The Emerging Role of ZKP in the Privacy Stack of Production Business Networks

Presented by: Peter Broadhurst, Co-Founder & Head of Engineering, Kaleido

kaleido

Enterprise Requirements for Blockchain Technology

- Privacy & Permissioning
- Performance
- Scalability
- Data Control
- Reliability

kaleido

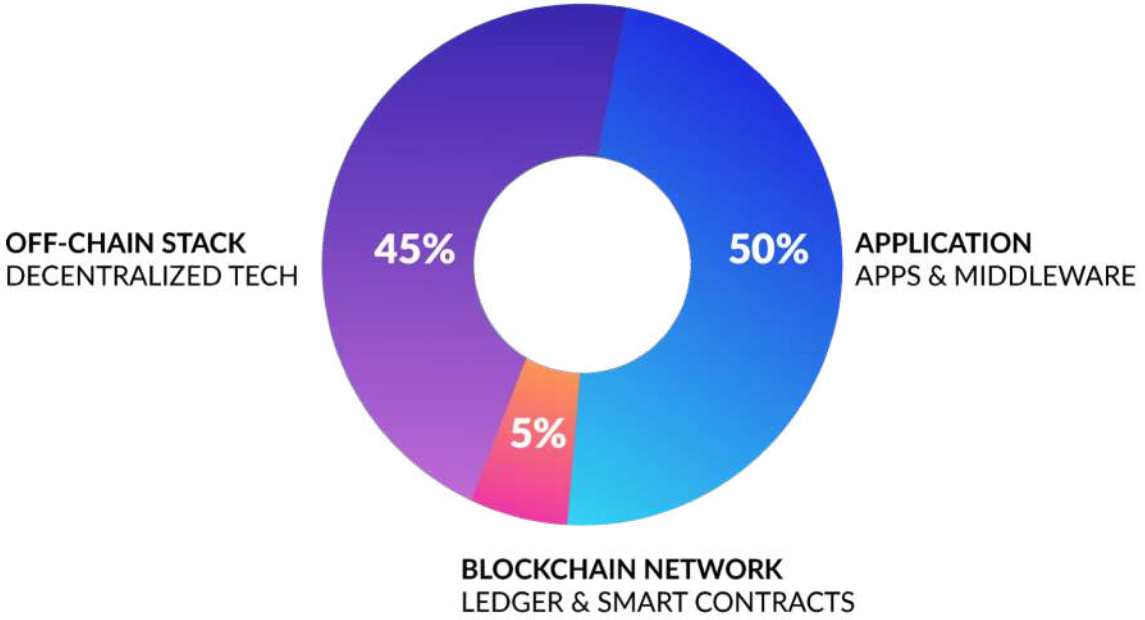
Modernizing Business Networks

Typical projects have over 40 components

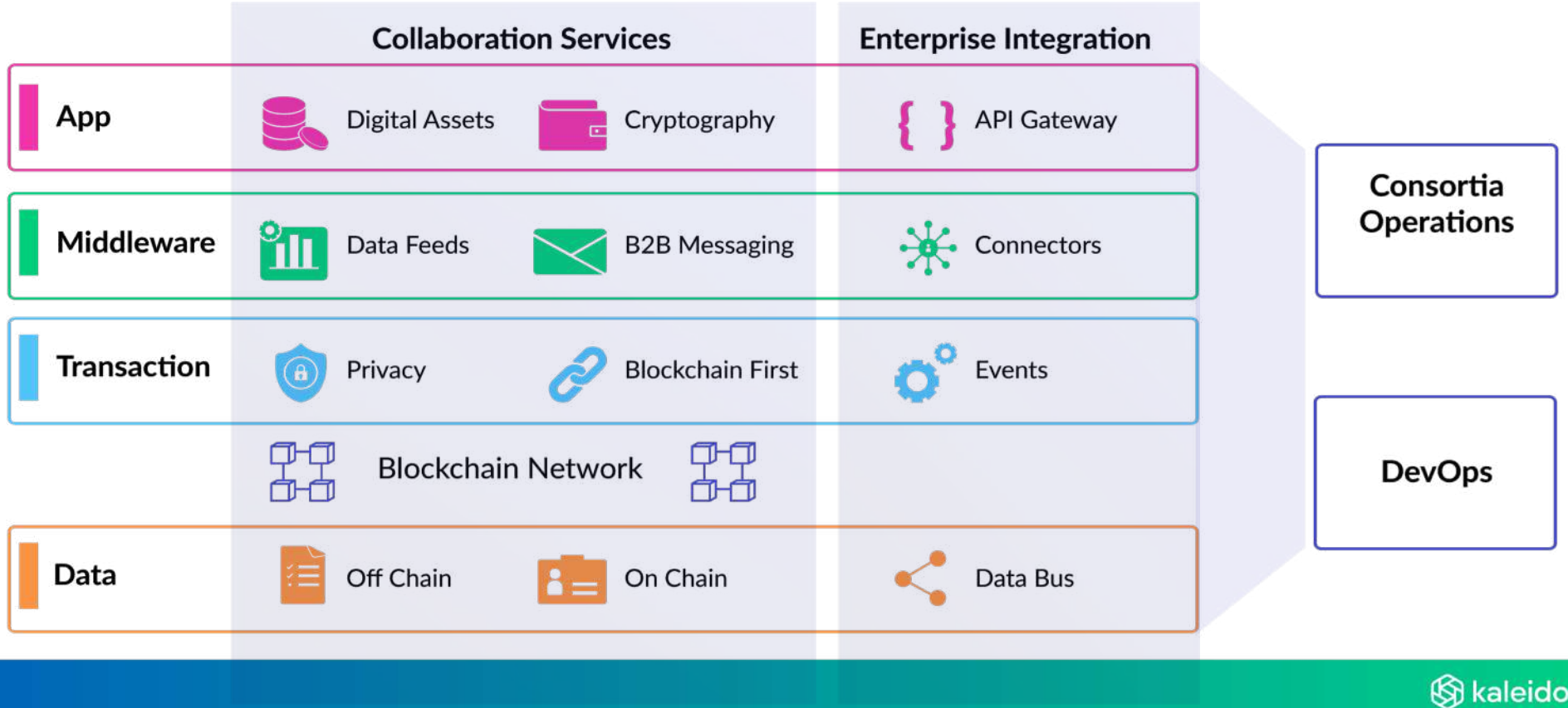
The chain is

ONLY 5%

of a complete blockchain solution



Full-Stack Blockchain for the Modern Business Network



The Challenge

The commodities trade financing industry is maintained by a surprisingly outdated set of systems and data management.

The business is huge, complex, multinational, and interconnected.

