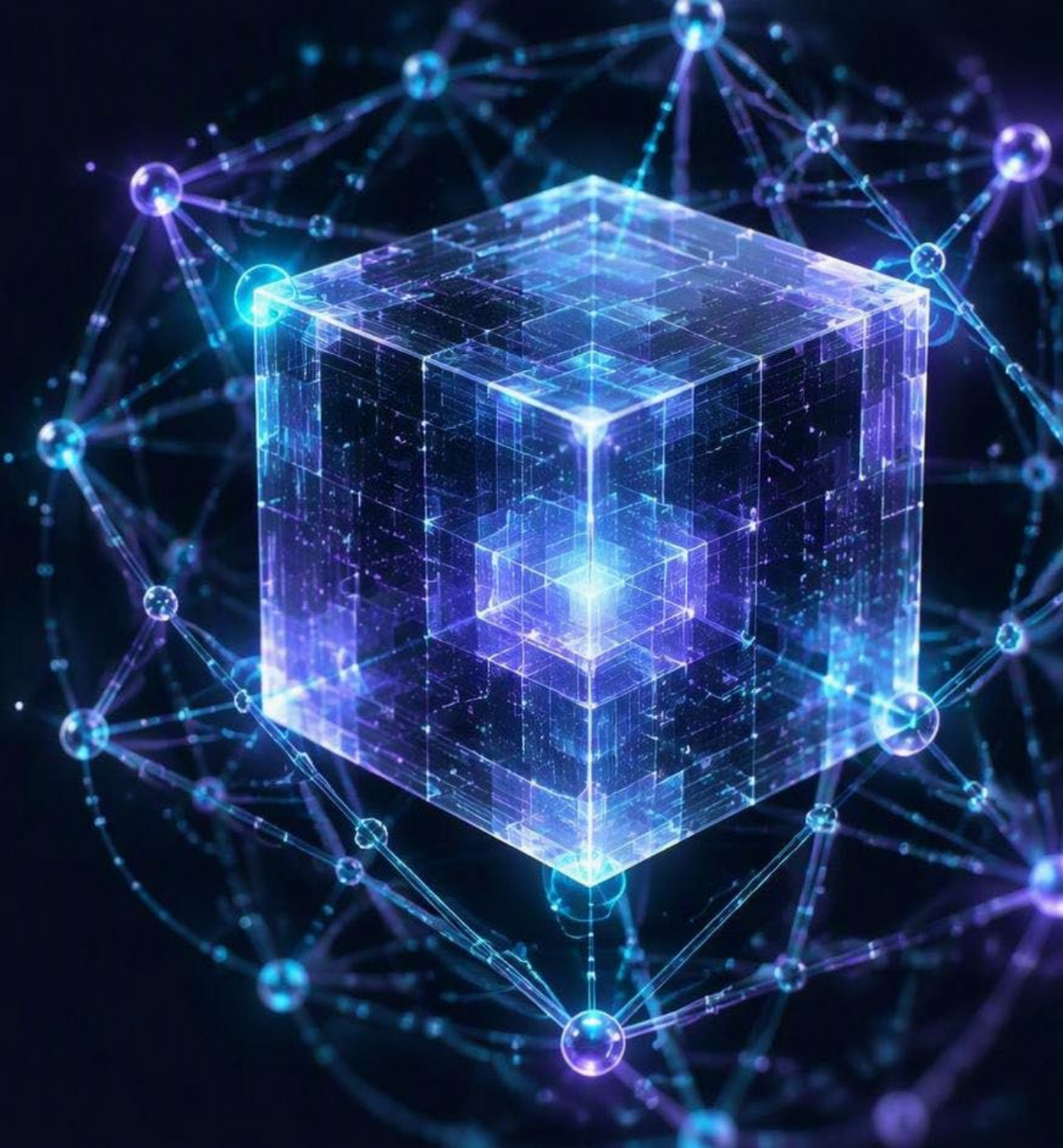
THE PRIVACY PARADOX

Can Blockchain Keep a Secret?

Privacy by Design for distributed ledgers

Sheree Ip | Curtin University

ISACA | Data protection • Confidentiality • Governance



Privacy by Design

Trust without unlimited visibility

The paradox in one picture

DESIGN GOAL

What blockchain promises

Shared truth • Tamper evidence • Independent verification • Resilience

DESIGN CONSTRAINT

What privacy requires

Purpose limitation • Data minimisation • Retention limits • Individual rights

Trust without unlimited visibility

What is actually visible on a ledger?

PAYLOAD

Messages, document contents, transaction details

METADATA

Amounts, timestamps, relationships, smart-contract calls

IDENTIFIERS

Wallet addresses, public keys, persistent pseudonyms

REPLICATION

Many nodes may retain copies for a long time



Pseudonymous ≠ anonymous.
A hash ≠ automatic anonymisation.

