years (18,921,600 blocks), 5% of each block's reward is paid by the ledger itself to one maintenance address fixed in the rules. It funds servers, development, security work and an independent audit. After three

years it stops by itself and miners receive the whole reward. The fund comes out of the reward, so total supply is unchanged; it comes to about 4.73 million IMN, 2% of the supply at year 16. Transaction fees always go in full to miners and serving nodes.

Fees reward nodes. When a wallet names the node that served a payment, half the fee goes to that node and half to the miner. A wallet or shop that runs its own node keeps half of every fee it pays, which rewards running nodes and keeps payments verified close to where they happen.

Internet Money's security starts with its design: fewer moving parts, each one checked by every node.

-
- **No virtual machine.** Every feature is a fixed rule of a few dozen lines, so there is no contract code to exploit and no re-entrancy, gas or upgrade-proxy class of bug.
-
- **Two signature schemes.** Coins on quantum-safe addresses stay safe as long as either Ed25519 or SQIsign holds.
-
- **Fixed consensus code.** The signature libraries are pinned to exact versions. Any change to consensus code arrives as a planned, announced release, never as an automatic update, so every node keeps agreeing on what is valid.
-
- **Defences on every input.** Blocks, transactions and peer messages are size-limited and decoded strictly. The mempool checks for room before verifying signatures, quantum-safe verification is rate-limited per client, and misbehaving peers are scored and banned.
-
- **Finality.** History older than 12 hours can never be rewritten, and a node raises an alert after any deep reorganisation so services can pause.

Tested in the open. Every feature has been through four rounds of penetration testing and reviews by three AI models (MiniMax, GLM and DeepSeek), and every finding was fixed and covered by a test. Fuzzing targets for the decoders, signature checks and peer protocol run on every change, alongside GitHub's CodeQL scanning, dependency audits and over 200 tests. A full independent audit by a security firm is planned and is one of the first uses of the maintenance fund.

Internet Money is the only one of these whose wallets are quantum-safe by default, and it pairs that with native tokens and a market on a fast, GPU-mined BlockDAG.

	INTERNET MONEY	BITCOIN	ETHEREUM	KASPA
Quantum-safe wallets	By default (Ed25519 + SQUsign)	Proposals under discussion	Planned, around 2029	Opt-in vault scripts in development
Block interval	5 seconds	10 minutes	12 seconds	0.1 seconds
Consensus	Proof of work, GHOSTDAG	Proof of work, longest chain	Proof of stake	Proof of work, GHOSTDAG
Mining hardware	Graphics cards	ASICs	None (staked)	Mostly ASICs
Coins made before launch	None	None	Yes (2014 sale)	None
Native tokens	Built in	Add-on protocols	Smart contracts	Built in since June 2026
Market, escrow, vaults	Built in, no contracts	No	Smart contracts	Through covenant scripts
Fee share for serving nodes	Half the fee	No	No	No

Summary of each network's base layer as of October 2026.

§11

ROADMAP

The protocol is feature-complete: everything in this paper is implemented in the reference node, wallet and desktop app. What comes next widens access to it.

READY TODAY

- Reference node, CPU and OpenCL GPU miners, Stratum bridge and mining pool
- Browser wallet and desktop app for Windows, Mac and Linux, quantum-safe by default
- Block explorer, JavaScript developer kit, checkout window and WooCommerce plugin
- Seed nodes on three continents, with release builds and a published node image

NEXT

1. A fair, announced main-network launch, with a genesis difficulty set for real hashrate.
2. Swaps with Ethereum from inside the wallet, and encrypted connections for miners.
3. Multi-signature shared wallets in the browser wallet and desktop app.
4. A full independent security audit, funded by the maintenance fund.
5. Hardware-wallet support and swaps with Bitcoin.
6. A bridge to Base, so IMN can trade on existing exchanges there.

§12

REFERENCES

- Internet Money protocol specification
- Internet Money source code and website
- SQIsign: algorithm specifications, version 2.0
- SQIsign project site
- sqisign-rs, the Rust implementation used by Internet Money
- PHANTOM GHOSTDAG: a scalable generalization of Nakamoto consensus

■ Are emerging post-quantum signature schemes better for blockchains? (Project Eleven)

■ Ethereum Foundation to implement quantum security by 2029 (ForkLog)

■ Kaspia Toccata activation record

■ Post-quantum vault spends on Kaspia testnet

Internet Money is open-source software under the MIT or Apache-2.0 licence.

Nothing in this paper is financial advice.

Internet Money (IMN) is open-source software under the MIT or Apache-2.0 license, provided without warranty. Nothing on this page is financial advice.

github.com/Internet-Money-Network