Governments have different regulations and political nuances

The Solution

A blockchain-based open network that brings commodity trade finance into the 21st century by:

- Optimizing financing processes
- Accelerating industry operations
- Digitized transactions
- Trusted source of documents to reduce fraud

komgo

MEMBERS INCLUDE

ABN·AMRO
ING
NATIXIS BEYOND BANKING
BNP PARIBAS
KOCH SUPPLY & TRADING
Rabobank
citi
MACQUARIE
CRÉDIT AGRICOLE GROUP
MERCURIA
SGS
GUNVOR
MUFG
SOCIETE GENERALE

The Results

In production with 15 global stakeholders in less than 4 months

Cash flow gains of 30 – 40%

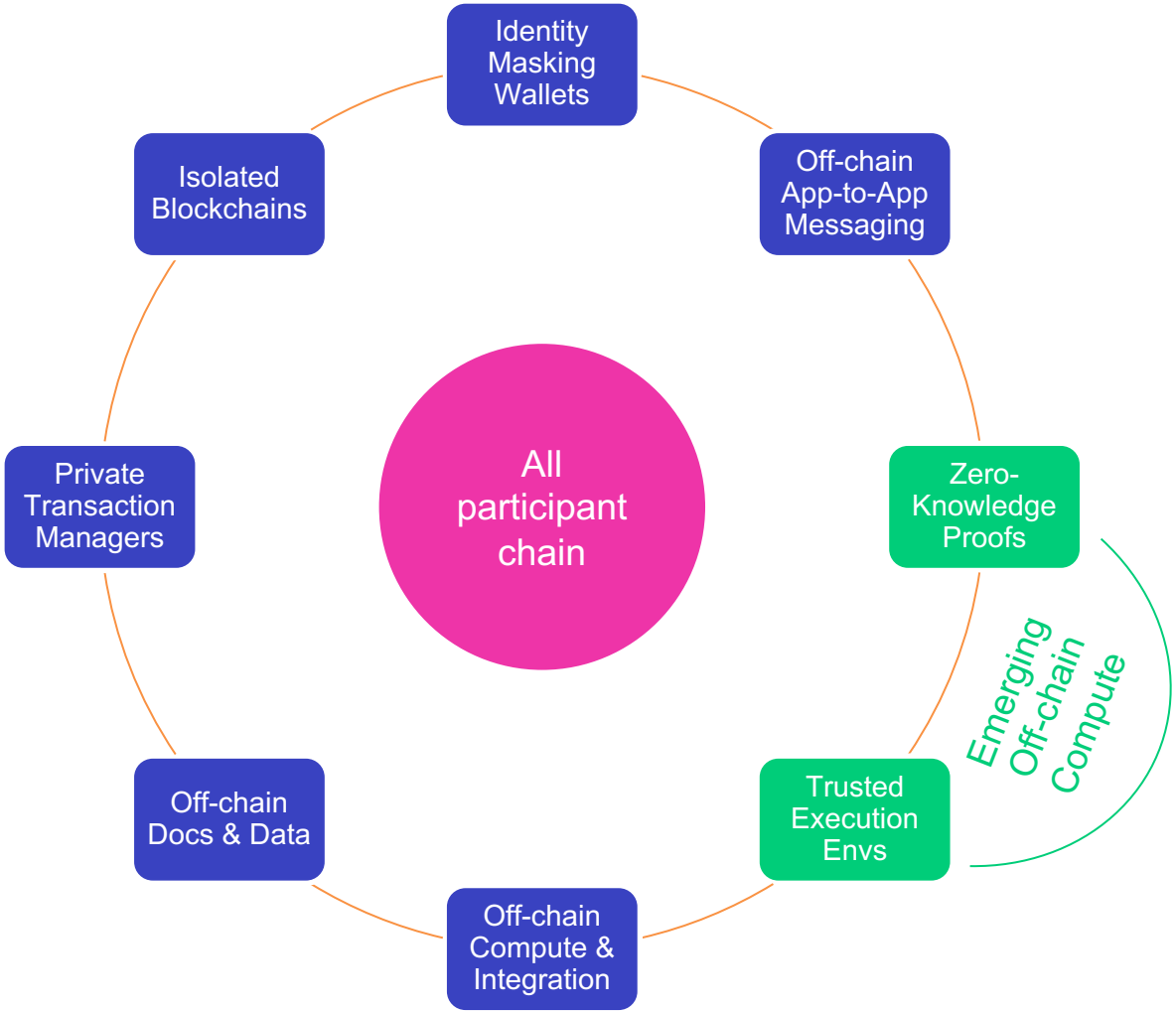
Full process allows maximum efficiency, 100x faster

