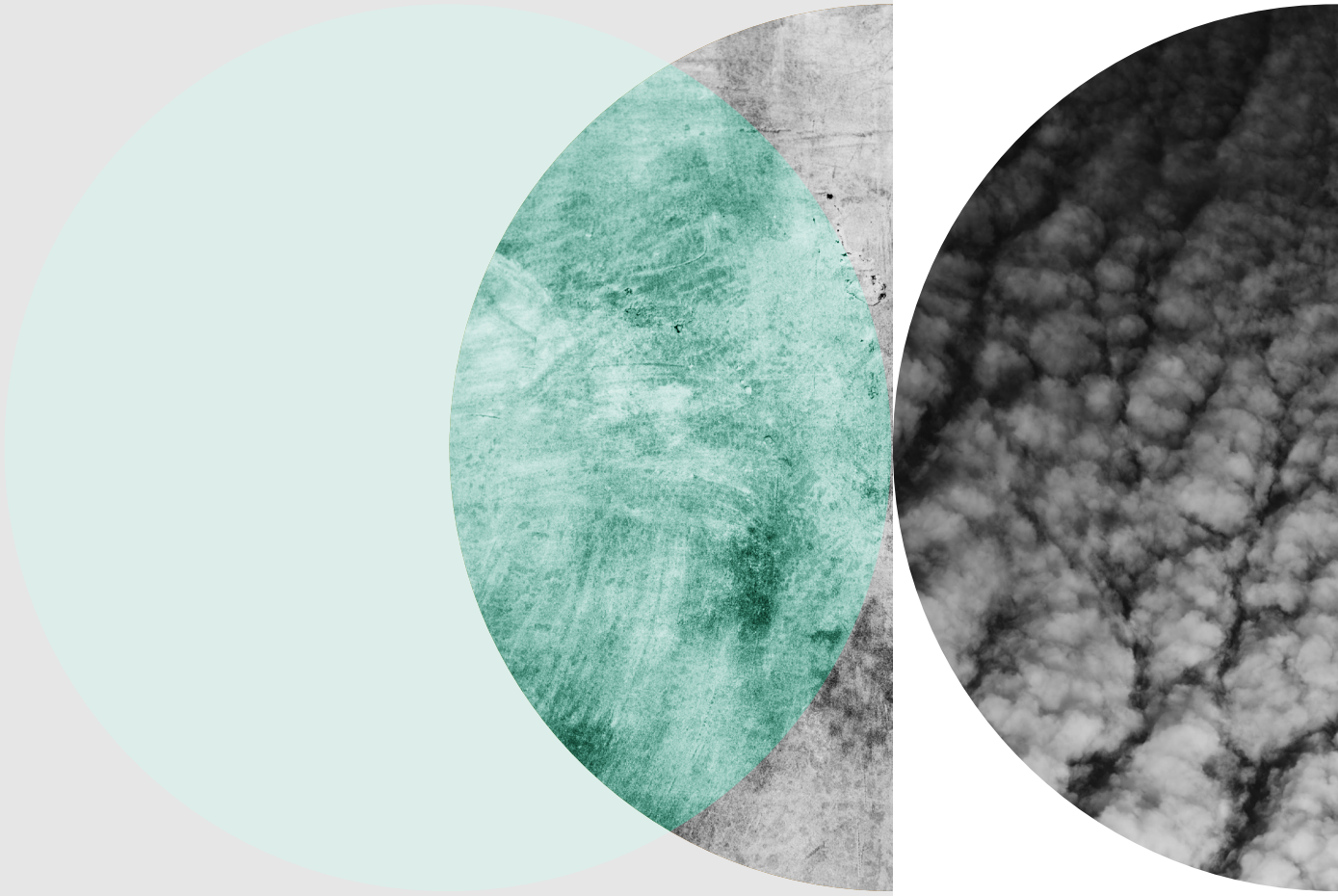
KEEP

MARCH / 2019

Business Primer



Contents

Background

Public blockchains offer significant, tangible benefits to businesses, but without a secure method for storing private data, these benefits can not be fully realized.