Where privacy principles collide

Minimisation

Do we need to publish this data at all?

Erasure / rectification

Can data be deleted, corrected, or made non-identifiable?

Storage limitation

What happens when the ledger outlives the purpose?

Transparency / accountability

Who determines purposes and answers rights requests?

Start with Privacy by Design — not a patch

1 Question the need → 2 Map the data → 3 Limit exposure → 4 Plan deletion → 5 Test and govern

Privacy architecture is an early design decision not a compliance checklist at launch.

Pattern 1 | Keep personal data off-chain

OFF-CHAIN

Encrypted records
Access controls
Retention + deletion

Verify integrity →

ON-CHAIN

Minimal commitment
Reference or proof
No raw personal data

Caution: hashes, pointers, and metadata may still identify people.

Pattern 2 | Prove without revealing

PRIVATE INPUT

Identity, age, account balance, or another sensitive fact

ZK PROOF

PUBLIC VERIFICATION

“The required condition is true”

Zero-knowledge proofs reduce disclosure;
they do not automatically hide transaction metadata or endpoint activity.

Pattern 2 | Prove without revealing

ZERO-KNOWLEDGE PROOFS

A zero-knowledge proof lets a prover convince a verifier that a statement is true, without revealing the secret information that makes it true.

Completeness
an honest prover with a valid claim can convince the verifier.

Soundness
a false claim should not convince the verifier.

Zero-knowledge
the verifier learns nothing beyond whether the claim is valid.

Pattern 3 | Control who sees what

PUBLIC

Anyone can inspect the ledger

Broad verification; highest exposure

PERMISSIONED

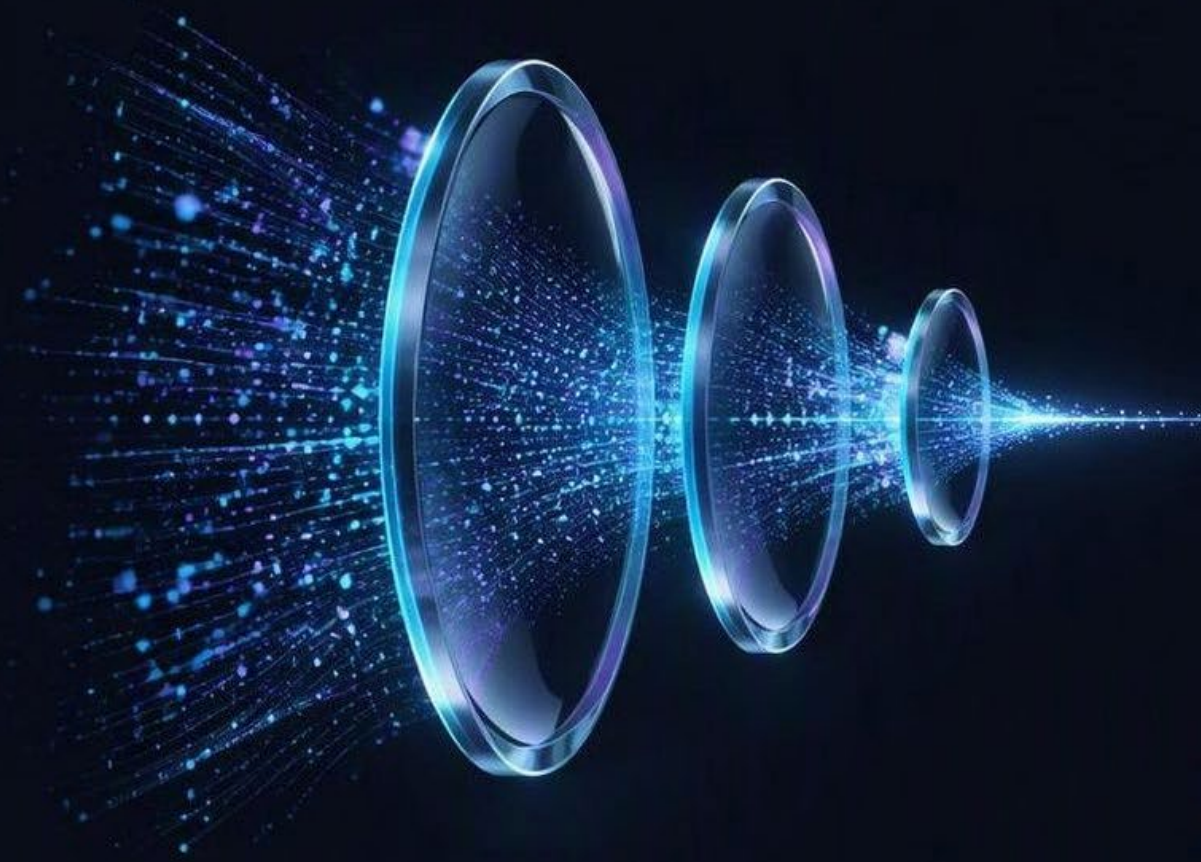
Membership and node access restricted

Governance matters; participants still see data

SELECTIVE DISCLOSURE

Release only required attributes or proofs

Smaller disclosure surface; verify linkability



A practical architecture: credentials without exposure

ISSUER

Verifies an attribute and signs a credential

→

USER

Holds credential; controls presentation

→

VERIFIER

Requests proof of a specific claim

Ledger role: **publish minimal trust or revocation of information, where justified.**