Coordination with decreased human error and fraud

POWERED BY kaleido

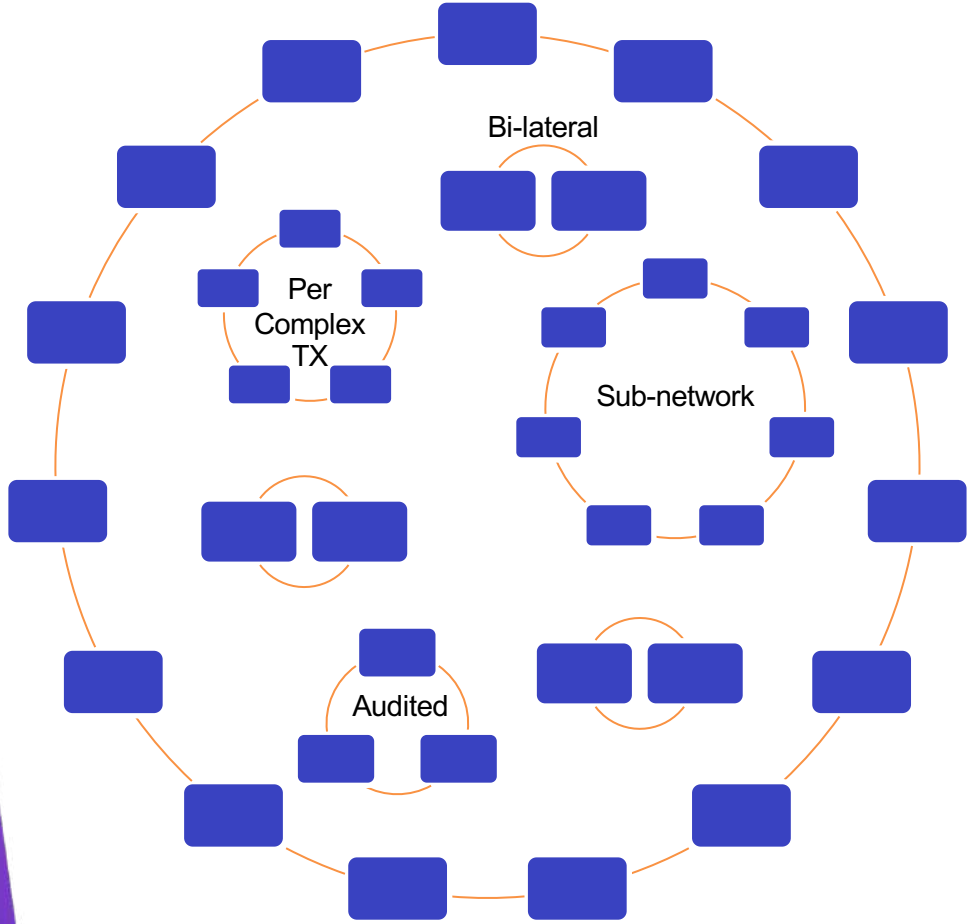
kaleido

Privacy Stacks in Production

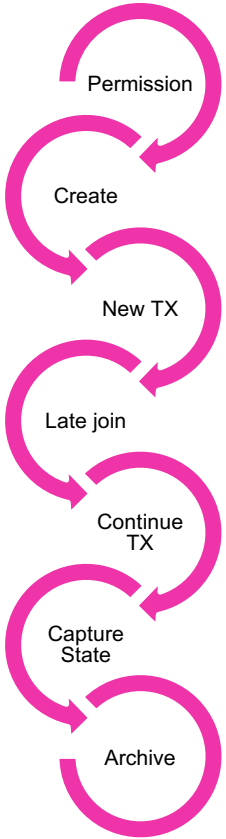


kaleido

Isolated Blockchains

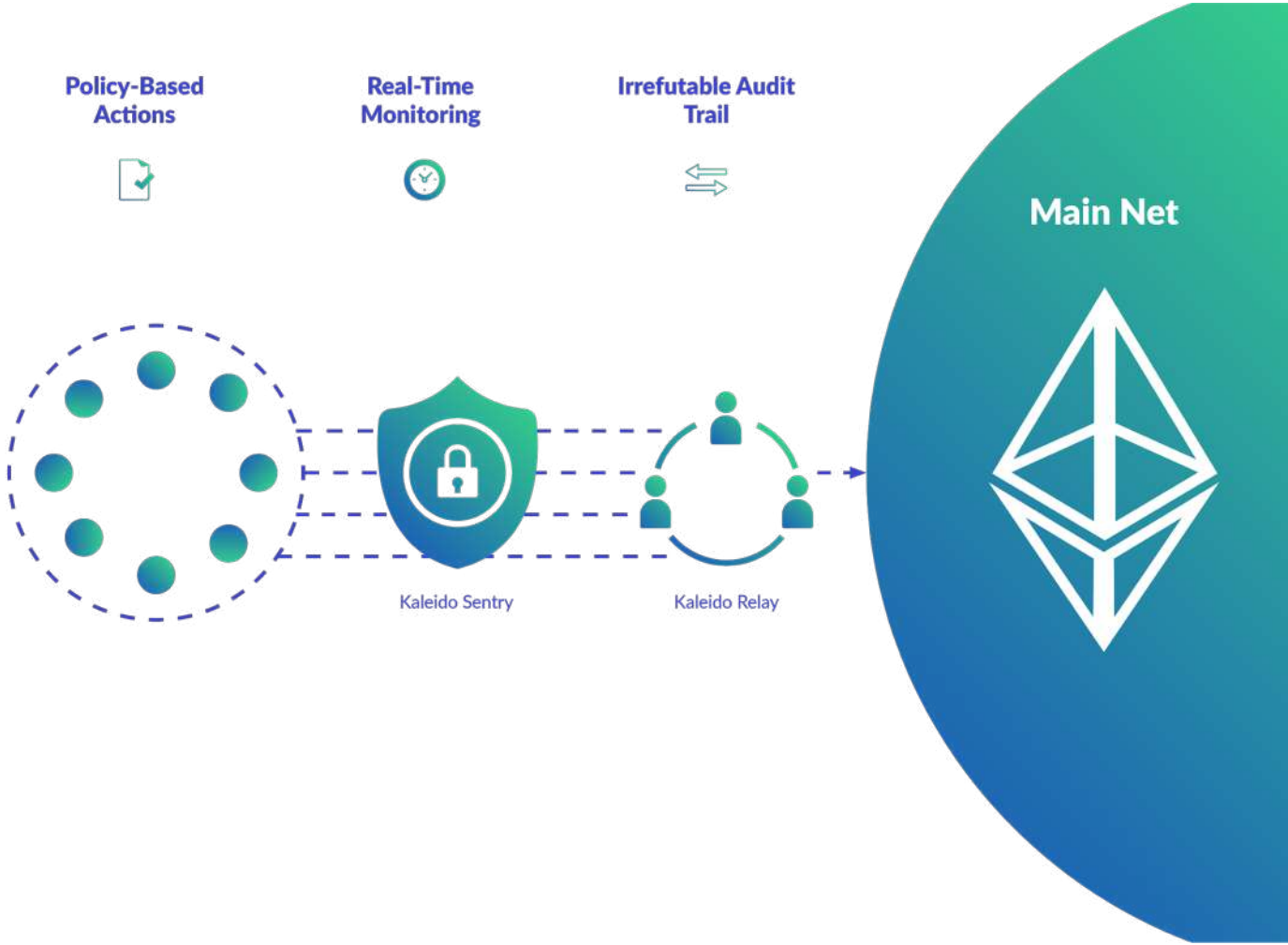


Lifecycle governance
Each chain is unique



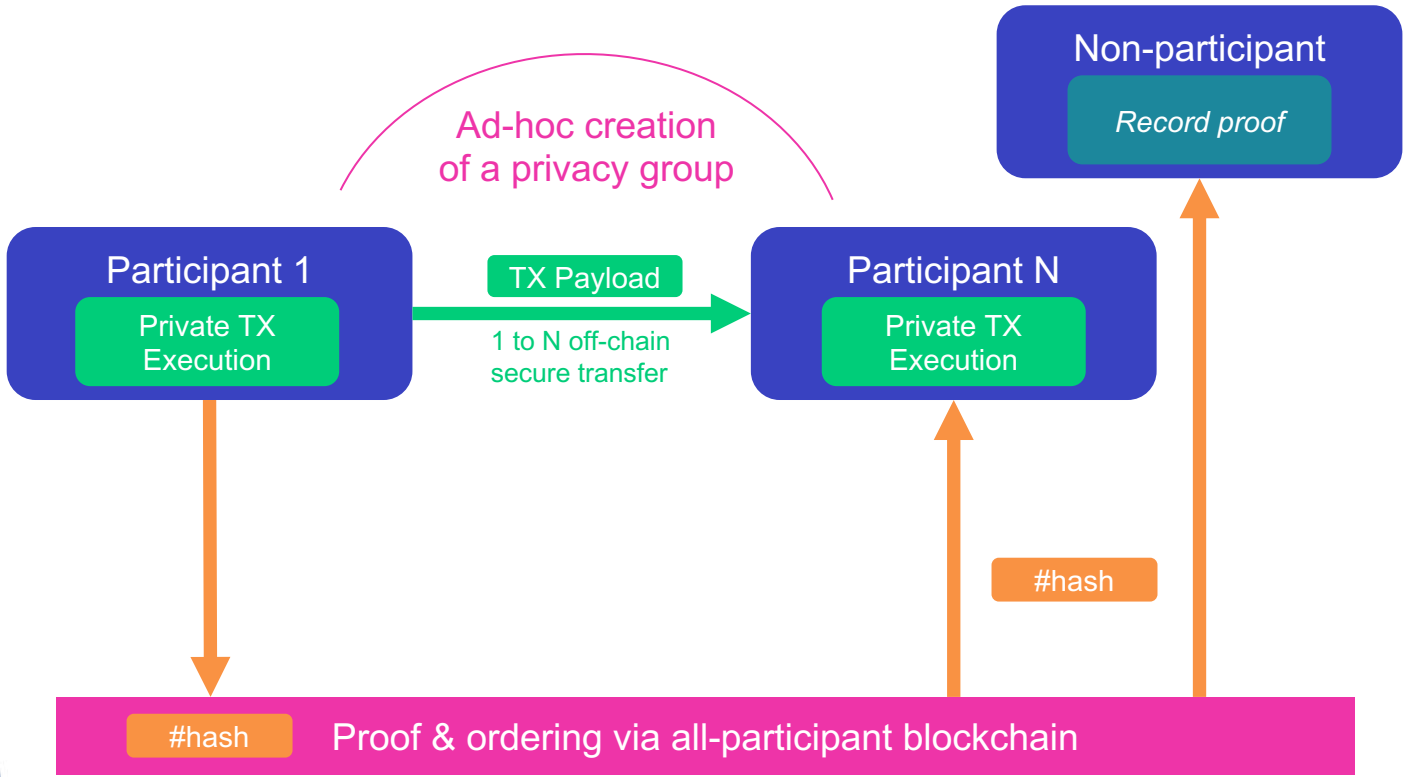
kaleido

Public Ethereum Tether Service



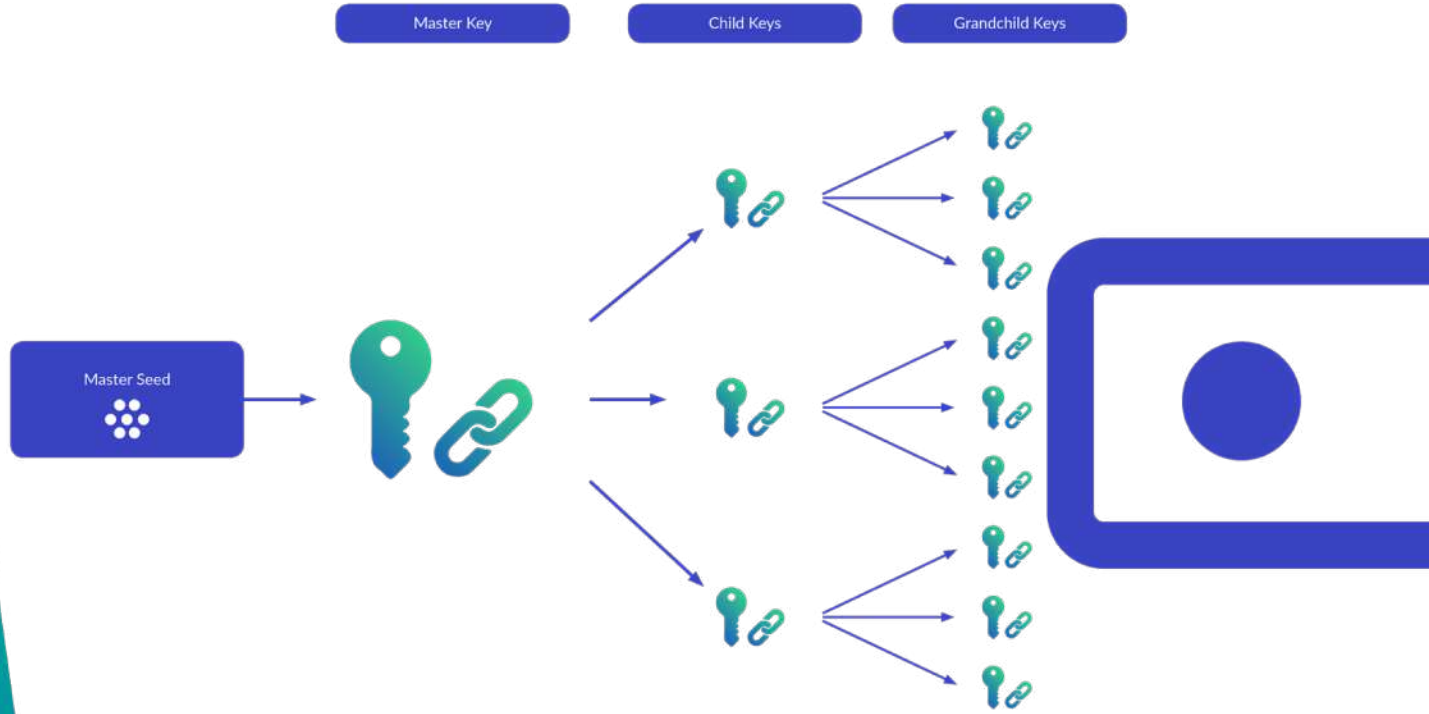
