

Rand Protocol

Private computation, hash-based proofs

Programmable and private: a layer-1 chain with a shielded note pool and a RISC-V zkVM, proved by a hash-based STARK with no trusted setup. For venture and strategic investors.

Investor overview · Version 6 · October 2026

Records of 2 October 2026: a live public test network (chain 20, cut on v0.6.8 on 1 October), not a main network. Draft for counsel's review before distribution; not an offer or solicitation of any security, token or financial product. Test-network RAND has no monetary value.

A public ledger taxes everyone with something to protect, and the largest pools of capital decline to pay it

Value lost on transparent ledgers, and the buyers it keeps away. Figures are third-party, each with its publisher and date.

WHAT A PUBLIC CHAIN PUBLISHES

- Orders, before they fill**
every swap readable in the mempool
- Positions and their triggers**
every loan down to its liquidation price
- Payroll and supplier terms**
every salary, every vendor's price
- Bids, quotes and votes**
every auction bid and every ballot

WHO READS IT

- Sandwich and MEV bots**
trade ahead of the order, then behind it
- Liquidation hunters**
push the price to where the line is
- Competitors, counterparties**
read margins, runway and terms
- Last bidders, vote buyers**
win on latency; pay against a ballot

WHO STAYS AWAY: THE VETO

- Funds and market makers**
will not trade a strategy in public
- Large borrowers**
stay off-chain or under-borrow
- Corporate treasurers**
settle on bank rails instead
- Issuers, dealers, DAOs**
accept worse prices and bought votes

\$60M

LOST TO SANDWICH ATTACKS
by Ethereum traders, 12 months to
Oct 2025 (EigenPhi via Cointelegraph,
Dec 2025)

\$226B

STABLECOIN SUPPLIER PAYMENTS
by businesses in 2025, every one
public (McKinsey, Artemis, Feb 2026)

