HYPERLEDGER URSA

What is Ursa?

HYPERLEDGER

Members Projects Community Resources News & Events Blog About

Type: Tool
Status: Incubation

Hyperledger Ursa is a shared cryptographic library that would enable people (and projects) to avoid duplicating other cryptographic work and hopefully increase security in the process. The library would be an opt-in repository for projects (and, potentially others) to place and use crypto. Hyperledger Ursa consists of sub-projects, which are cohesive implementations of cryptographic code or interfaces to cryptographic code. There are currently two sub-projects:

1. "Base Crypto" Library – Our first sub-project will be our "base crypto" library, of which the main feature is our shared modular signature library. This has the implementation of several different signature schemes with a common API, which allows for blockchain builders to change signature schemes almost on-the-fly (or to use and support multiple signature schemes easily).
2. Z-Mix – Our second sub-project will be Z-mix. Z-mix will offer a generic way to create zero-knowledge proofs that prove statements about multiple cryptographic building blocks, including signatures, commitments, and verifiable encryption. The goal of this subproject is to provide a single flexible and secure implementation to construct such zero-knowledge proofs. Z-mix consists of C-callable code but there are also convenience wrappers for various programming languages.

HYPERLEDGER

Members Projects Community Resources News & Events Blog About

HYPERLEDGER URSA

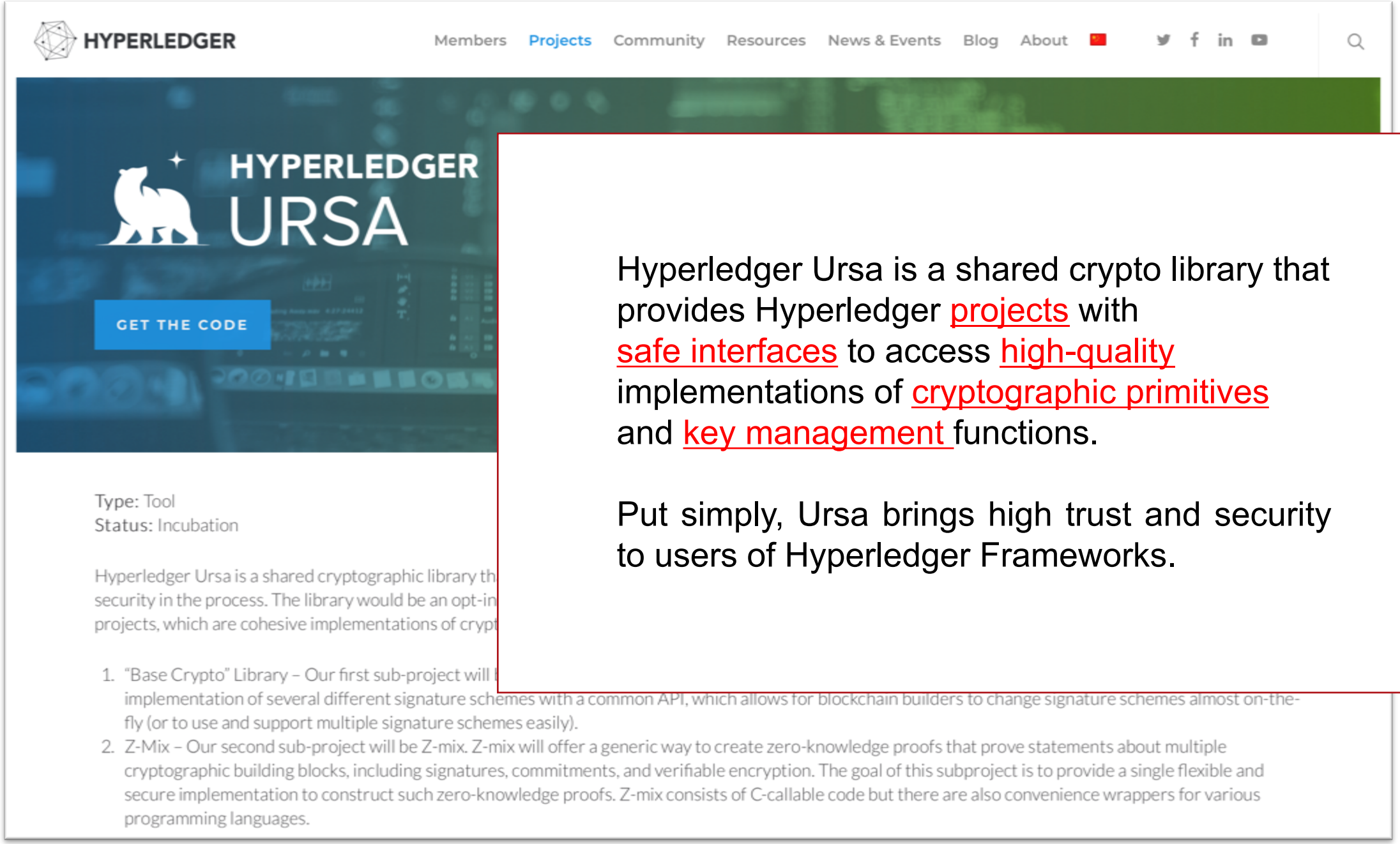
GET THE CODE

Type: Tool
Status: Incubation

Hyperledger Ursa is a shared cryptographic library th
security in the process. The library would be an opt-in
projects, which are cohesive implementations of crypt