kaleido

Private Transaction Managers



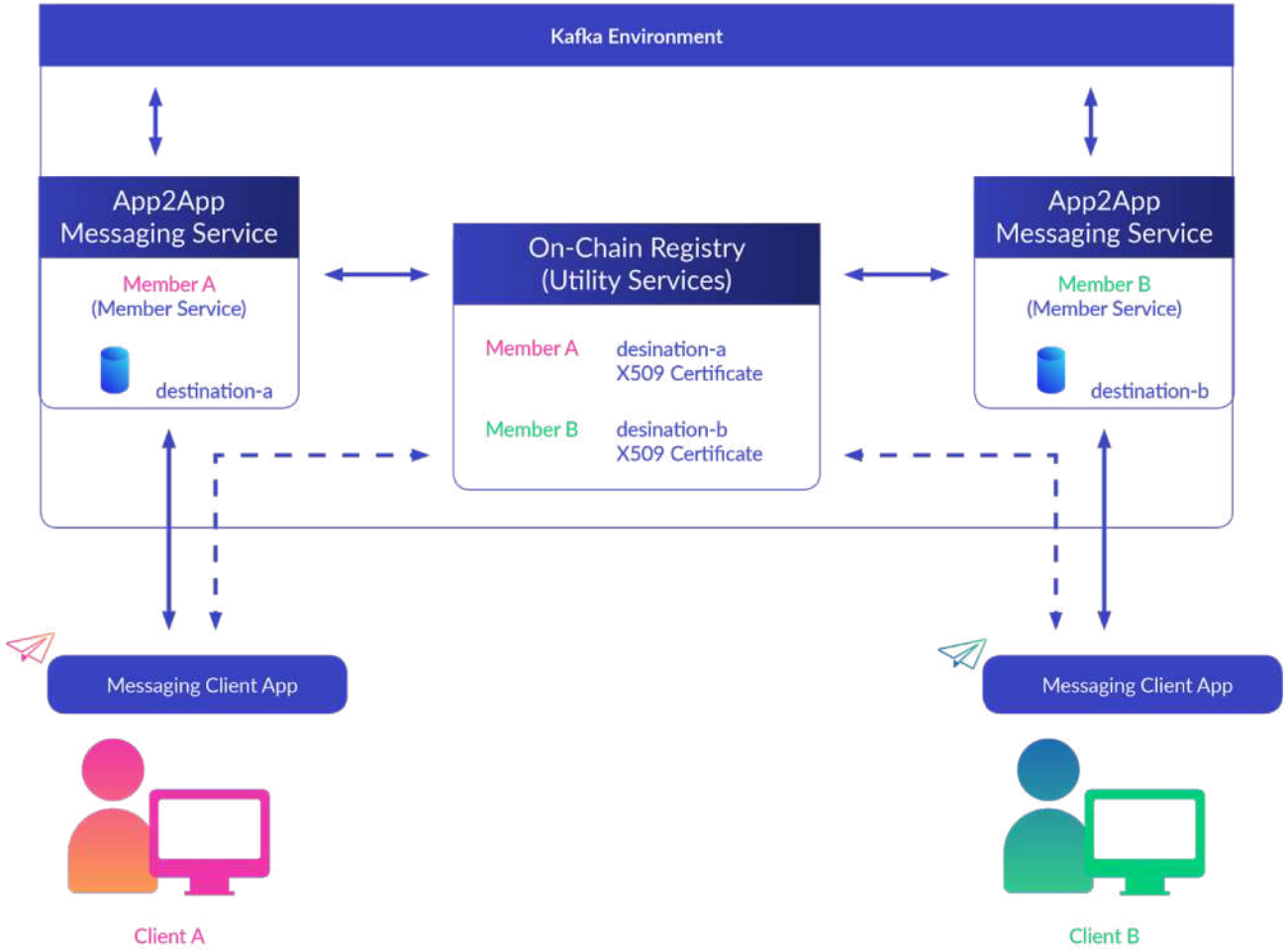
kaleido

Identity Masking HD Wallet



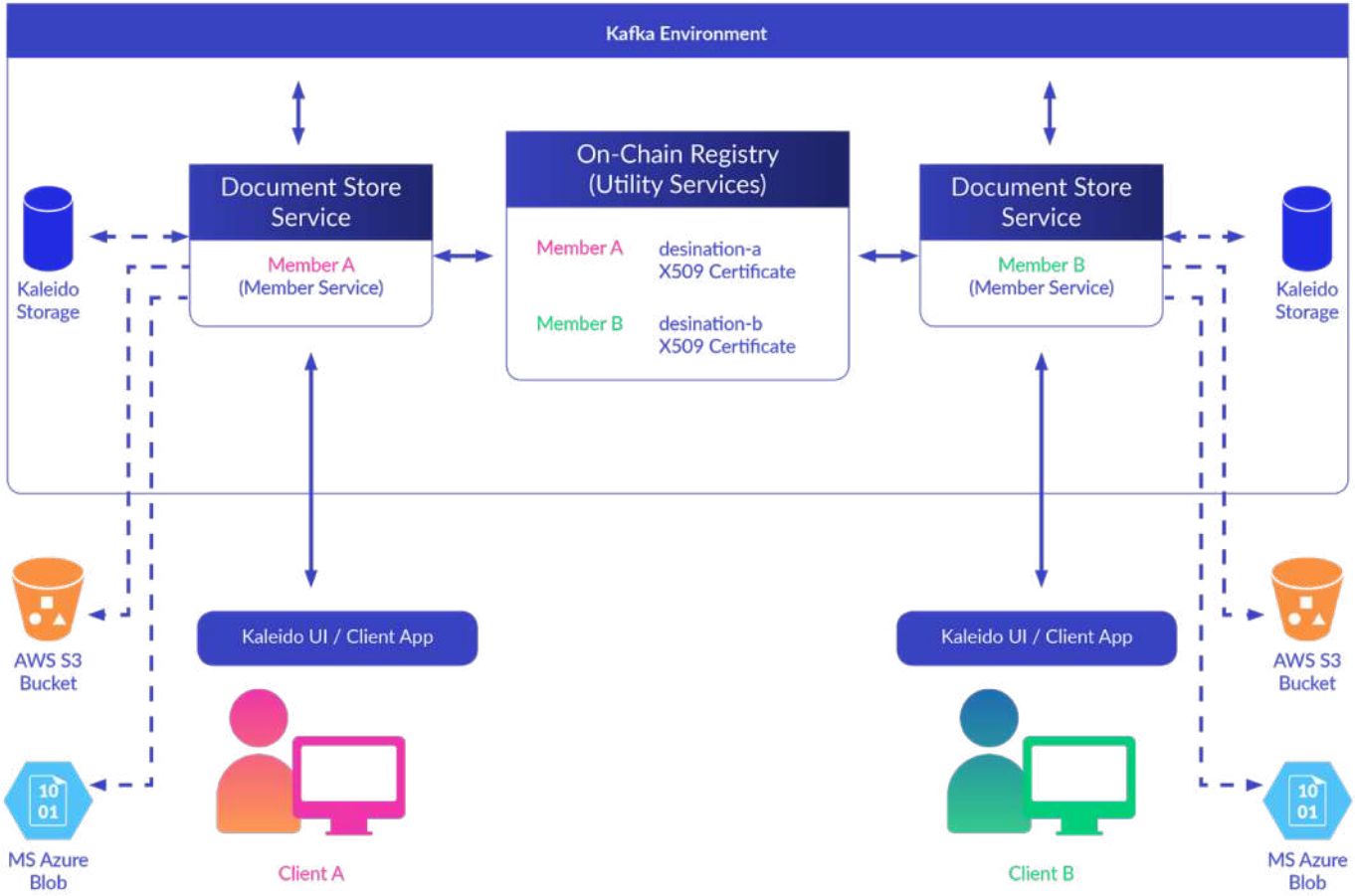
kaleido

App2App Messaging



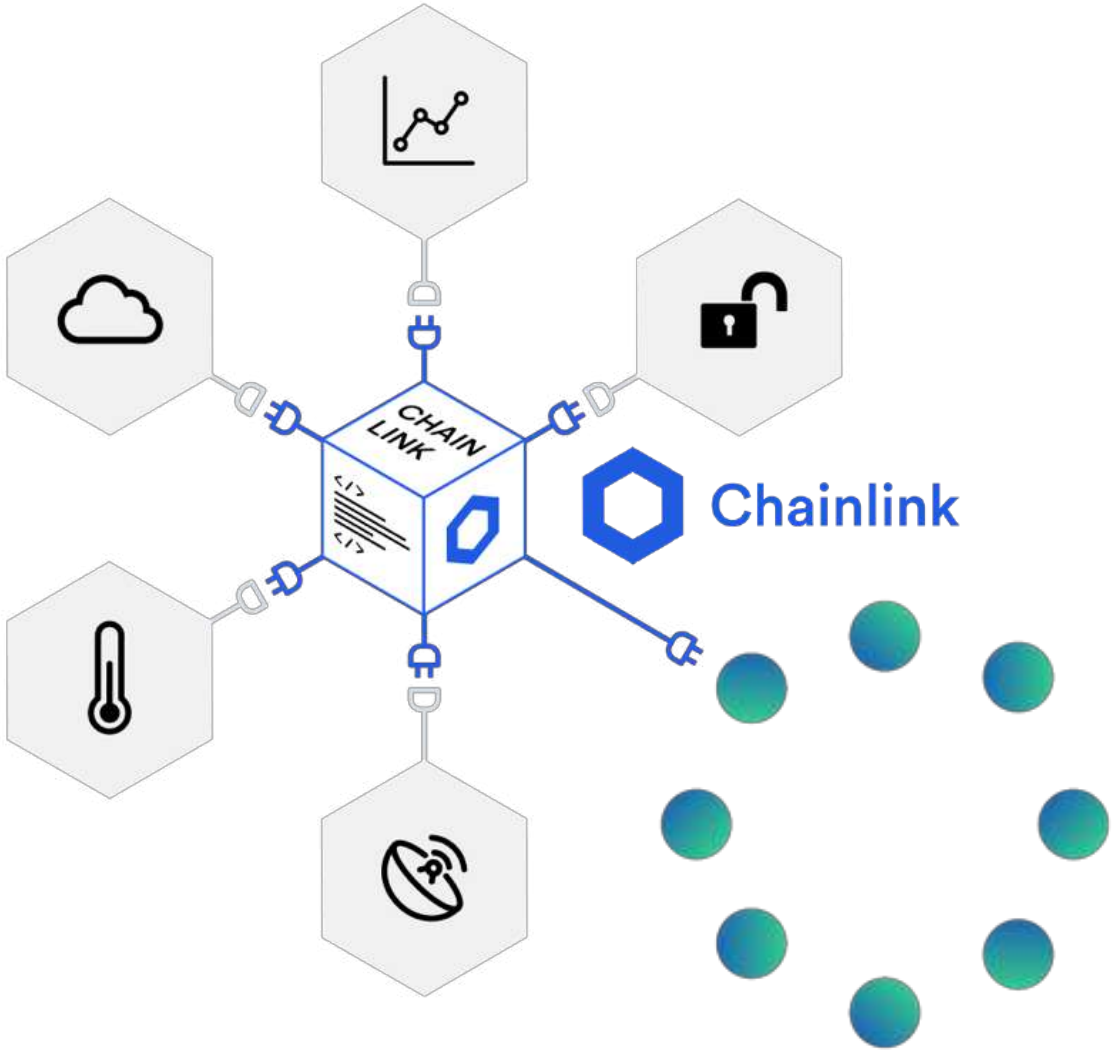
kaleido

Document Store



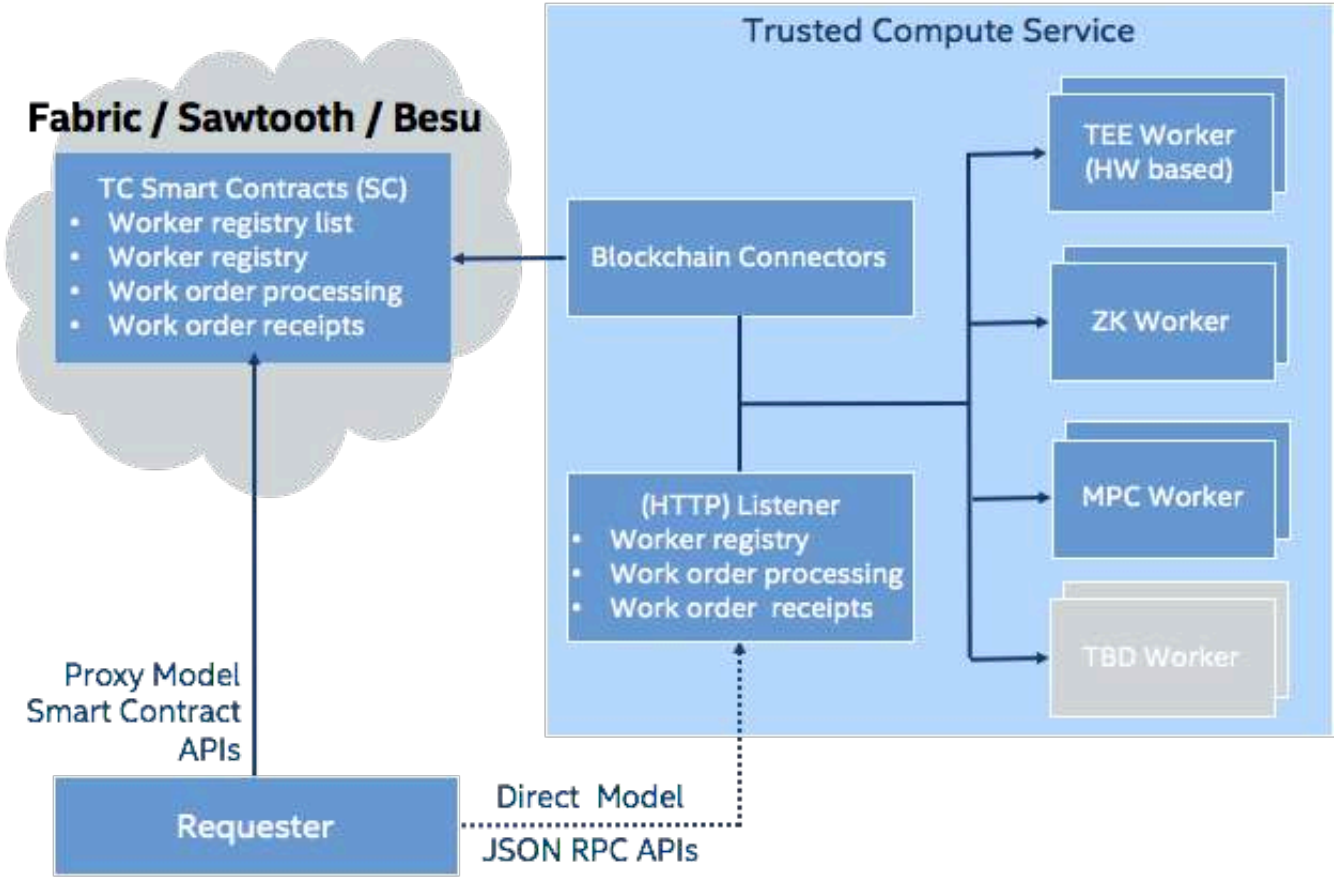
kaleido

Off-chain Compute / Integration



kaleido

Trusted Off-chain Compute



HYPERLEDGER AVALON

kaleido