Public blockchains have brought unprecedented transparency and auditability to records that are immutable, reliable, and censorship-resistant.

However, businesses looking to build applications on public blockchains are faced with privacy issues; smart contracts published to the blockchain can be accessed by competing interests. Functions like verifying real-world identity only to intended parties or sharing secure information after specific conditions have been met are nearly impossible without publishing this confidential information to the public blockchain.

Keep provides the solution.

Introducing Keep

Keep is a privacy layer for Ethereum that makes it possible for smart contracts to harness the full power of the public blockchain.

The Keep network features off-chain containers for private data called keeps that give smart contracts deep interactivity with private data without compromising transparency or auditability.

Protected by secure multi-party computation (sMPC), Keeps are used to securely encrypt private data. Keep is one of the first production-ready sMPC systems for distribution on the public Ethereum blockchain.

The Keep network requires trusted randomness within the protocol for trustless selection and security. Keep is developing a random beacon to do just this, combining threshold signatures with digital relays to provide public blockchains with verifiable, distributed, and trustless randomness. The Keep Random Beacon selects providers for each new keep, and can serve any decentralized application (dApp) that requires on-chain trusted randomness.

For anonymity and flexibility beyond what multi-signature can offer, Keep builds on Threshold Elliptic Curve Digital Signature Algorithm (T-ECDSA) for keep signers. ECDSA is a cryptographic algorithm that allows a single signing key to be backed by a group of signing nodes, ensuring only rightful owners can spend their funds. Specifically, T-ECDSA leverages zero-knowledge proofs to provide confirmation of transactions and signers without exposing the information or players themselves.

While Keep will launch first on Ethereum, the underlying code is being crafted to easily allow for porting to new blockchains for cross-chain functionality. Supporting T-ECDSA keeps, the network enables cross-chain interactions from Keep's anchoring smart contract blockchains to value-holding blockchains like Bitcoin.

Separately, these technologies expand opportunities for public blockchains. Together, they are the foundation for the Keep network, able to store and compute data hidden even from itself, and Ethereum's first private computer.

◆

Applications

Keeps allow contracts to access stored private data that can be bought, sold, transferred, and revealed on the public blockchain, enabling interactivity with far more private data than any other solution available today.

Within Keep's sMPC system, each individual is given access to a small portion of a secret which is encrypted. To gain or share access to that secret, the outputs are reported back from all the individuals and decrypted to reveal the secret. This unique approach allows for the safe transfer of information from one party to another on the public blockchain without each individual needing to be online, providing a superior solution to current hash-reveal approaches, private blockchains, and zero-knowledge proofs alone.

Keep gives you private smart contracts. The applications of this system are unlimited, providing users with autonomy over personal information, cross-chain applications, custom dark pools for financial order matching, private file storage from smart contracts, global record systems, and much more.

Specifically, keeps can be used for:

> Decentralized Signing
> Dead Man Switch
> Custodial Wallets
> Encrypted Blockchain Storage
> Marketplaces for Digital Goods

Decentralized Signing

Acting as a digital notary, contracts will be able to assert their identity off-chain without requiring a third party confirmation of blockchain state. Integrating with tools like PGP, SSH, and TLS keep is a bridge to public private key infrastructure.

Dead Man Switch

Knowing when to expose private information is just as important as keeping it hidden. With keeps you can have trusts, estate plans, and other contracts automatically activated to expose instructions and transfer funds.

Custodial Wallets

Ethereum smart contracts can use keeps to generate their own cryptocurrency wallets to send Bitcoin, Litecoin, and Dash, allowing for cross-chain exchange. T-ECDSA reduces possibility for attack because keys can be stored on multiple nodes, with some of the shares stored offline.

Encrypted Blockchain Storage

Keeps provide a bridge to private blockchain storage making it possible for smart contracts and DAO's to store files privately. You no longer need to trust a third party with your most sensitive, private data. Think medical records, credit reports, and private financial data.

