sikoba
RESEARCH

Call for Interns 2019

April 2019

1 Internship opportunities

Sikoba Research aims to conduct fundamental and applied research in the areas of cryptography, blockchain and distributed systems. We are developing the project **isekai**, a verifiable computation framework, which allows a 'prover' to ensure a 'verifier' that he executed a given computation. Verifiable computation is an active domain of research that has recently attracted focus due to practical implementations being developed. We are proposing several internships related to this area. These require only good programming skills, but not necessarily any knowledge of cryptography. We are open to proposals for other topics in the areas of cryptography, blockchain or consensus protocols.

First internship topic: WebAssembly

WebAssembly is a new technology which is making the web 3.0 by bringing native speed and multiple languages support to the web. We would like to have an **isekai** frontend which can read and interpret WebAssembly files (wasm), so that we can use the **isekai** backend to generate an arithmetic representation of the WebAssembly code.

Second internship topic: C extensions

In order to be able to generate a proof of the execution of a program, the program is first converted into an arithmetic circuit. However our conversion currently support only a limited set of the C programming language. The purpose of the internship is to support more features such as more data types (char, string, float, array..), function calls, integer division, float operations, memory allocations, etc. Note that the project is written in Crystal programming language.

Third internship topic: Bulletproofs

Bulletproofs is a zero-knowledge scheme having an implementation written in rust. The goal of the internship is to create a C library that is using the Bulletproof Rust API in order to generate and verify proofs from j1cs files.

Internship details and contact

These are paid internships based in Luxembourg, but a combination of remote and on-site work is also possible, For more information, please contact **Guillaume Drevon** at **gd@sikoba.com**, tel **+352 691 15 22 15**.

2 Sikoba Research

In this section, we provide an overview of the research topics of Sikoba Research.

2.1 isekai

Guillaume Drevon is in charge of developing isekai. Isekai is a verifiable computation framework, which allows a 'prover' to ensure a 'verifier' that he executed a given computation. The proofs that isekai produce are called zero-knowledge proofs, meaning that one can verify if a statement is true without having any other information. For instance, you could produce the proof that you have the password for a specific account, without revealing your password.

What we want to do with isekai is to propose a framework that will allow people to independently choose the programming language and the verification system, so that they can try several options without having to make early choices at the beginning of a project.

Github repo: `https://github.com/sikoba/isekai`

2.2 Cryptography research

Dmitry Khovratovich will be in charge of isekai research efforts, working on the following deliverables:

1. Theoretical paper on data-dependent memory and code access techniques: known effective approaches, available implementations, feature and performance comparisons, suggestions.
2. Implementation guidelines for data-dependent memory/code feature integration.
3. Introduction paper to Bulletproofs and STARK proof systems: features, performance, program format, comparisons, available implementations.
4. Implementation guidelines, gadget selection, benchmark targets for STARK and Bulletproofs.

2.3 Consensus protocols and tokenomics

2.3.1 Consensus Protocol

The focus of our research so far was on fast and efficient consensus protocols, which are able to achieve consensus in few steps under favourable circumstances. We will continue to complete our research in this area, but the focus as of 2Q19 will shift to the Optimisation Consensus Protocol.

We also plan to work on two related primitives:

1. *Threshold cryptography* in variable environments, in which nodes can dynamically join and leave the network.
2. *Cryptographic common coins*, which are required for efficient Byzantine consensus.

The research will mainly focus on evaluating the state of the art in these areas, with the aim of selecting a solution that fits the needs of the future sikoba blockchain.

2.3.2 Token Economics and Distributed Systems Governance

So far this year, we have worked on the POS (proof of stake) model for Fantom Foundation, as well on the Fantom token economic model in general.

Another topic that we are working on is blockchain governance and decision processes in completely decentralised organisations. One focus is on voting systems that reduce the risk of forks by favouring consensus over majority voting.

2.3.3 Other Topics

Among other topics, we plan to publish a paper on **standard blockchain transaction formats**. This is linked to work on user-defined transaction signatures, as well as to blockchain transactions signed by third parties.

3 Company Details

Sikoba Research Sàrl (`http://research.sikoba.com`) is a Luxembourg company incorporated in October 2018. It is a sister company of UK-based Sikoba Ltd (`http://www.sikoba.com`).

3.1 Tech Team

Aleksander (Alex) Kampa, Managing Director. ak@sikoba.com
Alex has been involved in blockchain projects since early 2015, with a focus on blockchain architecture, consensus models and smart contracts. As a researcher in monetary theory, his focus is on credit conversion. Alex also has extensive experience in financial software development. He studied engineering and economics at Ecole Centrale de Paris and holds an MS in statistics from Texas A&M. [LinkedIn]

Nimisha Walji, Operations Director, nw@sikoba.com
Nimisha is responsible for coordinating and overseeing all day-to-day activities of both Sikoba and Sikoba Research, including product development, research and marketing. She holds a MS in Computer Science from Bristol University and a PhD in Nanotechnology from Imperial College London.

Guillaume Drevon, CTO. gd@sikoba.com
Guillaume is focusing on applying secure computation and zero knowledge proofs to blockchain projects. Guillaume is an experienced software engineering manager, having led development teams in a wide range of technologies, from windows kernel to mobile applications and in various industries such as video games, satellite and transportation. He studied at Ecole Normale Supérieure (Ulm) in Paris, holds a MAS (DEA) in pure mathematics and was a lecturer in mathematics at Paris XII university for several years. [LinkedIn]

Dmitry Khovratovich, Cryptography Advisor. khovratovich@gmail.com
Dmitry is a prominent security researcher and cryptographer with [over 2800 citations]. His achievements include Argon2, winner of the Password Hashing Competition, and Equihash, which is a memory-hard Proof-of-Work used by Zcash and other blockchains. Dmitry is Principal Cryptographer at Evernym where he is working on the cryptographic engine behind the privacy-preserving Sovrin ledger. Dmitry holds a PhD in computer science from the University of Luxembourg. [LinkedIn]

Nemanja Borić, IT Advisor
Nemanja has led the development of the first version of isekai until the end of January 2019, and continues to provide support. He is a computer and electrical engineer from Serbia currently living in Berlin. Nemanja's main interests are in system programming, electronics and programming languages and their implementation. [stackoverflow]

3.2 Partners

Fantom Foundation

In October 2018, Fantom Foundation (`http://fantom.foundation`) agreed to support sikoba's research efforts until the end of 2020. The

areas of research will include trustless computing, consensus algorithms and token economics.

Manas.Tech

Manas.Tech (`http://manas.tech`) is our technology partner in charge of developing the sikoba platform. They also provide us with technical support for the Crystal language.

3.3 Technology

Crystal

We have chosen to use Crystal (`https://crystal-lang.org/`) as our main development language for isekai. Crystal is a high-level object-oriented language with a syntax similar to Ruby, but with an execution speed comparable to C.

Other languages

Our team has deep knowledge of C, C++, C# and Java. We also have expertise in Ruby and have worked on Solidity smart contract development.