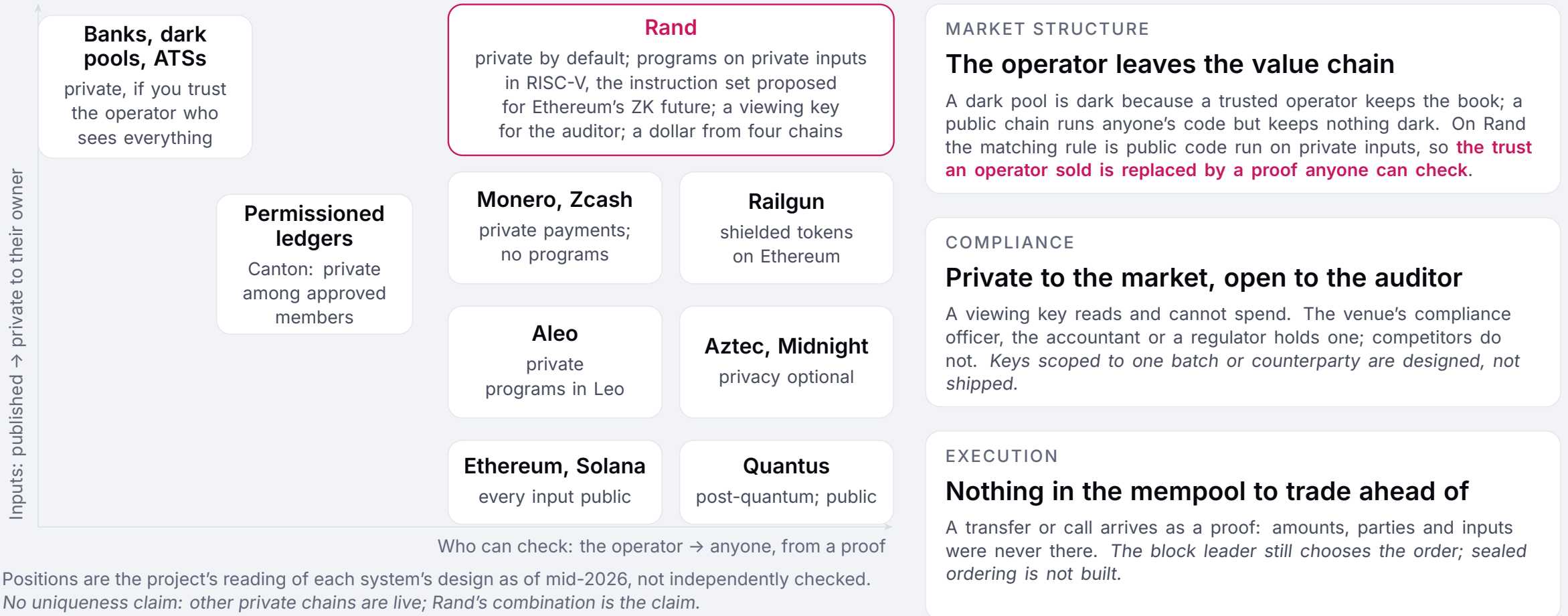
\$3.2B

OF LISTED EQUITIES ON CHAIN
of \$152 trillion listed worldwide
(rwa.xyz, 2 Oct 2026; WFE,
end-2025)

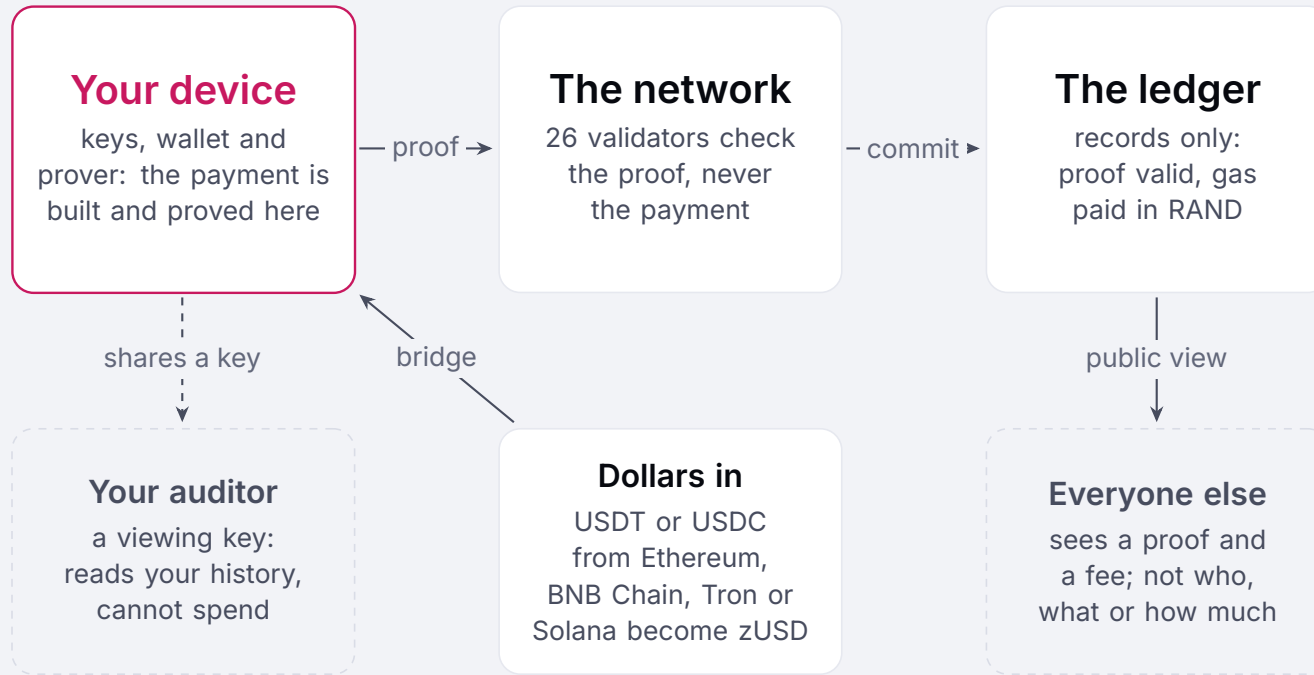
\$5.6T

HEDGE-FUND CAPITAL
the buyers of a dark pool, absent from
public chains (HFR, Q2 2026)

Until now a market could be verifiable or confidential, not both: Rand proves the rule ran without publishing the inputs



Keys and proofs stay on the user's device; the network checks a proof and never sees the payment



ON CHAIN 20 TODAY, 2 OCTOBER 2026

- **Private by default.** Value is held only as shielded notes: no accounts, balances or transparent mode. Fees, timing and bridge amounts stay public.
- **Programs in Rust or C** run in a RISC-V zkVM; the chain stores a proof and output words, not the inputs.
- **A dollar from four chains.** USDT or USDC locked on Ethereum, BNB Chain, Tron or Solana becomes one shielded dollar, zUSD. Core-team guardians attest (6 of 8); caps are small.
- **Wallets for six platforms,** an explorer and a public RPC. A viewing key reads and cannot spend. All 26 validators are run by the core team.