Real-world design pattern

Privacy in practice with 3NWeb and PrivacySafe

REAL-WORLD DESIGN PATTERN

3NWeb: Principle of Least Authority

Client-server architecture with less authority and less exposed data

01 No plain-text content

sent to servers

02 No unnecessary metadata

in client-server exchanges

03 Nothing exploitable on servers

when the first two rules hold

3NWeb: Pragmatic Design Goals

Private by design

Encrypt data before transit. Minimise metadata at every layer.

Long-term resilience

Stable, portable formats preserve access beyond developers and services.

Permissionless innovation

Anyone can build apps without central approval.

Vendor choice

Users choose their own devices and infrastructure.

Multi-device support

Apps and data move seamlessly across users' devices.

App-site separation

Users own and control their apps. Shared sites extend them without creating central dependencies.

3NWeb: Principle of Least Authority

Reference implementation

PrivacySafe

a powerful suite of secure, end-user apps built using these protocols,
and actively developed at github.com/PrivacySafe

3NWeb (IEEE SA Open) ↗

privacysafe.app ↗

github.com/PrivacySafe ↗

payments.privacysafe.app ↗

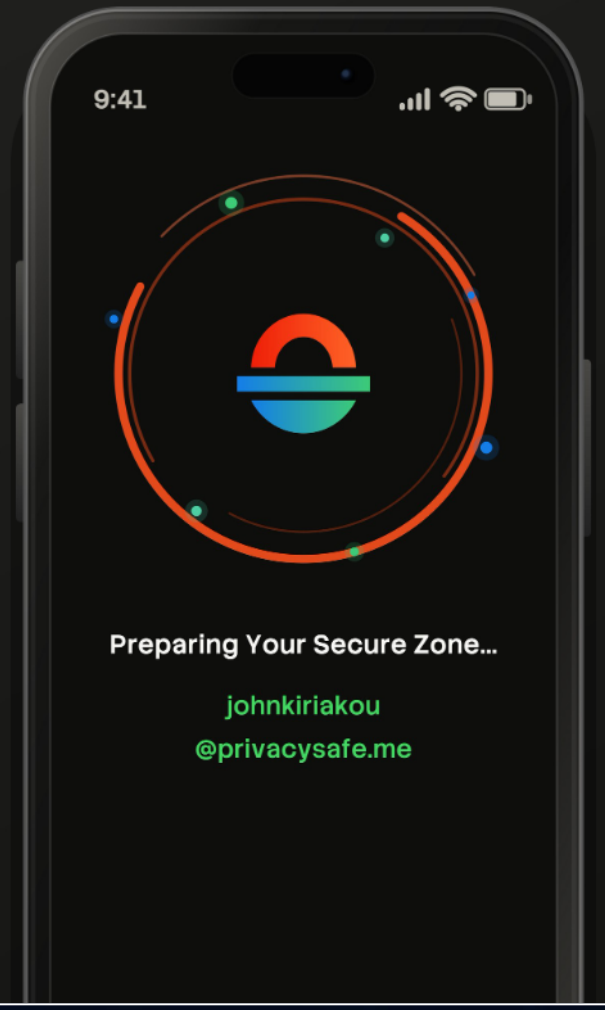
PRIVACYSAFE®

SECURE_ZONE_

Private by default. Public by choice.

