



Slock.it UG Proposal #1

Overview/Educational purposes only—for actual terms
please refer to the Proposal Smart Contract on the Blockchain

DAO.Security

Creation Date: Thursday, 26th May 2016

Offered by:
DAO.LINK Sarl, Switzerland
in collaboration with
Slock.it UG (haftungsbeschränkt)
HRB 30026

Prepared for:
The DAO Address:
0xBB9bc244D798123fDe783fCc1C72d3Bb8C189413

About Us

Slock.it UG (Haftungsbeschränkt)

Slock.it is the world's trailblazer in creating blockchain infrastructures. Our technology connects the blockchain to the physical world, effectively giving connected objects an identity, the ability to receive payments and the capability to enter into complex agreements.

Slock.it aims to address security, identity, coordination and privacy over billions of devices. As part of the collaborative economy, it allows for any object to be rented, sold or shared securely—without middlemen. And in the field of machine to machine communications, it allows for direct, cost-effective payments between objects, as well as doing away with costly centralized servers outlay. Ultimately, this provides a better customer experience as all transactions take place instantly and without bureaucratic contracts.

Slock.it's technology also reduces its clients operating costs thanks to simplified billing while enabling fraud proof accounting. We help replace corporate data silos and fragile data workflows with secure coordination around a shared, immutable blockchain state.

In the corporate space, we help energy producers address decentralization or risk being disintermediated. We also work with forward-thinking automotive manufacturers that understand the importance of exploring the service industry, including operating autonomous fleets of self-driving taxis.

Slock.it is already collaborating with both startups and established companies and has a track record proving its capability to deliver on this Proposal.

Slock.it is headquartered in Berlin, Germany and works with clients globally.

Meet the Team

Our team has been around since the inception of the blockchain revolution, and with 60 years of combined IT expertise, we bring a pragmatic approach to building enterprise-grade solutions with this exciting technology.



Simon Jentsch
Founder & CEO



Christoph Jentsch
Founder & CTO



Stephan Tual
Founder & COO

Simon Jentsch, Founder and CEO: With prestigious clients including Siemens and Bahn AG, Simon has been deploying enterprise solutions for the last 20 years as Project Manager, Developer and Software Architect. Simon is now leading the development of the foundation Slock.it framework, enforcing Ethereum smart contracts into the physical world.

Christoph Jentsch, Founder and CTO: Christoph's background is in theoretical physics, where he developed optimized software solutions for high performance computing on specialized hardware. Christoph has been part of the Ethereum project since 2014 as Lead Tester, securing and shaping the core protocol while working on the backend of the C++ client.

Stephan Tual, Founder and COO: Previously CCO for the Ethereum project, Stephan has three startups under his belt and brings 20 years of enterprise IT experience to the Slock.it project. Before discovering the Blockchain, Stephan held CTO positions at leading data analytics companies in London with clients including VISA Europe and BP.



Lferis Karapetsas
Lead Technical Engineer



Colm Herbert
Security Engineer



Griff Green
Community Organizer



Dr. Gavin Wood
Advisor



Dr. Christian Reitwießner
Advisor

Lferis Karapetsas, Lead Technical Engineer: After graduating from the University of Tokyo, Lferis developed backend software for companies such as Oracle. He has been part of Ethereum as a C++ core developer since November 2014, having worked on Solidity, the ethash algorithm, the core client and the Continuous Integration (CI) system.

Colm Herbert, Security Engineer: Colm, who holds a BENG from Maynooth University and a MSc from UCD, joins us after working in application security a payment processing company. He is a longstanding member of our community and has been involved with the development of the DAO 1.0 Framework since January.

Griff Green, Community Organizer: Griff recently obtained his Master of Science degree in Digital Currency and is one of the first people in the world to have a degree in this rapidly evolving field. He has been traveling around the globe for the last several years promoting digital currencies especially in the US, Ecuador, and Indonesia.

Dr Gavin Wood: Advisor: Gavin wrote the first implementation of Ethereum and is the Inventor and Architect of web three (the decentralized web). Until very recently Gavin was CTO of Ethereum, and is now the Founder of Ethcore, a blockchain consultancy.

Dr Christian Reitwießner, Advisor: Christian is the main developer of the Ethereum smart contract programming language, Solidity. Since February 2016, Christian is also leading the development of the Ethereum Foundation C++ implementation.

Table of Contents

[About Us](#)

[Slock.it UG \(Haftungsbeschränkt\)](#)

[Meet the Team](#)

[Table of Contents](#)

[Important Disclaimer](#)

[Overview](#)

[What it includes](#)

[Projected costs](#)

[Volatility of Ether](#)

[Licensing](#)

[Risk Mitigation](#)

[Terms](#)

[Signature](#)

Important Disclaimer

The Proposal's smart contract is interpreted in plain English within this document solely for the convenience of prospective DAO Token Holders. This document is not intended to be binding nor to be interpreted as a legal contract: only by voting for the Proposal smart contract on the Ethereum blockchain will The DAO accept its terms, and the entirety of these terms will be defined in the form of Solidity code.

Overview

This short proposal describes the setting up of a security cell to continuously monitor, pre-empt and avert any potential attack vectors The DAO may face, including social, technical and economic attacks.

What it includes

Initially, we had in mind for DAO.Security to include all aspects of what constitute the 'security' of the DAO, including the establishment and management of a Bug Bounty Program and several 3rd party audits of the DAO code itself.

However, the response of the community was loud and clear: they didn't feel there was a need for such complex (and costly) set of mechanisms, and would probably prefer to eventually see a community-based security working group established rather than a crack team on call 24/7 outright. We agree.

That said, we still feel that with over 14% of all ether now held in The DAO's smart contract, it is important to give The DAO a formal, established form of security from the get go, and for this reason would recommend the deployment of a single, full time expert at the helm of this cell.