The promise of Zero-knowledge Proofs for Enterprise

kaleido

The reality of ZKP in Production Enterprise Projects … today

kaleido

Progress towards ZKP Adoption

Trust in the Technology

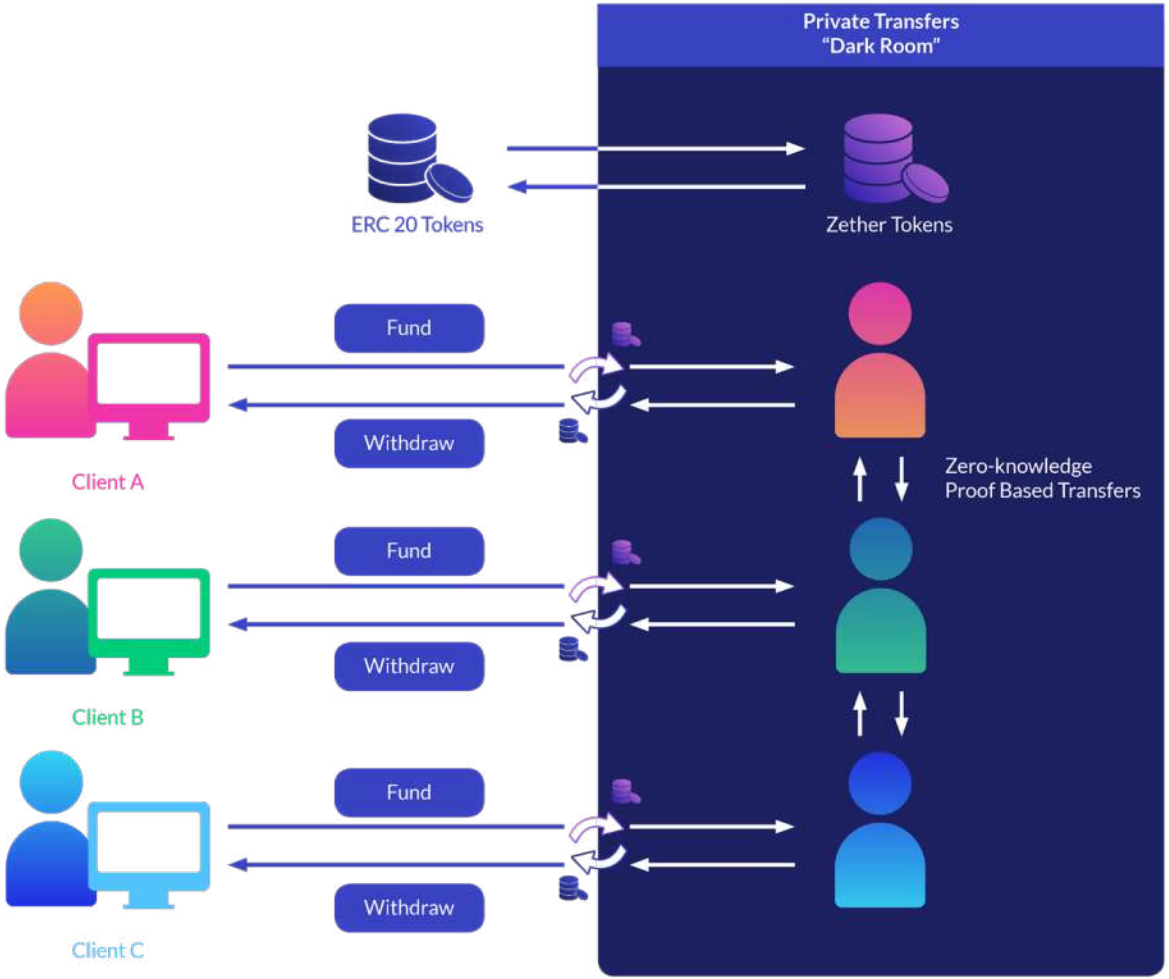
Implementation Complexity / Skillset

Flexibility of Proven Scenarios

Standards / Interoperability

kaleido

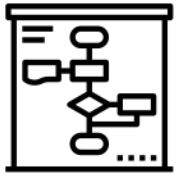
Zero Knowledge Token Transfer



kaleido