1. "Base Crypto" Library – Our first sub-project will
implementation of several different signature schemes with a common API, which allows for blockchain builders to change signature schemes almost on-the-fly (or to use and support multiple signature schemes easily).
2. Z-Mix – Our second sub-project will be Z-mix. Z-mix will offer a generic way to create zero-knowledge proofs that prove statements about multiple cryptographic building blocks, including signatures, commitments, and verifiable encryption. The goal of this subproject is to provide a single flexible and secure implementation to construct such zero-knowledge proofs. Z-mix consists of C-callable code but there are also convenience wrappers for various programming languages.

> "Hyperledger Ursa is a shared cryptographic library that would enable people (and projects) to avoid duplicating other cryptographic work and hopefully increase security in the process. The library would be an opt-in repository for projects (and, potentially others) to place and use crypto."



Hyperledger Ursa is a shared crypto library that provides Hyperledger projects with safe interfaces to access high-quality implementations of cryptographic primitives and key management functions.

Put simply, Ursa brings high trust and security to users of Hyperledger Frameworks.

Why?

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

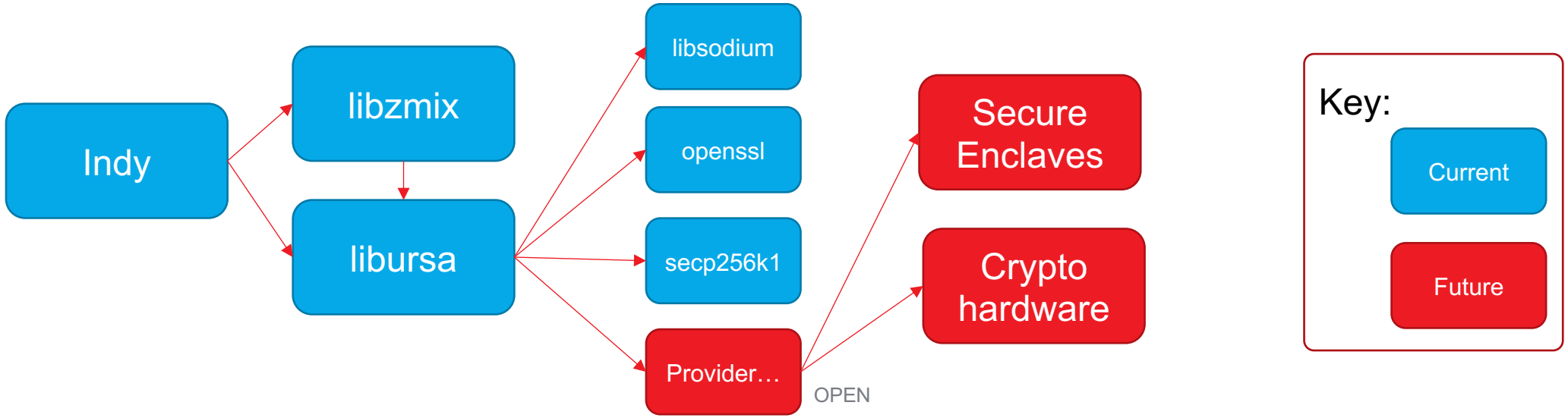
- Note: monoculture is bad, but own crypto is worse…

What do we have today?

- LibUrsa
  - Designed for cryptographic primitives like simple digital signatures, encryption schemes, and key exchange.
  - 2 interfaces:
    - Cryptographer interface for power and composable crypto
    - Developer interface for safety and ease of integration
- LibZmix
  - A generic way to create zero-knowledge proofs, proving statements about multiple cryptographic building blocks, containing signatures, commitments, and verifiable encryption.
- Hyperledger Indy using Ursa already 🎉

What do we have today?

- We DO NOT write the actual crypto (unless we really have to!)
  - We use other best-of breed implementations:
    - Libsodium
    - Openssl
    - Libsecp256k1 from bitcoin-core
    - …
  - We are architecting in support for 3rd party providers such as HSMs



Where are we going?

