UNIVERSITY of STIRLING

On smart contracts' security

towards safe computation and robust governance

Andrea Bracciali
abracciali@gmail.com

.: CifrisChain 2019:. **.:CONSOB:.** Roma, 9 May 19

Smart contract

Self-enforceable agreements

Smart contracts … formalize and secure relationships over computer networks. … are derived firm legal principles, economic theory, and theories of reliable and secure protocols. … By using cryptographic … , we can secure many algorithmically specifiable relationships…

… robust against sophisticated, incentive compatible (rational) breach

… any algorithmic intermediary can in principle be replaced by a trustworthy virtual computer.

[Nick Szabo 97]

Smart contract

Self-enforceable agreements

Smart contracts … formalize and secure relationships over computer networks. … are derived firm legal principles, economic theory, and theories of reliable and secure protocols. … By using cryptographic … , we can secure many algorithmically specifiable relationships…

… robust against sophisticated, incentive compatible (rational) breach

… any algorithmic intermediary can in principle be replaced by a trustworthy virtual computer.

[Nick Szabo 97]

Smart contract

Self-enforceable agreements

Smart contracts … formalize and secure relationships over computer networks. … are derived firm legal principles, economic theory, and theories of reliable and secure protocols. … By using cryptographic … , we can secure many algorithmically specifiable relationships…

… robust against sophisticated, incentive compatible (rational) breach

… any algorithmic intermediary can in principle be replaced by a trustworthy virtual computer.

[Nick Szabo 97]

Smart contract

Self-enforceable agreements

Smart contracts … formalize and secure relationships over computer networks. … are derived firm legal principles, economic theory, and theories of reliable and secure protocols. … By using cryptographic … , we can secure many algorithmically specifiable relationships…

… robust against sophisticated, incentive compatible (rational) breach

… any algorithmic intermediary can in principle be replaced by a trustworthy virtual computer.

[Nick Szabo 97]

Smart contract

Self-enforceable agreements

Smart contracts … formalize and secure relationships over computer networks. … are derived firm legal principles, economic theory, and theories of reliable and secure protocols. … By using cryptographic … , we can secure many algorithmically specifiable relationships…

… robust against sophisticated, incentive compatible (rational) breach

… any algorithmic intermediary can in principle be replaced by a trustworthy virtual computer.

[Nick Szabo 97]

Smart contract

Self-enforceable agreements

Smart contracts … formalize and secure relationships over computer networks. … are derived firm legal principles, economic theory, and theories of reliable and secure protocols. … By using cryptographic … , we can secure many algorithmically specifiable relationships…

… robust against sophisticated, incentive compatible (rational) breach

… any algorithmic intermediary can in principle be replaced by a trustworthy virtual computer.

[Nick Szabo 97]

Smart contract

Self-enforceable agreements

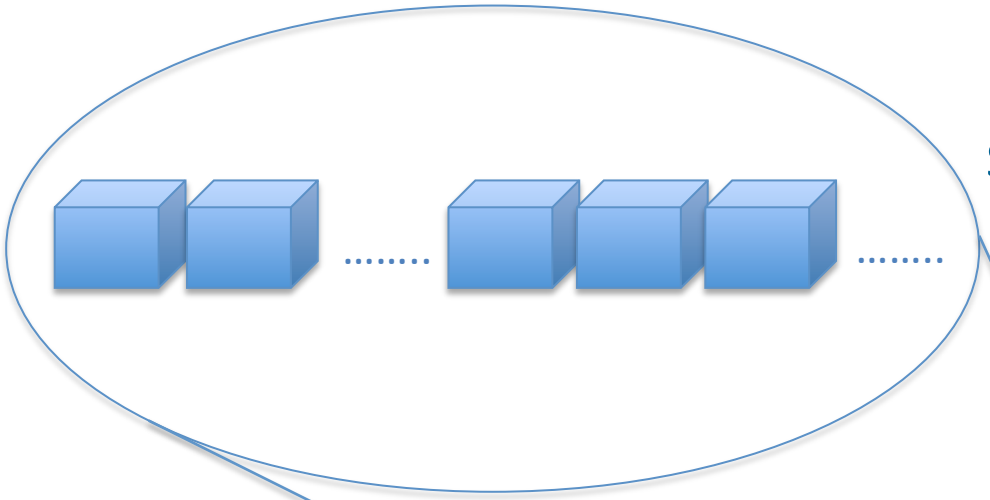
Smart contracts … formalize and secure relationships over computer networks. … are derived firm legal principles, economic theory, and theories of reliable and secure protocols. … By using cryptographic … , we can secure many algorithmically specifiable relationships…