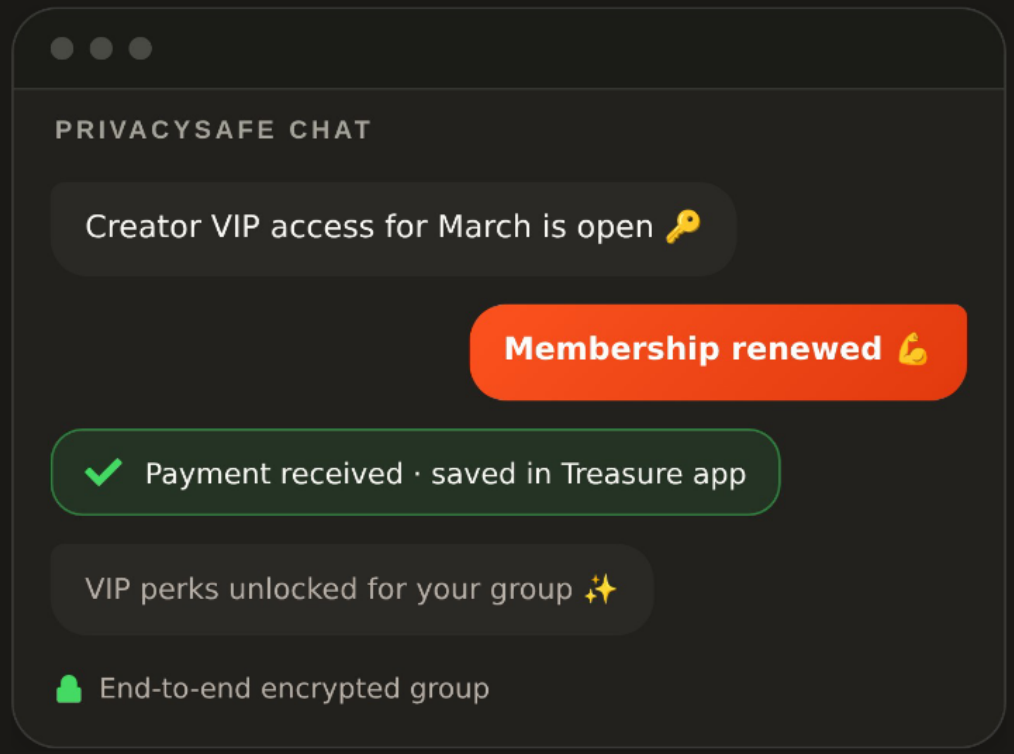
Your secure zone for private groups: sovereign identity, encrypted chat, shared files, and storage for crypto credentials and your treasure.
You hold the keys, join exclusive communities, and publish what you want when you want. Sync your data and wipe your device without worry.

No phone number required. Free/Libre and Open Source Software. Self-hostable. Shipping on Android / Google Play, Mac OS, Windows, GNU/Linux, and soon iOS.



MARKET_SIZE_

Markets are moving into private groups.



Billions of people have moved their most important communication to private groups

3B	1B	200M	80M	70M
WhatsApp	Telegram	Discord	Slack	Signal

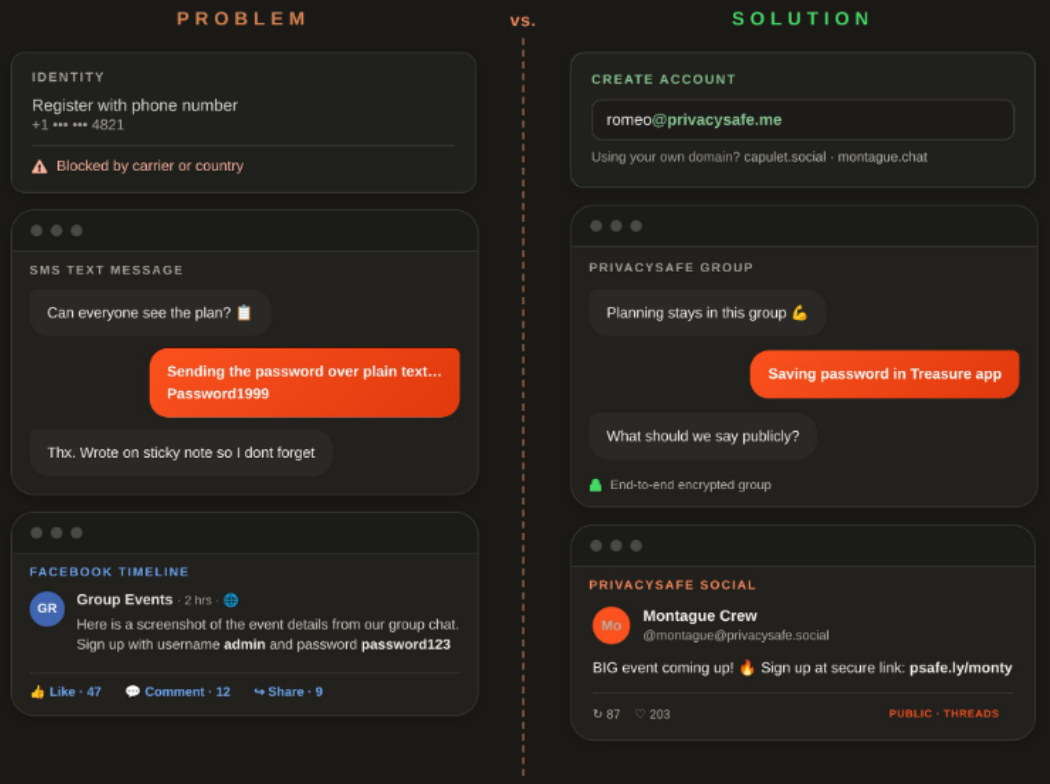
A FRACTION OF THE MARKET = MILLIONS OF USERS

4.35B combined monthly active users (MAUs). After applying a conservative 50% overlap adjustment for users who are not unique, the addressable base is roughly **2.2B users**. Capturing just **0.1% = 2.2M users**, **0.5% = 11M**, and **1% = 22M**.