2.9 MB

PROOF PER TRANSFER

hash-based STARK, no trusted setup

15 s

TO PROVE A TRANSFER

16 cores of one laptop; earlier build

32 ms

TO VERIFY A PROOF

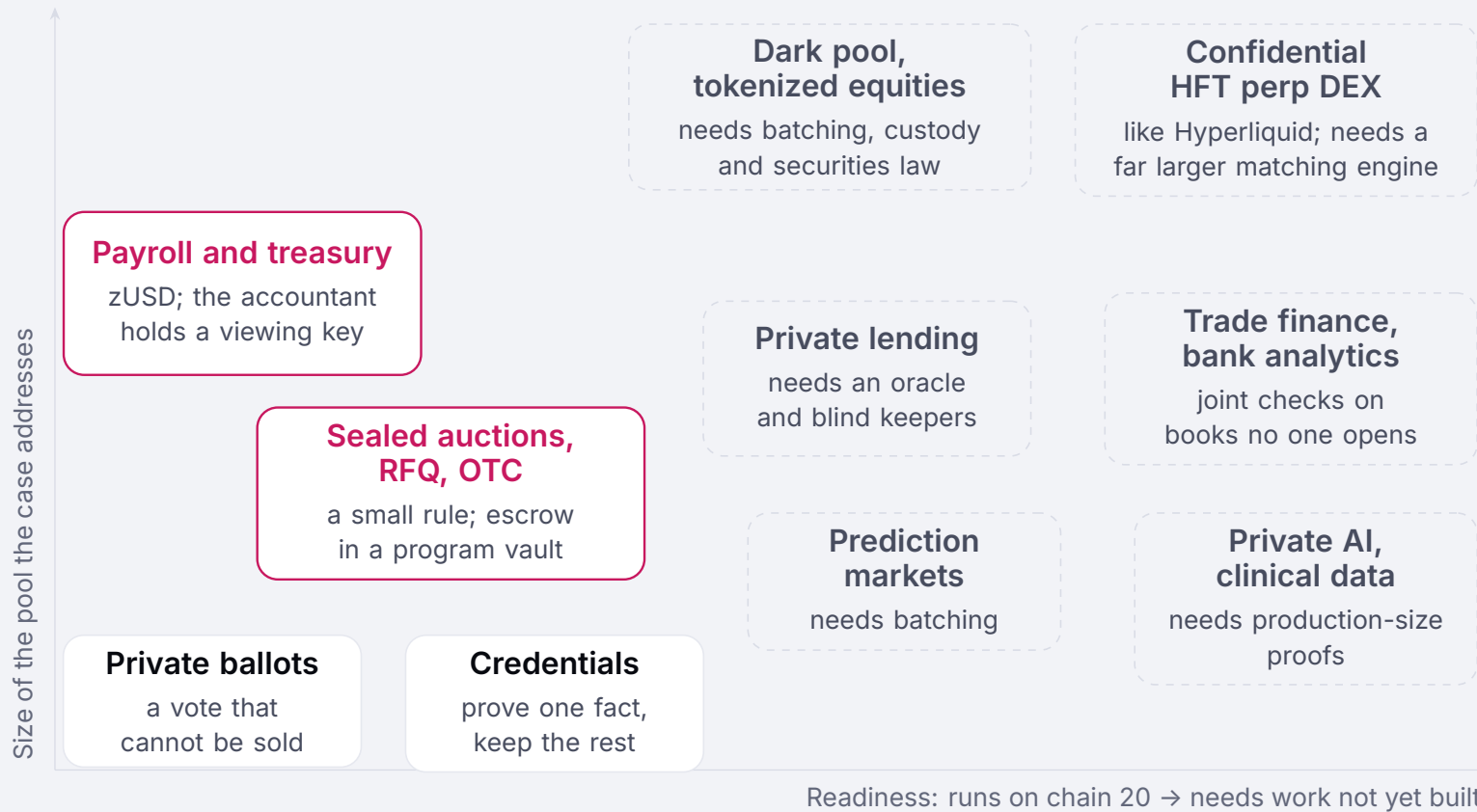
warm key, one laptop core

~7

TRANSFERS PER BLOCK

bounded by proof bytes, not compute

Twenty industries, one property: the first to ship are few, valuable transfers that today's chain already carries