… robust against sophisticated, incentive compatible (rational) breach

… any algorithmic intermediary can in principle be replaced by a trustworthy virtual computer.

[Nick Szabo 97]

Blockchain: a system of trust



Single source of truth

Inalterable data structure

Decentralised: no dominant position

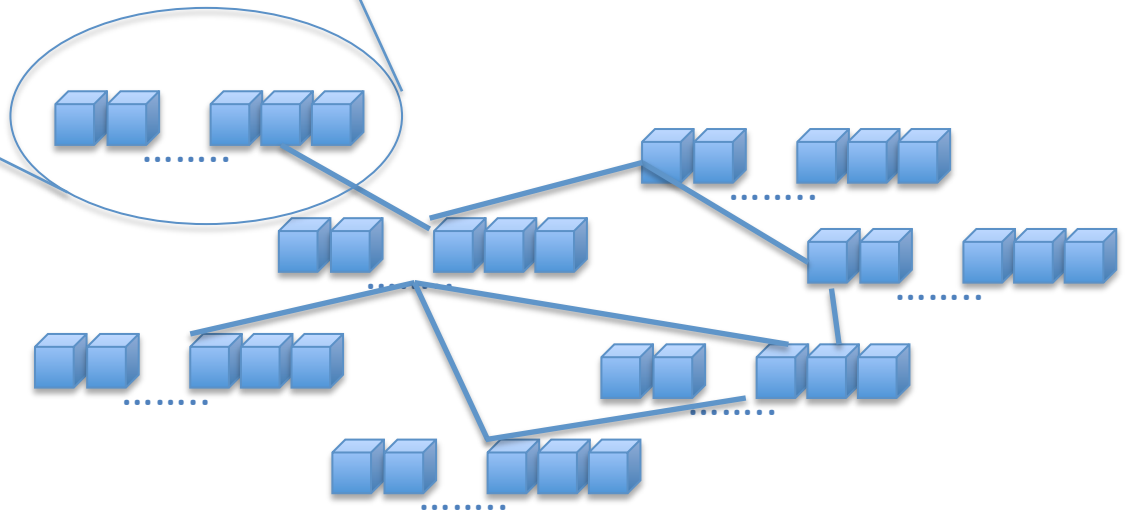
Cryptography protected,

incentivized,

consensus-based,

P2P distributed system

(with crypto-currency)



Bitcoin transactions

0f2d0b6725441fa93565190d60b6e267bd10823991dde83557e50ead034da44d

1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP (44.79421602 BTC - Output)	→	16iRbSf3jxQ9yNkWpjTS8qXERd266932GS - (Unspent)	1.2995 BTC
		1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP - (Unspent)	43.48871602 BTC

Coins from/to multiple addresses.

DUP HASH160 PUSHDATA(20)[3eae3697975ae35c475e52307f26b8db0d554dcb] EQUALVERIFY CHECKSIG

DUP HASH160 PUSHDATA(20)[b08f46e4d21cd0547a8a1e2e43e5440284f710a4] EQUALVERIFY CHECKSIG

A program validates the rights over value.

Decentralised governance.

No intermediaries.

Bitcoin transactions

DUP HASH160 PUSHDATA(20)[b08f46e4d21cd0547a8a1e2e43e5440284f710a4] EQUALVERIFY CHECKSIG

An extremely simple program – not even multiplications (!)

- executed by nodes when validating transactions, i.e.

on-chain, under consensus, within the perimeter of trust

- always possible to decide whether the “contract” is “correct”
- no exploitation of nodes (DoS attacks)
- basically no attacks (to the bitcoin protocol) so far.

