Smart-Toolbox

Smart-Toolbox für Community-Blockchains

Programm / Ausschreibung	Bridge, Bridge_NATS, Bridge_NATS 2018	**Status**	abgeschlossen
Projektstart	02.09.2019	**Projektende**	31.03.2023
Zeitraum	2019 - 2023	**Projektlaufzeit**	43 Monate
Keywords	Blockchain, Community-lockchain, Smart-Contract, Smart-Toolbox		

Projektbeschreibung

Der Begriff „Blockchain“ ist vor allem durch Anwendungen im Bereich Kryptowährungen bekannt geworden und hat in den letzten zwei Jahren rasant an Bekanntheit und Popularität gewonnen. Aufgrund dieser Popularisierung tendieren immer mehr Unternehmen dazu, die Vorteile replizierender, verteilter Peer-to-Peer-Systeme zu nutzen. Die grundlegende Eigenschaft der Blockchain ist die konsensuale Erstellung und Verwaltung von „Smart Contracts“, die das Verhalten von Blockchain-basierten Anwendungen festlegen.

Das von uns definierte Konzept „Community-Blockchain“ geht nun einen Schritt weiter. Das Projekt “Smart-Toolbox für Community-Blockchains” setzt dort an, wo derzeitige Blockchain-Systeme aufhören. Eine “Community” ist hier eine Gruppe von kooperierenden Personen, die in einer losen Verbindung stehen, beispielsweise MitarbeiterInnen verschiedener kooperierender Institutionen oder Firmen. Interaktion zwischen den Personen verlangt Konsens, Vertrauen und Vertraulichkeit.

Die “Smart-Toolbox” soll es Anwendungsentwicklern und –entwicklerinnen ermöglichen, Smart Contracts sehr leicht zu erstellen und deren Verhalten im verteilten System a priori zu überprüfen. Die “Smart-Toolbox” bietet dafür eine neue Pattern-Methodik an, die die Verifikation und Wiederverwendbarkeit von Smart Contracts vorsieht. Diese setzen auf ein vom Konsortialführer TU Wien entwickeltes Koordinations-Modell auf. Dieses hat die Besonderheit, Koordinations- und Applikationslogik konsequent zu trennen und damit beschreibbar und verifizierbar zu machen.

Das Projekt “Smart-Toolbox” wird es dem Verwertungspartner Österreichische Computer Gesellschaft (OCG) ermöglichen, folgende neue Services zunächst den Mitgliedern der OCG und später im Gesamtmarkt kommerziell anzubieten:

- Betrieb von “Community-Blockchains” basierend auf einer angepassten permissioned Blockchain-Infrastruktur mit austauschbaren Basis-Services. Beispiele für Basis-Services sind “Identity Provider Services” sowie “Store-and-Forward Services”, die zur Konsens-Bildung mit kleinem Quorum notwendig sind. Damit ist die Unabhängigkeit von Providern garantiert.

- Verifikation von Smart Contracts, die als Patterns formal spezifiziert werden. Das Verhalten von Smart Contracts kann mit Hilfe des Koordinations-Modells a priori beobachtet und evaluiert werden.

- Sicherheits-Überprüfungen / Monitoring von “Community-Blockchains”.

Die OCG will sich aufgrund des durch das Projekt gewonnenen Technologievorsprungs als der führende “Community-Blockchain-Service-Provider” profilieren und damit sowohl den OCG-Mitgliedern als auch der österreichischen Wirtschaft den Zugang zu innovativen Blockchain-basierten Community-Anwendungen erleichtern.

Abstract

The term "blockchain" has become known mainly through applications in the field of cryptocurrencies and has rapidly gained popularity in the last two years. With the popularization of blockchains, more and more businesses are looking for applications that take advantage of replicated, distributed peer-to-peer systems. The basic feature of Blockchain is the consensual creation and management of "Smart Contracts" that determine the behaviour of blockchain-based applications.

The concept "Community Blockchain", which we have defined, goes a step further. The "Smart-Toolbox for Community-Blockchains" project picks up where current blockchain systems are and builds on top of the current state of the art of permissioned blockchains. "Community" is a group of cooperating people who are loosely connected. Examples would be employees of various cooperating institutions or companies. Their interactions require consensus, trust and confidentiality.

The "Smart Toolbox" is intended to allow application developers to create Smart Contracts very easily and to check their behavior a priori in the distributed system. The Smart Toolbox offers a new pattern methodology that verifies and reuses Smart Contracts. These are based on a coordination model developed by the consortium leader TU Wien which has the peculiarity of consistently separating coordination and application logic and making it describable and verifiable.

The project "Smart Toolbox" will enable the company partner Österreichische Computer Gesellschaft (OCG) to offer the following new services commercially to the members of the OCG and later in the overall market:

- Running community blockchains based on a customized permissioned blockchain infrastructure with interchangeable base services. Examples of base services are Identity Provider Services and Store-and-Forward Services, which are necessary for small quorum consensus building. This guarantees independence from providers.

- Verification of smart contracts that are formally specified as patterns. The behavior of smart contracts can be monitored and evaluated a priori using the coordination model.

- Security checks / monitoring of Community Blockchains.

The OCG wants to make a name for itself as the leading "community block chain service provider" due to the technological advantage gained by the project, thus facilitating access to innovative blockchain-based community applications for OCG members as well as the Austrian economy.

Projektkoordinator

- Technische Universität Wien

Projektpartner

- Österreichische Computer Gesellschaft (OCG)