WHY THIS ORDER

- Today's chain suits few, valuable transfers. About seven fit a block and a proof takes about 15 s: **negligible on a payroll run or an OTC settlement, too slow for a retail swap.**
- Calls are capped at 16,383 cycles. A payroll split or a sealed-bid rule fits.
- Program vaults (v0.6.8) let a program hold and pay out value, which escrow needs; it is the newest part, with the least run time.
- The largest pools come last. Equities and lending need an oracle the program can read, batching rules and a custodian; a confidential perp DEX in the style of Hyperliquid needs a matching engine beyond the cycle cap and throughput far above seven transfers a block; AI needs proofs at production scale.

Cases from randprotocol.org/usecases; placement is the founders' judgement from the chain 20 maturity table. Pink: buildable today. Dashed: blocked on work not yet built.

WHY NOW

Why now: the dollars are on chain, and regulators now ask how privacy fits

SUPPLY (LEFT) AND TRANSACTIONS A YEAR (RIGHT), \$ TRILLIONS



Pink: supply (DefiLlama); dashed, Standard Chartered (\$2T by end-2028) and Citi (\$1.9T base, \$4T bull by 2030). Grey: transactions, Visa Onchain Analytics adjusted (raw about \$33T in 2025); dashed, Citi's ~\$100T a year by 2030 at fiat-like velocity, a scenario. Estimates drawn straight from today. Pools behind the use cases: cross-border B2B \$31.6T a year (FXC, 2024); hedge funds \$5.6T (HFR, Q2 2026).

Aug 2024	■ NIST	NIST post-quantum standards FIPS 203–205; Rand uses ML-KEM-768 and Dilithium2 (pre-standard ML-DSA).
Dec 2024	■ EU	MiCA fully applies Licensed stablecoins and service providers across the EU.
Mar 2025	■ OFAC	Tornado Cash delisted Sanctions on the privacy software lifted.
Jul 2025	■ US law	GENIUS Act A federal regime for payment stablecoins.
Dec 2025	■ SEC	Privacy on the agenda Roundtable on financial surveillance and privacy, 15 Dec.
Dec 2025	■ DTC	Tokenized securities No-action relief for DTC to tokenize custodied assets; rollout from H2 2026.
Sep 2026	■ Senate	CLARITY Act stalls Cloture failed 15 Sep: market-structure law still open.
Jul 2027	■ AMLR	Anonymity-enhancing coins barred At service providers; disclosure by design is the test.
2030–35	■ NIST	RSA and ECC retired Deprecated after 2030, disallowed after 2035 (IR 8547, draft).

WHY US

Why us: private by default, programs in Rust, post-quantum and no trusted setup; Aleo, Railgun and Quantus each lack at least two

	STATUS	PRIVATE BY DEFAULT	PROGRAMS, AND HOW YOU WRITE THEM	PROOFS AND SETUP	POST-QUANTUM
Rand	Test network (chain 20)	Yes, always	Rust or C on RISC-V; EVM and Solana bytecode translators (partial)	Hash-based STARK, no setup; MB proofs	Notes, signatures, proofs
Aleo	Mainnet 2024	Records private; much state public	Leo, its own language, or Aleo instructions	Pairing-based SNARK; universal setup	No
Railgun	Live on Ethereum, Arbitrum, Polygon and BSC	Opt-in, per token	No private programs; calls public DeFi	Groth16 SNARKs; trusted setup	No
Quantus	Mainnet Sep 2026	Optional privacy layer	None	Not a programmable chain	Yes, ML-DSA signatures
Aztec, Midnight	L2; mainnet Mar 2026	Optional, per function	Noir and Compact, their own languages	SNARKs with a universal setup	No
Zcash, Monero	Mainnets since 2016, 2014	Zcash opt-in; Monero yes	None	Halo 2; Bulletproofs	No

WHY DEVELOPERS CHOOSE RAND

No new language, and the ZK industry’s instruction set

Write Rust or C, build with the standard compiler, deploy the binary; the chain proves it ran. **RISC-V is what the leading zkVMs prove** (RISC Zero, SP1) and what Vitalik Buterin proposed for Ethereum’s execution layer in April 2025, so tools and talent carry over. Aleo, Aztec and Midnight need their own languages. Cost: megabyte proofs.