Bitcoin smart contracts

Still some forms of contract are possible!

EXAMPLE (other examples exist): A buys an item from B for 1 BTC. No trust relationship between A and B, but both A and B trust C.

A (1 BTC) ➡ Z 2out3[A, B, C] (1 BTC)

2out3[A,B,C] requires 2 correct keys out of 3 to redeem 1 BTC from Z

1. A pays 1 BTC to a deposit Z.
2. A and B in agreement: they provide their keys to transfer 1 BTC to B, otherwise
3. C makes a decision and signs together with A or B, accordingly.

   1 BTC is transferred to either A or B according to C's decision

Decentralised computing

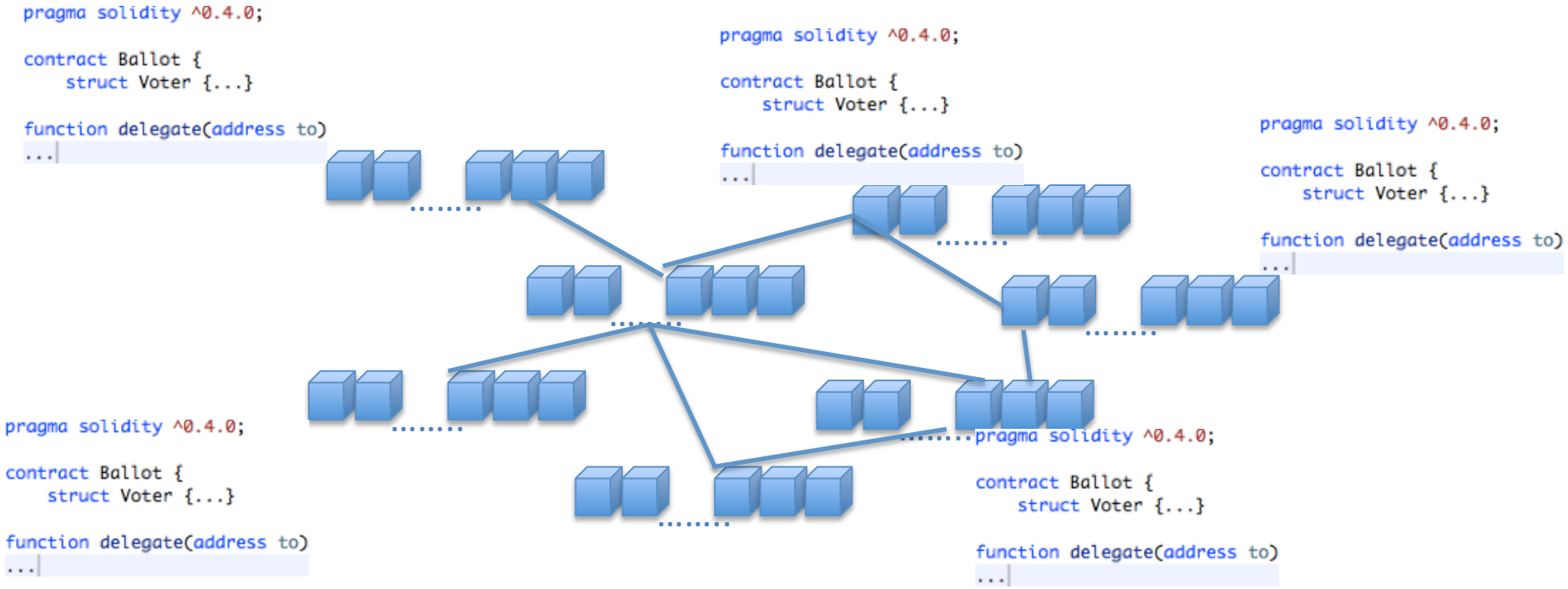
www.ethereum.org

ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER
EIP-150 REVISION

DR. GAVIN WOOD
FOUNDER, ETHEREUM & ETHCORE
GAVIN@ETHCORE.IO

Building unstoppable applications!