Illustrative sensitivity analysis based upon publicly available information.

SOCIAL_SHIFT_

Old-fashioned group chats are a mess.



Phone numbers expose people

Phone numbers tie identity to a person, carrier, and country. They can be blocked, reassigned, or taken over, while also making it easier to correlate activity across accounts.

Sensitive data should not be scattered.

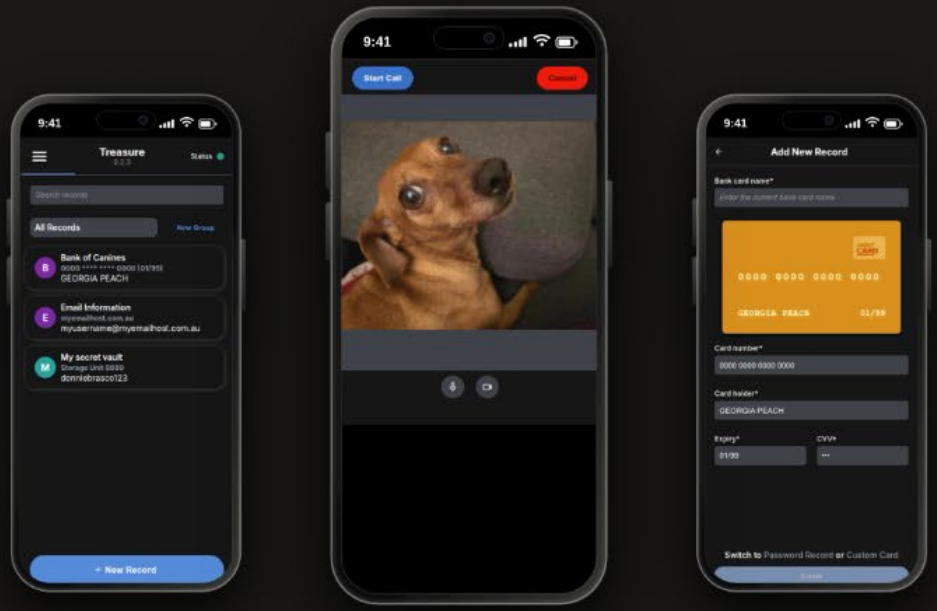
Spreading sensitive data across apps and services the user can't control encourages weak security practices, accidental disclosure, and unwanted copying.

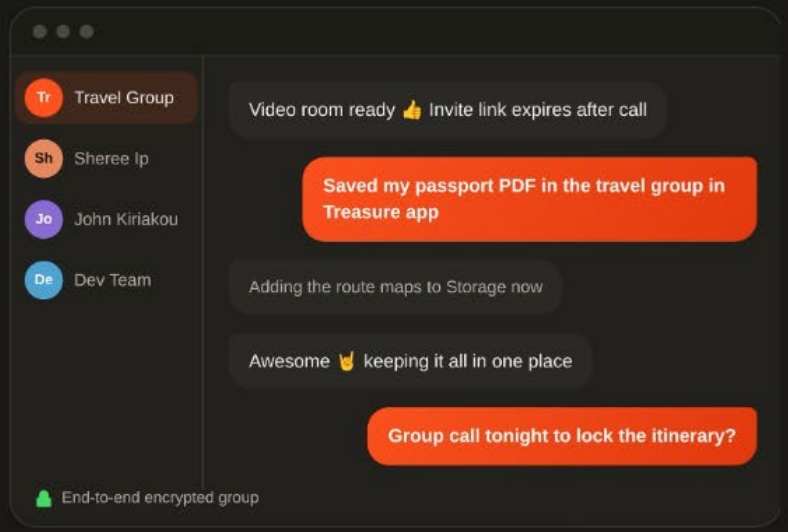
Private groups still need a public voice.

Groups should be able to choose what stays private and intentionally publish only what belongs in public.

OUR_SOLUTION_

Discord falsely promised a “server.” PrivacySafe gives groups a secure zone.