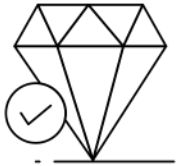
Opportunities for ZKP based Privacy in Smart Contract Logic

Rules of the Game



Complex State Transition Logic

All the State Provable to All Participants

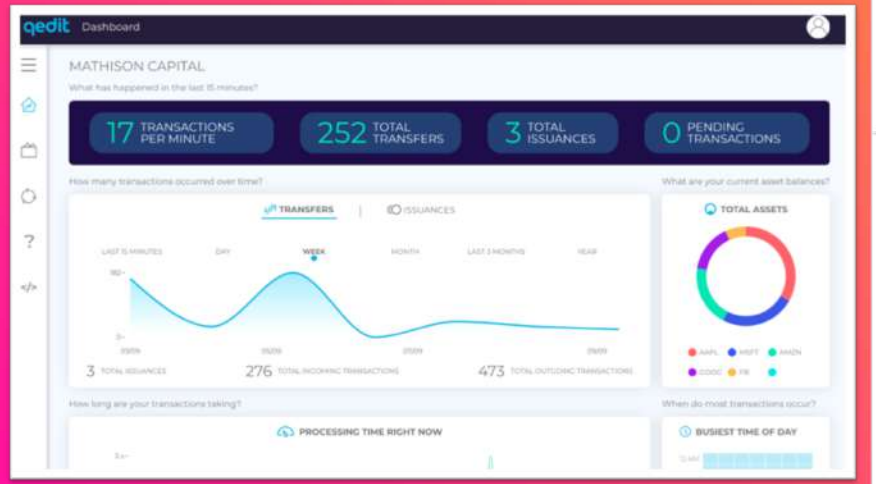


Pin Data & Things Off-chain, On-chain

kaleido

qedit

Private Asset Transfer



Keep sensitive transactional data off the blockchain with zero-knowledge proof cryptography