Radically different computation model (affecting security)



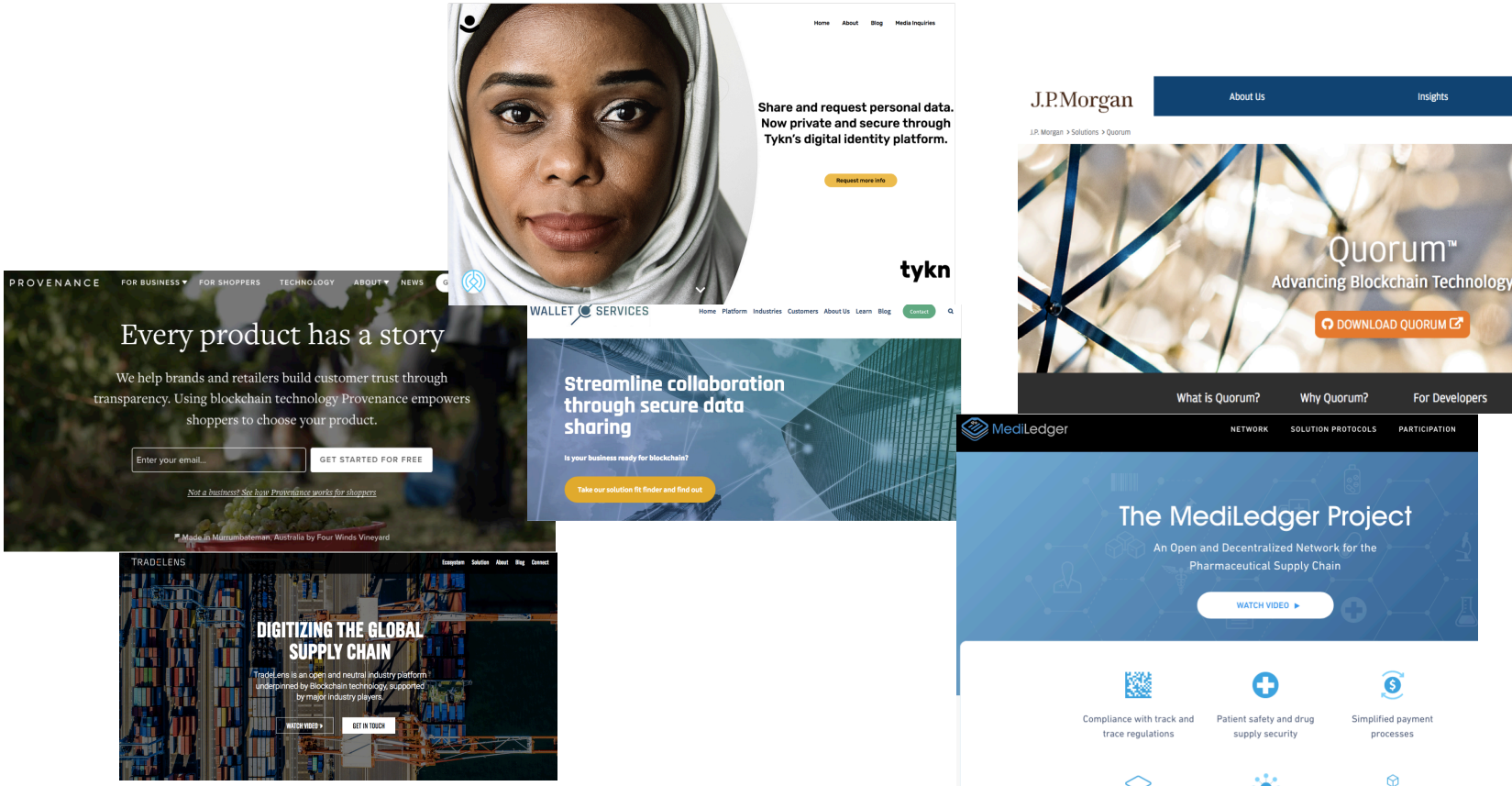
Decentralised computing

- Smart contracts are deployed on the blockchain.
- Each node executes the same program, updating the replicated state.
  Execution has a cost and is limited (*gas* to run it).
- Have an owner, can be activated and deactivated, but not changed.
  Errors can not be corrected.*
- Their immutability* is part of their trusted status -- they manage value!
- Functionalities can be invoked (as transactions) and data/information injected
  … untrusted*, from outside the consensus