This person will act as first point of contact for security disclosures: Having an official first point of contact for the channeling of security concerns will help maintain a calm, level headed way of addressing such matters, while ensuring a swift, professional reaction.

He will continuously monitor, pre-empt and avert any potential attack vectors The DAO may face, including social, technical and economic attacks. He will also help the community with analysing major Proposals for attacks. This will include highlighting 51% attacks, mis-matched bytecode, and social engineering/collusion attacks.

We would hope that this Proposal will be renewed (and therefore renegotiated) yearly.

Projected costs

This engagement is for a single year (total of 366 days). The total cost is 8,000 ETH, disbursed on a monthly basis through the use of an Ethereum blockchain-backed smart contract proposal.

In the smart contract code (located at <https://github.com/slockit/smart-contract/blob/master/DAOSecurity.sol>), the `oneTimeCosts` (the initial deposit) is set at 1,595 ETH, while the `minDailyWithdrawLimit` (the daily withdrawal limit) - is set as 17.50 ETH. To minimize admin work, DAO.LINK will execute the withdrawal function on a month-to-month basis.

It is important to note that The DAO can retrieve any unspent ETH held in this Proposal smart contract by calling the `returnRemainingEther()` function, effectively 'firing' Slock.it UG and instantly removing all source of further funding. This ability aligns incentives and provides The DAO with adequate oversight on the project.

DAO Framework 1.1	Free of charge
The development of the DAO Framework 1.1, a 'stopgap' iteration to be released within weeks of signing the Proposal and addressing specific social attack - the technical list of these changes is detailed in the github issue repository for the DAO Framework and is limited to issue 165, 164, 163 and 148.	
Security Monitoring Cell, 1 Year	8,000 ETH
Deployment of 1 of our best security experts full time for the next year.	
TOTAL	8,000 ETH

Volatility of Ether

The potential volatility of Ether is undeniably a major concern for both our organization and the DAO Token Holders supporting this proposal.

It's a concern for the DAO Token Holder as the price of Ether could dramatically increase from the current valuation of USD 12 at the time this proposal was written. Of course, this would mean that the overall ETH reserve would also increase in value proportionally, but it understandably doesn't warrant for the DAO to 'overpay' for this project either.

It's a concern for our organization, and any Contractor going forward, as Ether can fluctuate widely but our outgoings for this project are fixed, and sometimes, in the case of our employees, fixed by law. Compounding this issue is that Ether can only be retrieved from the proposal up to a pre-agreed maximum (the `minDailyWithdrawLimit`). If Ether was to drop below 12 USD, this would potentially mean redundancy processes as part of our organization, and if it stayed at half that valuation for much longer than 3 months, potential bankruptcy, which would of course terminate the project.

As experts in the field, we have of course explored all potential avenues to mitigate this risk. We have studied oracles, stable coins, talking to banks, even BTC relay... unfortunately, while some of them look promising, none of these were deemed ready for the prime time and support a project of this magnitude.

A reasonable compromise that would satisfy both sides is the following: as the DAO is an Ethereum smart contract, all values will be denominated in ETH. Should the course of ETH fluctuate so much that it reaches sustained levels that could incapacitate either party, a new smart contract will be drafted and tested. Once an agreement has been reached on this new smart contract, the old one will be invalidated.

It's important to note that only the DAO can invalidate the smart contract, not the Contractor, giving it the upper hand in these negotiations.

Licensing

Slock.it UG will make all the code, smart contracts, user interfaces, applications, and everything forming the output of this Proposal free and open source under the MIT license.

Risk Mitigation

Every effort will be made to proactively identify risks ahead of time in order to implement a mitigation strategy from the project's onset. Our team will leverage a methodical process by which the various risks are identified, scored and ranked.

The most likely and highest impact risks were added to the project schedule to ensure that the assigned risk managers take the necessary steps to implement the mitigation response at the appropriate time during the schedule.

As part of our agile development methodology principles, Project Managers will provide status updates on their assigned risks in the daily stand-up meetings.

Terms

This document does not constitute a formal commercial Proposal and is provided "AS IS" and for educational purposes only. The terms located in the smart contract listed on the Ethereum blockchain supersede any undertaking, promise, assurance, statement, representation, warranty or understanding, including but not limited to any and all interpretations of this document.

Third Party Content may be made available directly to you by other companies or individuals under separate terms and conditions, including separate fees and charges. Because we may not have tested or screened the Third Party Content, your use of any Third Party Content is at your sole risk. We do not accept liability for any fees incurred or damages caused by your use of any Third Party Content. We do not guarantee the availability of any Third Party Content for any purpose. We do not guarantee the accuracy or precision of any information provided to us by any third party, including, without limitation, network information, pricing information or other statistical data. We may change, discontinue, or deprecate any of the Third Party Content.

WE AND OUR AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THIS DOCUMENT OR ANY THIRD PARTY CONTENT, INCLUDING ANY WARRANTY THAT THIS DOCUMENT WILL LEAD TO THE DEVELOPMENT OF PRODUCTS OR SERVICES.

IN ADDITION, WE AND OUR AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE THAT ANY PRODUCT OR SERVICES DELIVERED, IF ANY, WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR CONTENT OR THE THIRD PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED.

EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR AFFILIATES AND LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

Signature

This Proposal document purposely omits a signature section as it's provided solely as a convenient plain english interpretation of the smart contract located on the Ethereum blockchain.

All DAO Token Holders are invited to accept or reject the smart contract on the Ethereum blockchain before the expiry of the 14 calendar days debating period, starting from the time of the smart contract submission.

It is The DAO's responsibility to establish whether or not this Proposal document is an accurate representation of the aforementioned smart contract terms.