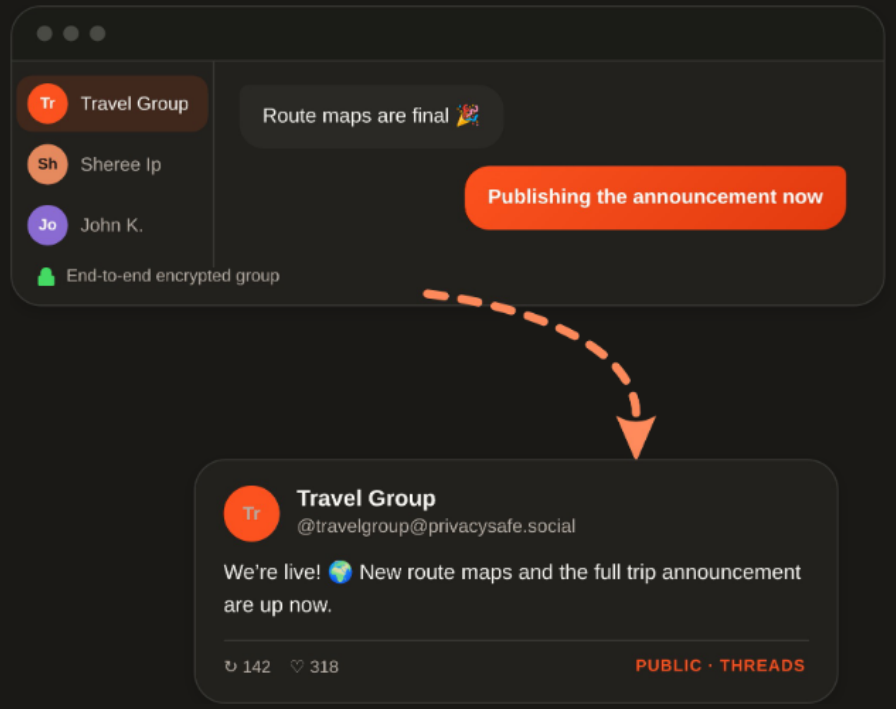




Our secure zone is like a personal “cloud” but much safer. The users control the keys, control access to their chats, and control the domains that their identities are tied to. B2C consumers can become B2B enterprise with our software on their domains and their hardware.

PUBLIC_BRIDGE_

Your private data stays protected. Share publicly, on your own terms.



PrivacySafe grows through communities who already know and trust each other. Groups stay private by default and, when a group has something to say, it publishes to the public social web on its own terms.

We launched **PrivacySafe.Social** for this purpose and people can connect with thousands of other decentralized servers and millions of users.

One group decision can bring dozens, hundreds, or thousands of members into the network together.

PrivacySafe Community Payments: Public settlement, private access

01 / PRIVATE IDENTITY

Sign in with a PrivacySafe address; your membership and content stay in the private app.

→

02 / PUBLIC PAYMENT

Pay the creator directly in AUDD or USDC on Solana, using Solana Pay or x402.

→

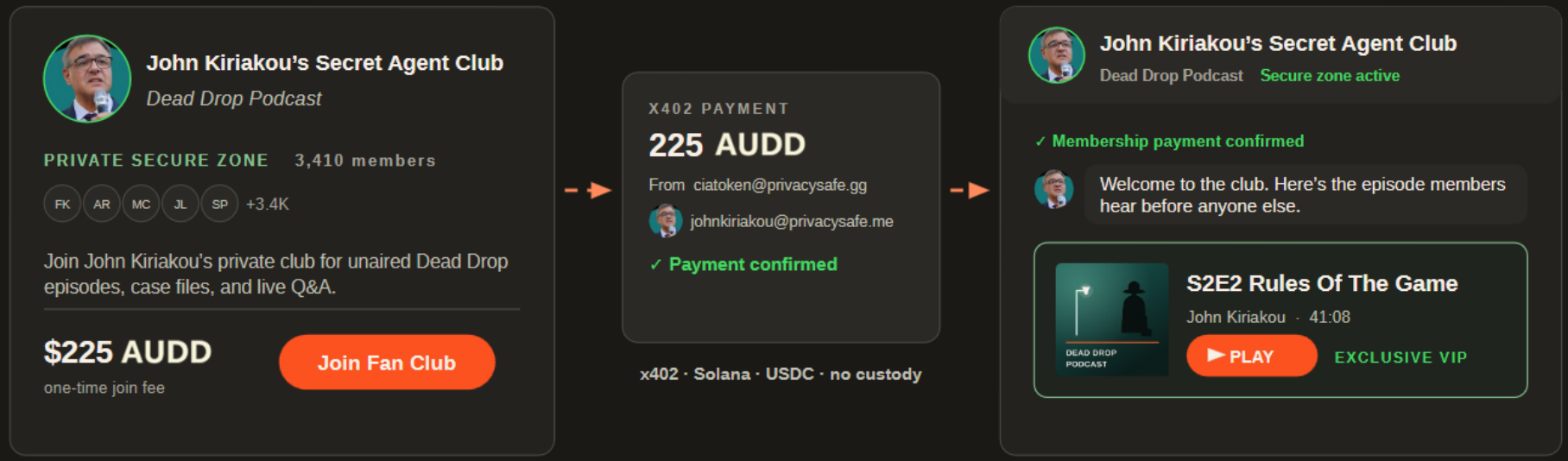
03 / VERIFIED ACCESS

Verify finality on Solana, then unlock an end-to-end encrypted community.

