From contracts to “smart” contracts

Massimo Bartoletti
University of Cagliari

Roberto Zunino
University of Trento
From contracts to “smart” contracts

Idea: a contract is a behavioural property of a service.

Service composition only possible after verifying (statically) that services respect their contracts.

Secure service orchestration (Bartoletti, Zunino, Degano, Ferrari)
Secure service orchestration (Bartoletti, Zunino, Degano, Ferrari)

Idea: a **contract** is a behavioural property of a service.

Service composition only possible after verifying (statically) that services respect their contracts.

Problem: **dishonest** services can change their code.
From contracts to “smart” contracts

Contract-oriented programming (Bartoletti, Zunino)

Idea: a **contract** is a behavioural property of a service. Contract violations are sanctioned.

Before publishing a service, one can statically verify that it respects the declared contracts (so to avoid sanctions)
From contracts to “smart” contracts

Toolchain for contract-oriented programming:
- Automatic verification for honesty
- Call-by-contract
- Middleware to monitor contract violations
- Automatic sanctions...

Contract-oriented middleware (Bartoletti, Cimoli, ...)
From contracts to “smart” contracts

Toolchain for contract-oriented programming:
- Automatic verification for honesty
- Call-by-contract
- Middleware to monitor contract violations
- Automatic sanctions...

Problem: centralization

Contract-oriented middleware (Bartoletti, Cimoli, ...)

2006 2010 2015 2016 2017 2018
From contracts to “smart” contracts

- Disintermediation: no central authority
- Contract code is the law - it cannot be changed
- Contracts can transfer currency
From contracts to “smart” contracts

A survey of attacks on Ethereum smart contracts (Atzei, Bartoletti, Cimoli)

Dissecting Ponzi schemes on Ethereum (Bartoletti, Cimoli, ...)

An empirical analysis of smart contracts (Bartoletti, Pompianu)

10.2016
03.2017
From contracts to “smart” contracts

A survey of attacks on Ethereum smart contracts (Atzei, Bartoletti, Cimoli)

Dissecting Ponzi schemes on Ethereum (Bartoletti, Cimoli, ...)

An empirical analysis of smart contracts (Bartoletti, Pompianu)
From contracts to “smart” contracts

A survey of attacks on Ethereum smart contracts (Atzei, Bartoletti, Cimoli)

Dissecting Ponzi schemes on Ethereum (Bartoletti, Cimoli, ...)

An empirical analysis of smart contracts (Bartoletti, Pompianu)

10.2016

03.2017
From contracts to “smart” contracts

- A survey of attacks on Ethereum smart contracts (Atzei, Bartoletti, Cimoli)
- Dissecting Ponzi schemes on Ethereum (Bartoletti, Cimoli, ...)
- An empirical analysis of smart contracts (Bartoletti, Pompianu)

10.2016 03.2017
From contracts to “smart” contracts

A survey of attacks on Ethereum smart contracts (Atzei, Bartoletti, Cimoli)

Dissecting Ponzi schemes on Ethereum (Bartoletti, Cimoli, ...)

An empirical analysis of smart contracts (Bartoletti, Pompianu)

10.2016

Problem: writing secure smart contracts with Ethereum is very **difficult**.
- Turing-equivalent language, with unfortunate design choices
- No (usable) formal models of smart contracts and of their security

03.2017
From contracts to “smart” contracts

Constant-deposit multiparty lotteries on Bitcoin (Bartoletti, Zunino)
From contracts to “smart” contracts

Constant-deposit multiparty lotteries on Bitcoin (Bartoletti, Zunino)

Smart contracts use advanced Bitcoin features
- poorly documented (obsolete sites)
- only trustworthy documentation is the code
- too low-level!

Need for formal models
From contracts to “smart” contracts

- Constant-deposit multiparty lotteries on Bitcoin (Bartoletti, Zunino)
- A formal formal of Bitcoin transactions (Atzei, Bartoletti, Lande, Zunino)

From contracts to “smart” contracts

- Constant-deposit multiparty lotteries on Bitcoin (Bartoletti, Zunino)
- A formal formal of Bitcoin transactions (Atzei, Bartoletti, Lande, Zunino)
- SoK: unraveling Bitcoin smart contracts (Atzei, Bartoletti, Cimoli, Lande, Zunino)
From contracts to “smart” contracts

- Constant-deposit multiparty lotteries on Bitcoin (Bartoletti, Zunino)
- A formal formal of Bitcoin transactions (Atzei, Bartoletti, Lande, Zunino)
- SoK: unraveling Bitcoin smart contracts (Atzei, Bartoletti, Cimoli, Lande, Zunino)
- BitML (Bartoletti, Zunino)
Other blockchain research

blockchain.unica.it

Scientific School on Blockchain Technologies, Pula (CA), 12-15 June, 2018