Enterprise-Grade Quality

Keep transaction details private while maintaining high availability and performance with a robust, production ready solution.

Standard Complaint Cryptography

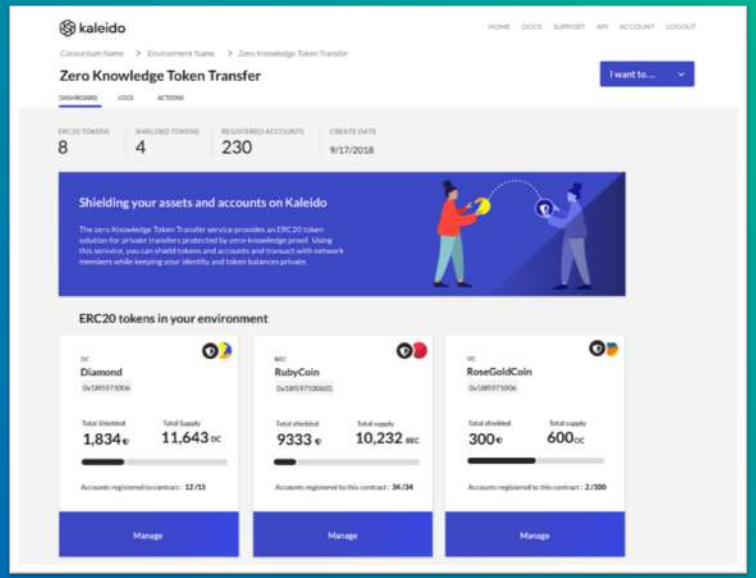
Future-proof your blockchain with a privacy solution that adheres to specifications defined by ZKProof.org, an open initiative of industry and academia to standardize the use of zero-knowledge proofs.