Marketplaces for Digital Goods

With keeps, you can easily and securely sell digital goods like ebooks, videos, MP3's and more by keeping files private until payment is verified. There's no need for a server and custom download processor to manage these files.

Token Mechanics & Incentives

Keeps must be highly available, robust against data loss, and maintain both confidentiality and data integrity. The Keep network's operating system is driven by incentives, underpinned by a staking-based economic consensus mechanism.

Used for staking, the KEEP token is a type of utility token, sometimes called a 'work token,' that is required for participation on the network. Node operators and keep providers are required to prove and lock up their holdings; to "stake" their network cryptocurrency. Staking incentivizes these players to run a reliable system by rewarding them with fees for their work.

Incentives for network participants:

Clients
Those who pay to use the keeps' storage capacity for secrets. Clients have the ability to purchase private data storage on keeps using the native token or ETH. They can choose from different keep types depending on the secret being stored and the guarantees needed.

Providers
Those who hold keep tokens and use them to compute and store secrets. Providers are paid to use their computing power and storage by operating keeps. Providers stake the network token to be selected to secure new keeps. For each new keep they help operate, the provider is required to put down an additional security deposit, and the rate the provider pay is agreed upon. Over time, providers are paid out for securely running keeps, and risk loss of deposit and pending payments for misconduct.

Staking also plays a major role in maintaining the integrity of the Keep network by minimizing attack incentives, since bad actors are at risk of losing staked value. Staking provides Sybil-resistance, making a network takeover incredibly expensive.

Market

To bring clients and providers together, the network includes a fair provider selection process. All staking providers participate in a random beacon used to select which will participate in a new keep. Independently and together, staking will be required for the random beacon, for T-ECDSA keeps, and for the full scale privacy protocol.

Keep uses staking for work selection, meaning that participants put their KEEP tokens forward in a bid to operate keeps (off-chain containers for storing private data) and earn cryptocurrency. In order to be chosen to provide a node for a new keep, a provider must lock up a minimum stake in KEEP for a withdrawal period. Used only for staking and the right to earn ETH cryptocurrency, the KEEP token is categorized specifically as a work token.

The Keep network's staking mechanism is structured so that the owning address of a token can perform minimal work and delegate most of the network operations to a separate operator address. This allows for the underlying wallet of the owning address to be kept in cold storage, making ownership of a token more secure, while maintaining flexible participation in the network.

The KEEP token will derive its value from use and demand. The greater the number of dApps that require trusted randomness and projects that use ECDSA keeps, the greater the complexity of the operation being run. With complexity comes increased staking incentives and demand for staking. As demand for service within the network grows, so too will the value of the token as more revenue flows to providers.

The Team

The team is comprised of a seasoned group of software engineers, strategists, and operators who create, build, and grow products in the crypto space.

Matt Luongo, Project Lead
Matt Luongo co-founded his first company in 2011 and has technical leadership experience at Insightpool and Agency Spotter among others. He has been working in cryptocurrency and blockchain since 2014 when he founded Fold and has since launched Keep. Matt is based in Atlanta, GA and is a husband and father of two.

Corbin Pon, Developer & Ops
Corbin is a graduate of the Georgia Tech College of Computing and native of Massachusetts. He's worked extensively in defense industry and was a researcher for the application of technology in International Development before being convinced to start several companies with Matt.

→

Antonio Salazar Cardozo, Head of Engineering
Antonio has crafted software across companies and open source projects for over 10 years, with a persistent emphasis on community, collaboration, quality, and usability.

Laura Wallendal, Head of Growth
Laura has extensive experience with growth, sales, business development and marketing strategy at a variety of companies. She's worked with teams of all sizes and has founded several tech companies.

Michael Gluzman, Head of Design
Michael heads design for Keep with a focus on delightful user-experiences and durable brands. Prior to Keep, he led design for Fold and a handful of note-worthy brands at The Coca-Cola Company.

Piotr Dyraga, Tech Lead
Piotr has held software engineering and lead roles across a range of industries including banking, networking, supply chains, and aviation. He loves to combine theoretical computer science with practical experience and he's delighted to do it at Keep. Outside of work, Piotr enjoys mountain biking and astronomy.