WHERE OTHERS ARE AHEAD

Users, liquidity and smaller proofs

Aleo, Zcash and Monero are mainnets with users; Railgun sits where Ethereum’s liquidity already is; their proofs are kilobytes where Rand’s are megabytes. Rand’s claim is the combination. *Others’ positions: our reading of their public documents, mid-2026, not independently checked.*

A year of research, then a live network in three weeks; the seed buys the steps to a main network

4

RESEARCH PAPERS

21 December 2025, then revised in git

28

NODE RELEASES

v0.1 (16 Sep) to v0.7.1 (2 Oct 2026)

7

TEST CHAINS

chains 14 to 20, 20 Sep to 1 Oct

2,172

COMMITTS

233k lines of Rust, 2 Oct 2026

RESEARCH, DEC 2025 TO SEP 2026			SHIPPED, SEP TO OCT 2026			NEXT, MONTHS FROM THE SEED CLOSE		
Dec 2025	Papers	Four papers Protocol, post-quantum security, stablecoin design, investor summary.	16 Sep	v0.1	First release A week after the first commit.	0-3	Operate	Keys leave the team Three operators by 1 Nov (target).
Jan 2026	Proto	First prototype An SVM node with confidential tokens; the RandScan explorer.	20 Sep	chain 14	Test network First public test chain.	3-6	Scale	Founding round Gated on the test-profile exit.
Jun 2026	Design	EVM execution Execution moved from SVM to EVM; private gas settlement.	28 Sep	v0.6	Delegated proving A prover that can read, never spend.	6-9	Secure	Independent audit Slashing on; scoped viewing keys; a custodian.
Aug 2026	Design	Private computation Confidential programs; shielded bridged dollars.	29 Sep	chain 17	Split authorisation The spend key's proof stays on the device.	9-12	Open	Outside validators An open validator programme; larger programs.
Sep 2026	Rebuild	RISC-V zkVM A hash-based STARK, no trusted setup; the node from 9 Sep.	1 Oct	chain 20	Programs with state Program vaults, a consensus fix, a bridge round trip.	12-16	Sell	Validator sale To operators who ran a stage.
			2 Oct	v0.7.1	Signed releases Built by CI, attested and signed.	16-18	Launch	Main network Genesis frozen; no calendar date published.

VALUATION

The seed is \$0.03 a token, \$30 million on RAND’s 1 billion maximum supply: a third of the next round’s price

Round prices from the seed materials of 29 September 2026 (tokenomics Draft 2). Proposed, not set in code: test-network RAND has no monetary value.

\$30M

SEED VALUATION
\$0.030 a token, open now

\$100M

FOUNDING ROUND
\$0.100; gated on a measurement

\$150M

PUBLIC AUCTION
\$0.150, a week after genesis

16-18

MONTHS TO GENESIS
lock-ups count from genesis

ROUND	PRICE	VALUATION	SUPPLY
Seed, open now	\$0.030	\$30M	11%
Founding	\$0.100	\$100M	9%
Validator and prover	\$0.120	\$120M	4%
Strategic	\$0.150	\$150M	2%
Public auction	\$0.150	\$150M	4%

Why \$30 million

Our own number for a two-founder, pre-revenue, pre-mainnet project: 1.5× Solana’s \$20M seed, and a fraction of what privacy projects raised at in 2025–26: Zama \$550M, Aztec about \$557M, Octra and Arcium \$200M.

WHERE VALUE ACCRUES TO RAND

- Every fee is paid in RAND, whatever asset moves; validators stake at least 1,000 RAND each.
- The bridge earns 10 bps of zUSD in and out: at 1% of 2025’s \$226B in B2B stablecoin payments, about \$2.3M a year.

No return is implied or assured, and a token price can fall to zero. The company has no revenue today. Valuations are on the 1 billion maximum supply; the comparables in full and downside scenarios are for counsel’s review.

THE ROUND

The round: \$3.3 million for 11% of RAND's 1 billion maximum supply, sold as SAFTs; about 18 months of runway

Seed terms as set out on 29 September 2026; counsel is to review them before this deck is distributed. Nothing here is an offer.