Smart contracts

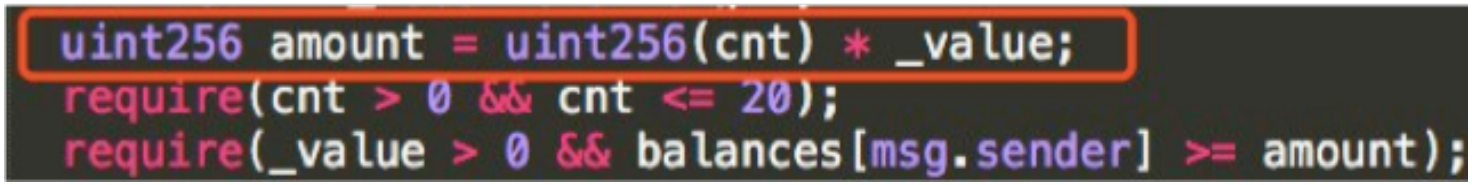
Huge hype, disintermediation, market efficiency in

identity, supply chain, democracy, finance, health… (non exhaustive examples)



www.provenance.org tykn.tech www.tradelens.com/wallet.services www.jpmorganchina.com.cn/country/CN/EN/Quorum https://www.medileger.com/

Issues – programming level

- 
```
uint256 amount = uint256(cnt) * _value;
require(cnt > 0 && cnt <= 20);
require(_value > 0 && balances[msg.sender] >= amount);
```

code revised (migration to the new code)

- PARITY WALLET ATTACK 30M USD (2017)

  similar code/language level issue:

  - the program was not suitably protecting the identity of the owner
  - mismanagement of the source code (human/engineering aspects)

  migration to corrected wallets (whenever possible)

Issues – governance level

- THE DAO ATTACK 70M USD (2016)

  Major success story in smart contracts (initially)

  Up to 170M USD crowd funding smart contract

  "Legally" draining crypto-money by exploiting the program exposed features and language weaknesses.

Huge debate: IS THE CONTRACT LAW (WHERE IS THE TRUST)?

IT CAN BE LAW BECAUSE UNTAMPERABLE!

Led to COMMUNITY MAJORITY DECISION of rewriting history,

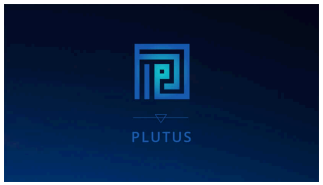
i.e. abandoning part of the chain, and

SPLIT OF THE COMMUNITY in Ethereum and Ethereum Classic

Solutions – programming level

Current trends -- _some examples_ underdev (in no order!):

- Smart-contract secure (by construction) languages and tools …
  - cardano's Plutus,
  - BALZaC, …



A formal model of Bitcoin transactions

Nicola Atzei[1], Massimo Bartoletti[1], Stefano Lande[1], Roberto Zunino[2]

[1] Università degli Studi di Cagliari, Cagliari, Italy
[2] Università degli Studi di Trento, Trento, Italy

- Verification frameworks …
  - ~ 1M contracts analysed
  - Fully automated analysis

Finding The Greedy, Prodigal, and Suicidal Contracts at Scale

Ivica Nikolić
School of Computing, NUS
Singapore

Aashish Kolluri
School of Computing, NUS
Singapore

Ilya Sergey
University College London
United Kingdom

Prateek Saxena
School of Computing, NUS
Singapore

Aquinas Hobor
Yale-NUS College and School of Computing, NUS
Singapore

CERTORA

- towards … as secure as centralised technologies,
  - e.g. credit card

https://iohk.io/blog/smart-contracts-language-for-cardano-launches-at-plutusfest/ www.certora.com

Governance/Decentralisation

Why your BTC will be there in 50 years?

Who is in charge?

- Coders
  - maintain the infrastructure, make decisions, take emergency actions …
- Consensus
  - under-development
  - multidisciplinary models,
  - incentives, game theory, economics, cryptoeconomics
  - "Incentives are the hardest thing to do" [Micali]

https://www.coindesk.com/no-incentive-algorand-blockchain-sparks-debate-cryptography-event

Governance/Decentralisation

Why your BTC will be there in 50 years?