Promethea Rachke, Protocol Designer
Promethea is a software engineer and is an autodidact functional programmer with a strong interest in secure systems, exotic technologies, and novel cryptography.

→

Prashanth Irudayaraj, Research Manager
Prashanth has broad set of experiences ranging from Product Development at Alcoa, and Operations at Tesla. He worked as Research Faculty at the GTRI, where he was first introduced to blockchain technology.

Nik Grinkevich, Developer
With a decade of full stack and dev ops under his belt, Nik loves creating succinct and quality technical architecture. He's worked in a variety of sectors including fintech, adtech, and edtech.

Raghav Gulati, Developer
Raghav holds a background in math and distributed systems. His most recent job was at Backplane. Previously, he's held engineering and lead roles at Shyp and Insightpool. In his spare time, Raghav is a partner at the actively managed cryptocurrency hedge fund Sha Capital.

Jakub Nowakowski, Developer
Jakub is a software engineer with a financial background. He has been involved in multiple banking and telecom projects across all stages of the Software Development Life Cycle.

Erin Ng, Developer
Erin loves building beautiful applications, inside and out. She's helped companies such as Fitbit, Apple and Microsoft create delightful web experiences. Before teaching herself to code, she studied art at UC Berkeley.

→

Marcin Pawlowski, Developer
Marcin has a solid academic background blended with a healthy dose of startup experiences. He has published a number of papers about security, networking and cryptography.

Markus Fix, Developer
Markus has a long history of building resilient, distributed systems all over the world for the financial industry, the global supply chain and emergency response, fluent in all kinds of programming languages.

Nicholas Evans, Developer
Nicholas has taken some miscellaneous contracts in the space, but most recently worked at ConsenSys, where he held sessions on smart contract development and security, solved technical challenges, and trained developers on Solidity.

Eliza Petrovska, Community and Content Manager
Elizabeth is a blockchain enthusiast with a background in management, business, and online blogging. She has studied psychology and alternative medicine. She is also fluent in Russian.

◆

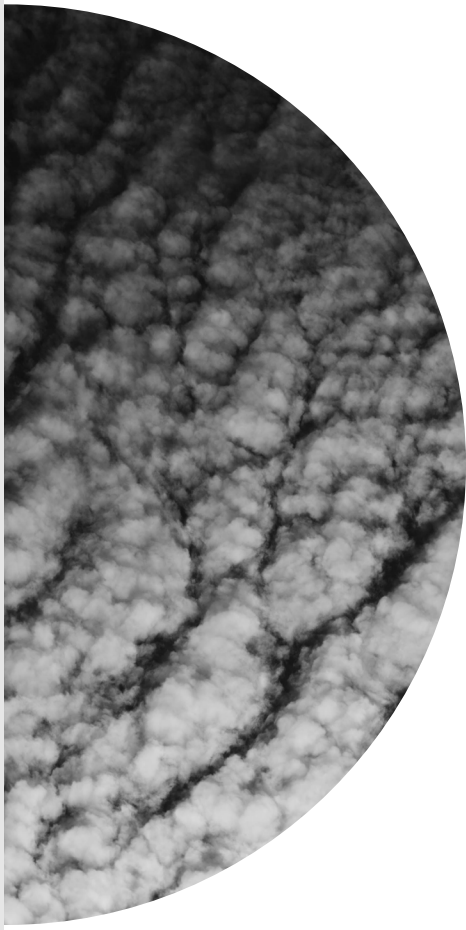
Summary

The Keep network makes it possible to store private information on the Ethereum blockchain. Using keeps, extensions to public blockchains, smart contracts can securely store private data off-chain, refer to it, and grant and revoke access, impacting the worlds of finance, healthcare, and business among many others. Permissioned access to private data paves the way for new blockchain use cases, and makes existing blockchain-based solutions possible.

◆◆

KEEP

MARCH / 2019



https://keep.network
support@keep.network