- Technology advancements
  - HSM integration
  - Enclave integration
  - More algorithms and crypto

- Frameworks integration
  - Indy – more
  - Fabric
  - Sawtooth
  - Iroha

  } Transition policy / priority TBD

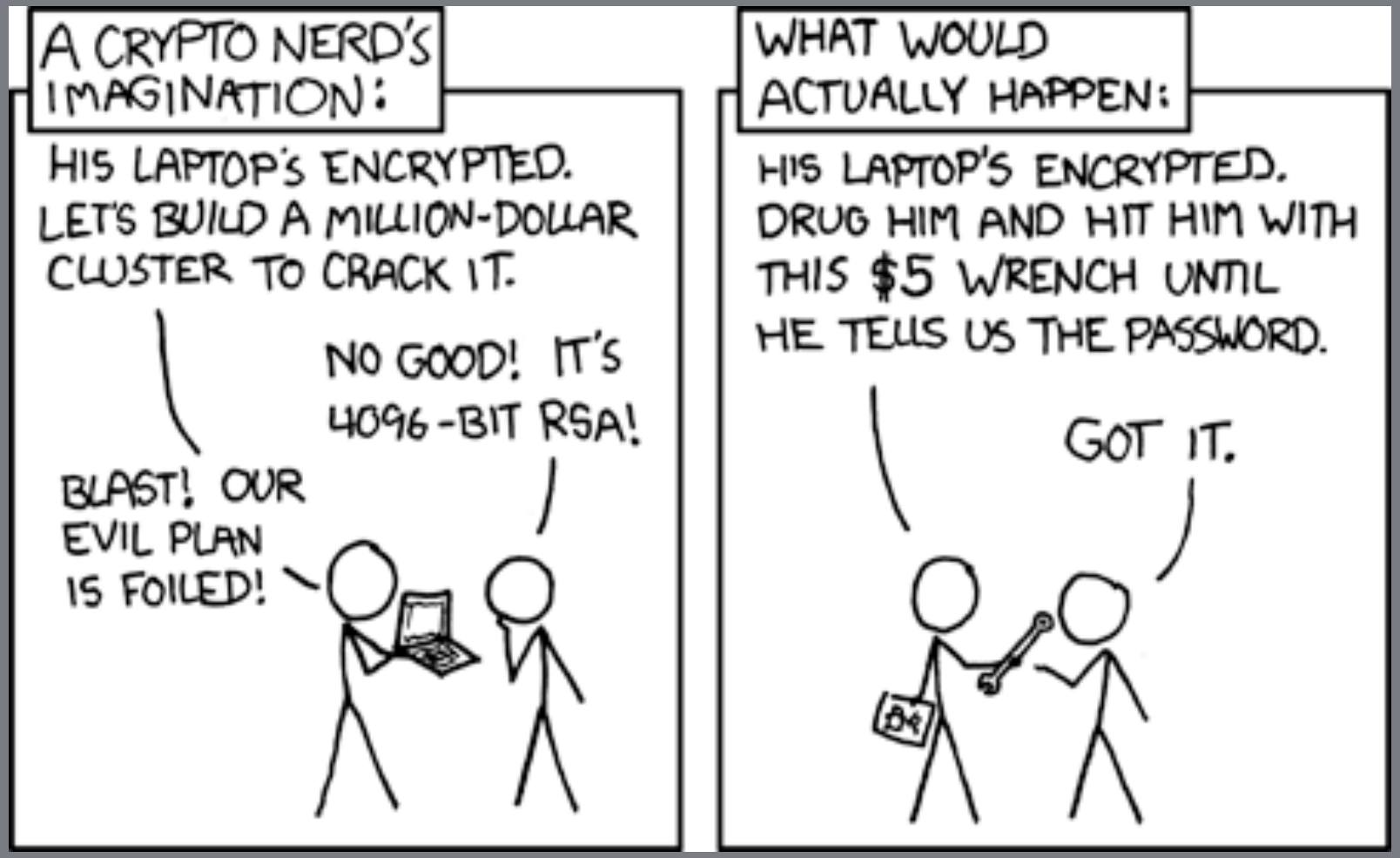
- Non-framework integration
  - Aries (AnonCreds)

Who’s involved?

- Among other highly valued contributors we have:
  - Hyperledger security staff
  - Identity security experts
  - Zero-knowledge proof experts
  - Cryptography experts
  - Crypto hardware experts
  - Key management experts

- Strong governance structure around contributions
  - Depending on sensitivity
  - Depending on impact

Who’s involved?



Who’s involved?

PLEASE JOIN US!

Ways to collaborate

- Use cases and requirements
- Standards, RFCs
- Reviews and feedback
- Contributions*

HYPERLEDGER
URSA

*Conditions apply. Qualified applicants only ☺

jitsuin

Truth In Things

Thank you

Jon Geater
CTO & Co-Founder
jon.geater@jitsuin.com
+44 7500 786537