Smart Contracts - Approved on Jan 31 2019

Introduction

Smart contracts provide automation in blockchain solutions. They are immutable, decentralized and deterministic, which make them ideal to remote third-parties and let peer-to-peer interactions. Once agreed between the parties and deployed on a distributed ledger, their activities and outcomes can be verified, so they can be trusted by all stakeholders. Everybody involved in DLTs are interested in smart contracts and the benefits they bring, but are also worried because there are many aspects about smart contracts they don't understand including legal and ethical insecurities. The main goal of this workgroup will be to give an academic perspective to this research topic and in parallel make clear to users, developers, researchers, businessmen, decision makers and others interested in smart contracts practical ways to utilize them on the different DLTs that are under the Hyperledger umbrella and explore all potentials from deploying them in everyday software solution scenarios.

Scope

The scope is to define concepts regarding smart contracts and to produce material to describe the various aspects and meanings, trying to come up to standards or good practices. The audience for smart contracts is large and spans from researchers, developers, businessmen, decision makers, policy makers, law makers, software users, citizens to governments, banks, financial institutions, insurance providers, etc

Some research topics and separation of interest are:

- □ Models of and mechanism for computation, such as:

  - Stack machines vs automata vs manipulating algebraic types embedded in a another language

  - Scope for less expressive languages (that may have more tractability for formal methods)

  - Execution determinism, and sources of non-determinism in existing languages

  - Cost models for metering computation (e.g. gas)

  - Paradigms for smart contracts - e.g. 'identity-oriented', functional, process-oriented - extent to which smart contracts benefit from special purpose languages

  - Parallelism of execution, state independence (i.e. parallel processing in a single block)

- □ Formal guarantees on outputs of smart contracts
- □ Smart contract packaging, code reuse, and dependency auditing
- □ Smart contracts as representatives of obligations and fulfillment (i.e. 'law')

  - What properties should smart contracts with 'legal charge' have?

  - What relations can smart contracts have with actual contracts and agreements?

  - At what scale to smart contracts best contribute to certainty and execution of agreement?

  - What relationship do legal smart contracts have to models of computation?

- □ Generation of smart contracts from existing artifacts (natural language, business process, state machines, non smart-contract code)
- □ Data structures and state

  - Verifiable and authenticated data structures - e.g. Merkle dags, log-backed maps,

  - How best to expose through smart contract languages/libraries

  - Sharing state back-ends across execution engines

  - Conflict-free and additive data structures

- □ Privacy

  - Multi-party secure computation

  - Differential privacy

  - Zero knowledge and practical building blocks - types of commitments and witnesses

- □ Tooling and compilers for existing virtual machines

  - WASM/eWASM

  - EVM

- WebIDL

□ Design Patterns for Smart Contracts

Work Products

The anticipated initial work products will include (but is not limited to):

- White Paper about smart contracts and the respected aspects concerning their development, deployment and usage
- Taxonomy of smart contracts
- Find practical ways to connect stuff 'out there' with things we could use within implementations
- Performance of smart contracts across the different HL DLT frameworks
- Identifying use cases, case studies
- Survey and continuously keep a record for the state of the art and academic content
- Produce 'Requests To Build' that could feed into feature planning on the different Hyperledger frameworks
- Exploring security, privacy, legal boundaries
- Proposing solutions to the problems identified
- Identifying conferences or other opportunities to connect face to face

Collaborators (other groups)

This working group will collaborate with other Hyperledger working groups, the TSC, Linux Foundation staff, and the project maintainers. Especially the following Working Groups and their subgroups will be of great importance in achieving the anticipated results.

Workgroups

- Architecture Working Group
- Identity Working Group
- Performance and Scale Working Group
- Whitepaper Working Group

SIGs

- Healthcare SIG
- Public Sector SIG
- Social Impact SIG
- Trade Finance SIG

Interested Parties

The following individuals have already expressed an interest in joining this working group, and we hope they will become contributors over the first year:

Name	Company	Email Address
Sofia Terzi	CERTH-ITI	sterzi@iti.gr
Silas Davis	Monax	silas@monax.io
Sean Young	Monax	sean.young@monax.io
Dan Selman	Accord	dan@clause.io
Vipin Bharathan	dlt.nyc	vipinsun@gmail.com
Mohan Venkataraman	Chainyard	mohan.venkataraman@chainyard.com
Prasanna Badmanabhan	Pichain LTD	prasanna@pichainlabs.com
Srinivasan (Murali) Muralidharan	State Street	srinivasan.muralidharan99@gmail.com
Sumabala Nair	IBM	sumapnair@us.ibm.com
John Carpenter	Global Blockchain Summit	john@globalblockchainsummit.com
Bobbi Muscara	Ledger Academy	Bobbi@LedgerAcademy.com
Mic Bowman	Intel	

Proposed Chair

The following individual has volunteered to serve as the initial chair for the working group:

I Sofia Terzi am volunteering to run this group initially, unless somebody else with interest in the group volunteers.