USE OF FUNDS	SHARE	WHAT IT PAYS FOR
Engineering	45%	Four hires: node and standing review, bridge and infrastructure, wallet and product, proof systems
Independent audit	15%	\$350–750K programme: circuits, recursion VM, bridge, consensus, wallets
Custody decentralisation	12%	Independent guardian and validator operators, RPC diversity, timelocked multisigs
Legal and compliance	10%	Counsel's opinions per role, the sale structure, custodian onboarding
Test network and go-to-market	10%	Operator rewards, design partners, viewing-key tooling
Reserve	8%	Contingency

Burn about **\$190K a month** on the base plan: the seed alone covers about 18 months.

- **Milestones before the founding round:** the first independent audit under way; guardians and validators at operators other than the core team (three by 1 November 2026, a target); design partners signed. *Already done: the CON-4 consensus fix, live on chain 20 in v0.6.8.*
- **Main network:** genesis 16–18 months after the seed closes, gated on measurements rather than dates; no calendar date is published.

The ask

\$3.3M across at least four investors (maximum ticket \$0.9M under the 3% cap). **Instrument:** a **SAFT (simple agreement for future tokens) for 110M RAND**, 11% of a **maximum supply of 1 billion RAND**, at \$0.03 a token (\$30M fully diluted), issued by Randprotocol Development LLC (Wyoming) and delivered at genesis. **Lock-up:** 12-month cliff after genesis, then 24 months linear. **Rights:** pro rata in the founding round, information rights, an observer.

- **What the SAFT buys:** the right to 110M RAND at genesis, not equity in the LLC; supply is capped at 1 billion. *The company has no revenue today.*
- **Diligence:** the papers, the live test network, the measured figures with their sources, the internal review reports, the tokenomics model; a term sheet within four weeks of a first meeting.

TEAM

The team: two founders who designed the protocol and are building it themselves, from the papers to the wallets

Biographies as on randprotocol.org/team, 6 October 2026, from the founders' LinkedIn profiles and Google Scholar.

FOUNDER · PROTOCOL AND CODE

Dendi Suhubdy

Machine-learning research at Mila, Université de Montréal, with Yoshua Bengio: the MILABot chatbot, ChatPainter and Fraternal Dropout, and a contributor to Theano (671 citations). Brings market experience as **co-founder of Bitwyre**, a crypto spot and derivatives exchange whose trading engine and architecture he built (since 2019), and **of Systematic Trading Group**, a proprietary trading firm (2025). Co-founded Grokvideo, a text-to-video search engine in Montreal (2018–22, since acquired), sold two further companies in 2025, and has invested in KAST and Parts Order. At Rand he writes the code, every commit to date.

[LinkedIn](#) · [Google Scholar](#)

FOUNDER · SECURITY AND DESIGN

Anish Mohammed

Cryptographer and security researcher with 20+ years of experience in cryptography, distributed systems and blockchain. An early member of the Ethereum Swarm team and reviewer of the Swarm Orange Paper, he later **co-founded Panther Protocol, serving as CTO and Chief Scientist**, and was **principal architect at Boson Protocol**. Anish has advised Ripple and Ocean Protocol and has published and lectured extensively on zero-knowledge proofs, privacy, blockchain security and cryptographic protocols, including research in the IACR Cryptology ePrint Archive and academic work on privacy and security.

[LinkedIn](#)

HIRING WITH THE SEED

Four roles

A senior node engineer and standing reviewer; bridge and infrastructure; wallet and product; proof systems. **Key-person risk is one engineer today.** The first independent audit is a condition of the founding round.

ENTITY

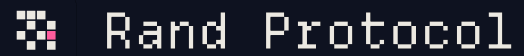
Randprotocol Development LLC

Wyoming; the seed's issuer. No foundation is formed yet, so the LLC holds every foundation role. Cap table: founders 60:40; no other SAFTs, grants or options. *Rand's IP to be assigned to it before close.*

IN PRINT, OPEN SOURCE

Five papers; GPL-3.0-only

randprotocol.org/papers. The full node (zkVM and recursion VM), the wallets, the bridge and the circuits are on github.com/randprotocol; the wallet core is WebAssembly built from the open-source clients.



Thank you.

randprotocol.org

github.com/randprotocol

Dendi Suhubdy · Anish Mohammed

Randprotocol Development LLC, Wyoming

Not an offer or solicitation of any security, token or financial product.
Test-network RAND has no monetary value. Draft for counsel's review
before distribution.