Public: payment and settlement metadata | **Private:** chats, stored content, membership experience

PAYMENTS_SYSTEM_

PrivacySafe helps people to monetize their communities.



Just one example. x402 payments built for AI agentic workflows.

Artists + Musicians · Consultants · Lawyers · Health Professionals · Public Figures

Privacy governance

Accountability and audit across the data lifecycle

GDPR and governance: who is accountable?

01 CONTROLLER / PROCESSOR

Identify roles and responsibilities across nodes, developers and operators.

02 RIGHTS + RETENTION

Document lawful basis, correction / erasure pathway, and retention periods.

03 RISK + TRANSFERS

Assess cross-border replication, linkability and security risks; conduct a DPIA where required.



ISACA audit questions: test the design

01 Why is a distributed ledger necessary for this use case?

02 What personal data or linkable metadata reaches the chain?

03 Who can correlate users, transactions or events?

04 How are retention, erasure and key loss handled?

05 Who owns controls, incident response and rights requests?



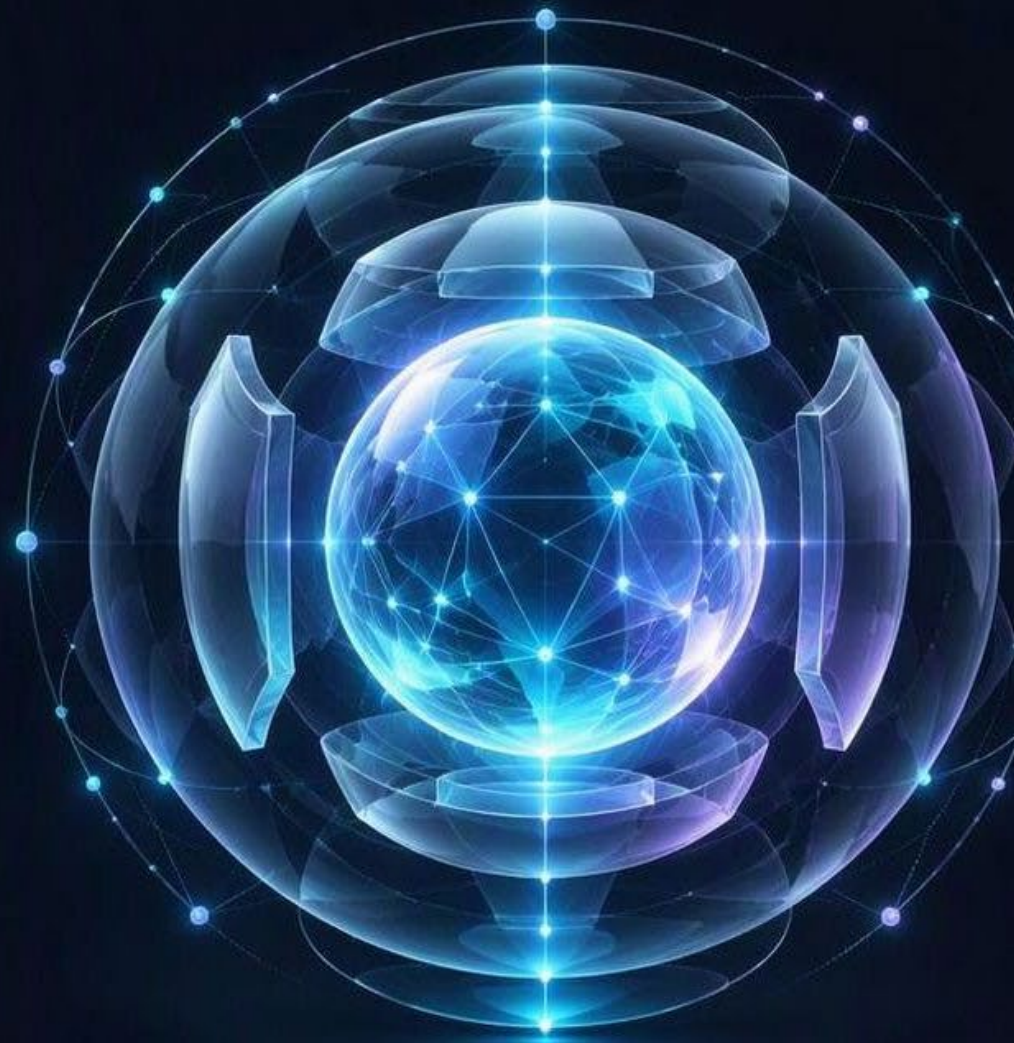
THE TAKEAWAY

Can blockchain keep a secret?