Who is in charge?

- Nodes / Users
  - adoption
- "Owners" - foundations
  - seed funding, ICOs, …
  - manage and support development and bootstrap
  - adopt a _decentralised_ governance …
  - Tezos: … subject to consensus (as a transaction)
  - CAVEAT: owners as in permissioned blockchains not discussed here

Tezos Foundation

CARDANO FOUNDATION

FOUNDATION

quadrans FOUNDATION

Governance/Decentralisation

Why your BTC will be there in 50 years?

Who is in charge?

Can the technology alone be in charge?

Does a smart contract require/support a jurisdiction?

- Incomplete Contracts
  - contracts cannot specify what is to be done in every possible contingency [Grossman, Hart, Moore 85-95]

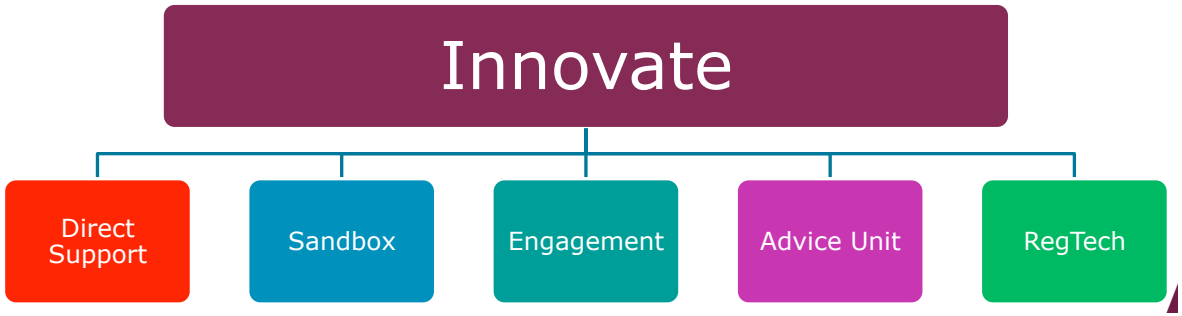
- Ricardian Contracts
  - a legal agreement in a format that can be expressed and executed in software [Grigg 96]

Innovation: current approaches (examples)

- UK – FCA

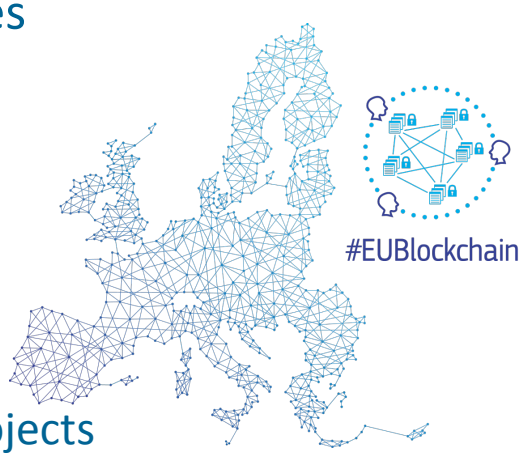
  Innovate (fintech)

  16B USD S1-2018



- Spain – ALASTRIA

- EUROPE – Digital Single Market :: Blockchain Technologies
  - European Blockchain Partnership
  - EU Blockchain Observatory and Forum
  - International Association for Trusted Blockchain Applications (INATBA)
  - Horizon Prize on Blockchains for Social Good
  - H2020 Blockchain and distributed ledger technologies projects



www.fca.org.uk alastria.io/ https://ec.europa.eu/digital-single-market/en/blockchain-technologies

Smart contracts' security

Summary

- Innovative trust framework
- New context – new multidisciplinary theories
- Disruptive innovation
- Security of smart contracts in progress (to be nurtured!)
  - Programming: at hand, but requires efforts
  - Governance/decentralisation: require efforts, lots of interest, exciting moment!
- International dimension/space for cooperation

Andrea Bracciali

abracciali@gmail.com