Controlled Transparency & Scaling

Use permissioned auditing tools and stay compliant with GDPR, CCPA and other local data privacy regulations. Generate zero-knowledge proofs using proprietary proof chaining (parallel proofing) technology that keeps pace with your transaction volume.

kaleido

Zero Knowledge Token Transfer



An ERC20 Token solution for private transfers

Innovative & Proven ZKP Technology

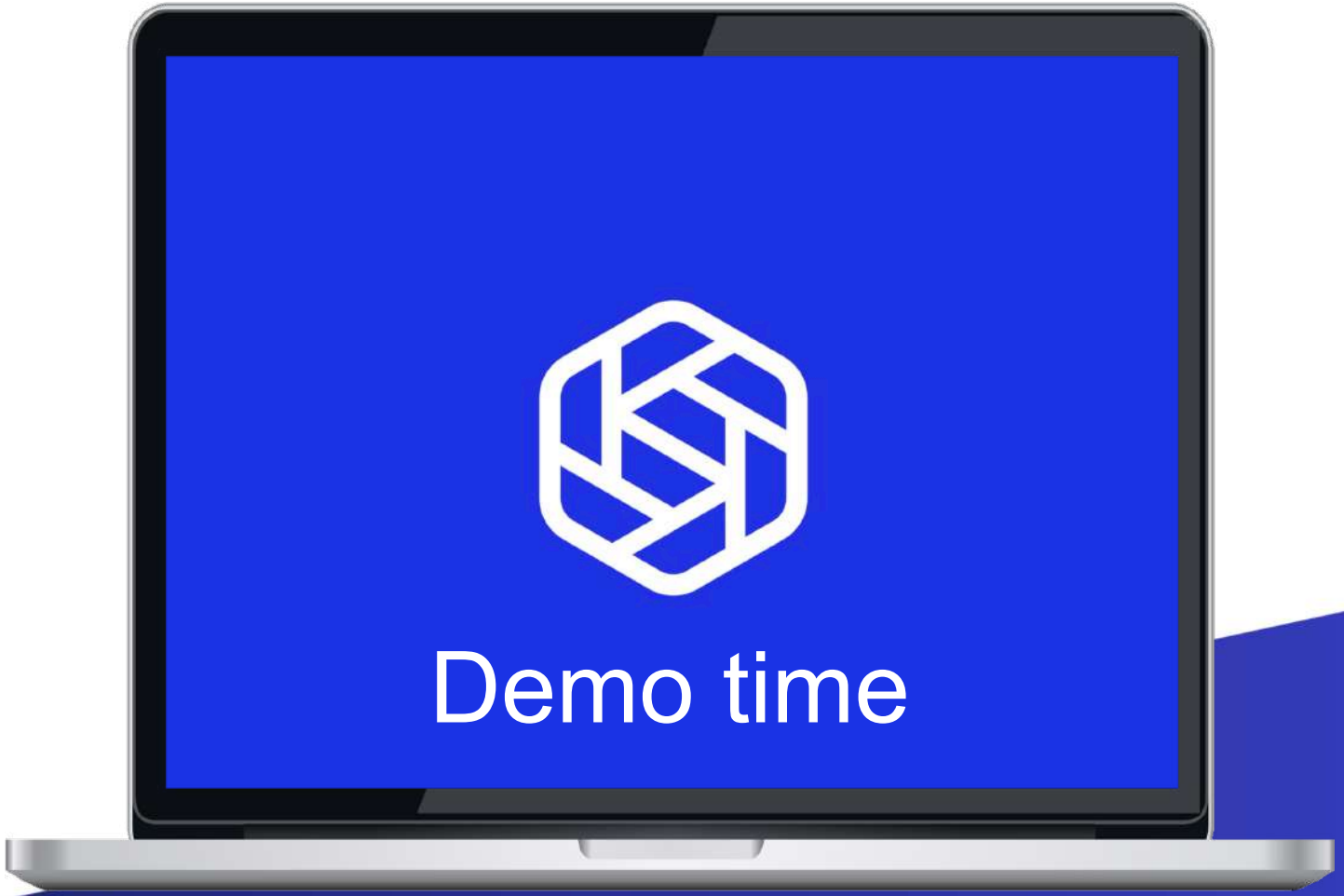
Zero Knowledge Token Transfer makes use of the latest technologies around zero-knowledge proofs and advanced cryptography.

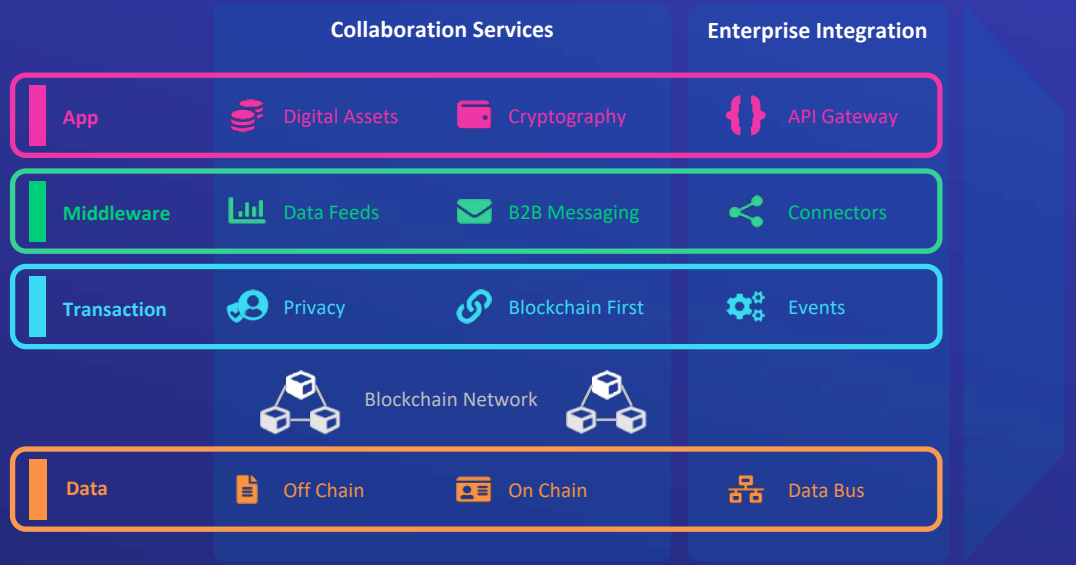
Fully integrated with ERC20

Incorporate ERC20 (fungible) tokens for any use case requiring privacy and anonymity.

Anonymous Token Transfers

Transact with members of your network without disclosing the details of token amounts or parties involved.


Demo time

kaleido

- Industry-first innovations
- Full-stack blockchain solution
- Built for enterprise
- Grows with your network
- Consultative approach
- Production infrastructure
- Production support
- Deep expertise