Yes — but only if we design for privacy from the outset.

Keep sensitive data off-chain. Prove only what is needed.

Limit visibility. Define accountability and deletion before launch.



Infosecurity Magazine

Log In Sign Up

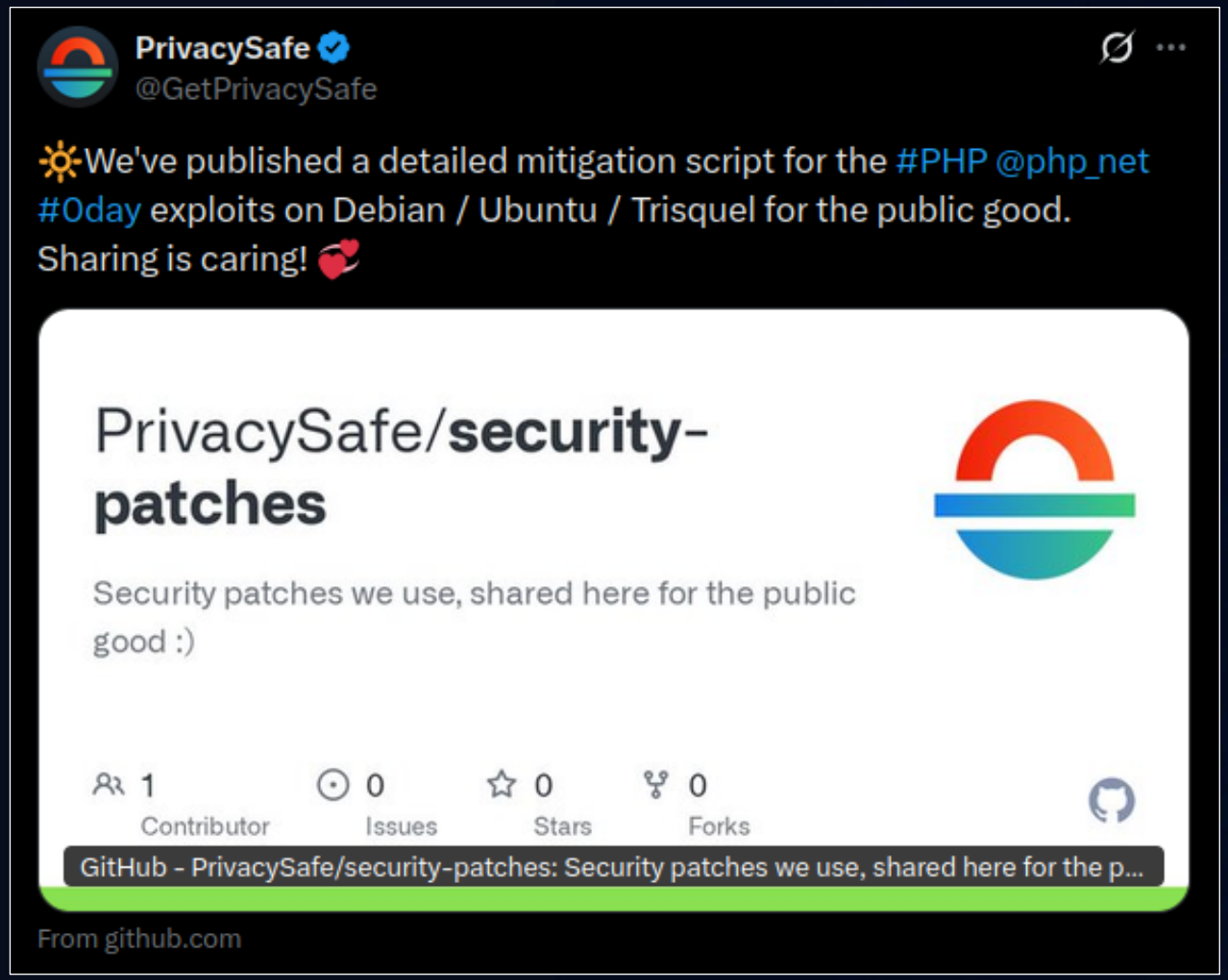
News Topics Features Webinars White Papers Podcasts Events & Conferences Directory

Infosecurity Magazine Home » News » Critical PHP Vulnerabilities Leaked Ahead of Scheduled Security Patches



NEWS 21 October 2026

Critical PHP Vulnerabilities Leaked Ahead of Scheduled Security Patches



Patch: psafe.ly/php0day

YOUR QUESTIONS. YOUR PERSPECTIVE.

Questions & discussion

Where would you draw the line
between transparency and privacy?

SLIDES. APP. PROOF OF CONCEPT. DEMO.

Thank you

privacysafe.app/sheree

Sheree Ip

Associate Lecturer
Curtin Law School

s.ip@curtin.edu.au

