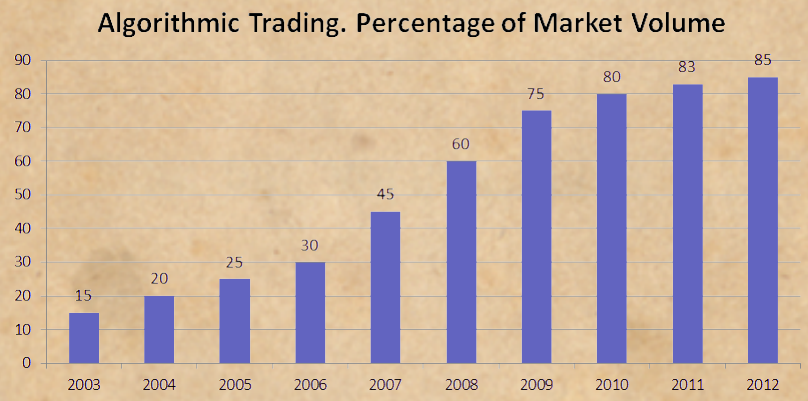
Introduction

The technologies behind blockchains such as Bitcoin or Ethereum suffer from many limitations. The lack of confidentiality and privacy guarantees in current blockchains is hindering their adoption, particularly in banks and big companies: in a recent survey to 134 global market participants working on blockchain technology[Ass16], 64% of banks and brokers said that transaction confidentiality was a significant concern with blockchain technology and 52% was worried about the security of private keys. And likewise, the lack of private smart contracts is a limiting factor to their universal adoption: only a very limited subset of all the possible smart contracts are being developed and executed, only those for which leaking all the input data, program execution and results is tolerable. Additionally, the concern of governments and regulators are not being met: there is no way to enforce regulations and no one can differentiate between criminal and law-abiding smart contracts. As a consequence of all the aforementioned problems, 10% of ICO funding gets stolen[Cha17] with the average financial loss incurred increasing by 20% annually and software bugs are being exploited with very high losses ($150 MM, Parity wallet[Tec17]).

Algorithmic/program trading keeps growing in other financial technologies not including blockchains: many trades on traditional exchanges are already done by computer programs[GK13], not human traders (more in equities, but also in FX/derivatives and catching up in bond markets). It's expected that a major part of this trading migrates to blockchains, but this transition will only can occur after confidentiality and privacy issues are fully resolved.



The Raziel project uses cutting-edge cryptographic and verifiability technologies to solve all the above-mentioned problems, providing stronger property rights over intangible intellectual property in order to ease adoption of blockchains and increase their profitability.

Market Need

The interests of all the involved stakeholders are being met:

Regulation-aware: in the crypto-currency space, the needs of governments and regulators are being overlooked much to the detriment of their widespread adoption in public and private settings. In order to further advance and promote these technologies to the grand public, it should be possible that laws and regulations could be coded on smart contracts in order to enhance public trust and commerce.

Verifiable Smart Contracts: executing smart contracts from unknown parties implies tacitly accepting considerable risks. By annotating the code of the smart contracts with proofs and providing said proofs before execution, said risks could be removed. Additionally, third parties (regulators, NGOs, private companies) could provide specifications against which said smart contracts must be proven secure.

For more detailed explanations, see sections 5 and 7.4 of the research paper[CS17b].

Stronger property rights over intangible intellectual property. The use of the latest secure computation techniques allows treating data confidentially while keeping the intellectual property rights of the owner/producer in multiple executions. In a financial context, this could be applied to financial series and investment strategies: the producer could rent access to private data to third parties without these parties learning anything about it. Ultimately, fully encrypted smart contracts could be exchanged without revealing anything about the data contained within them to third parties: *de facto*, new types of property rights are being created.

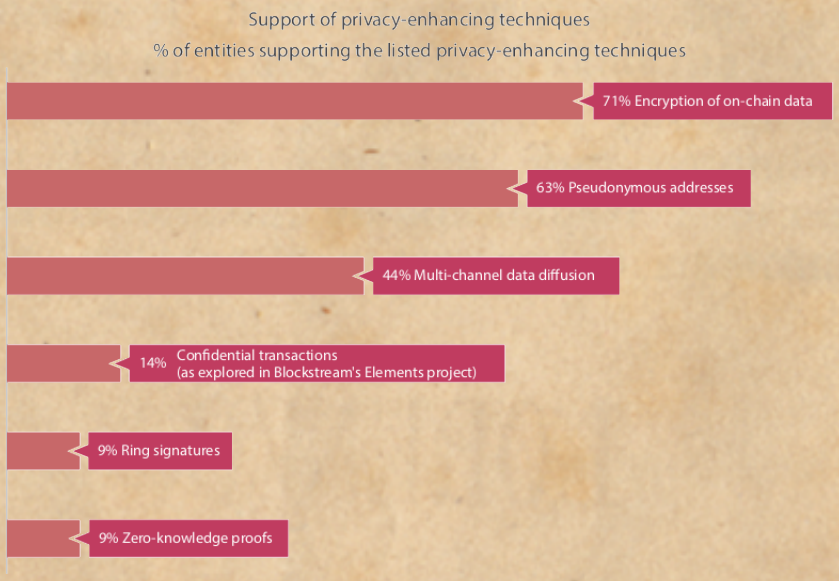
Different types of encrypted smart contracts will be considered:

- protecting only the inputs of the different parties, but the program and the outputs being public
- additionally, only releasing the output to a subset of the parties, others being unable to learn the output
- additionally, protecting the code of the smart contract from malicious third parties
- smart contract securely stored on disk/cloud and transferable between different exchanges/blockchains: interoperability is a key feature to guarantee mass adoption between heteregeneous systems

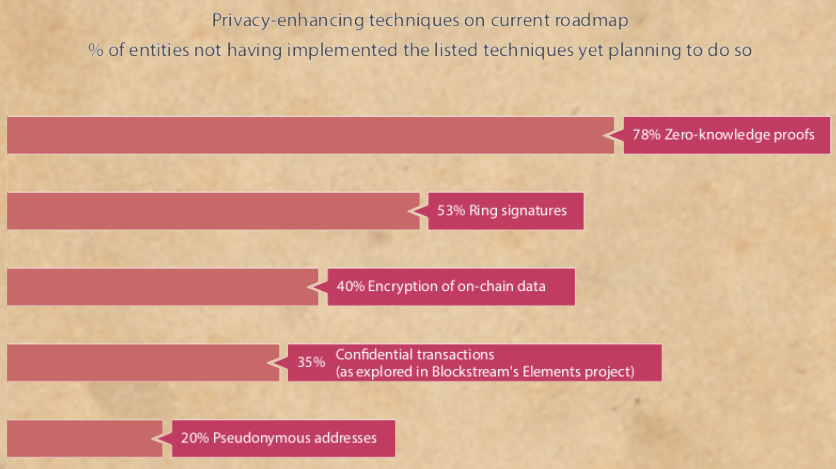
For more detailed explanations, see sections 4, 7.1 and 7.5 of the research paper[CS17b].

Privacy-Enhancing Technologies

The following figure shows the current support of privacy-enhancing technologies[HR17] being adopted in blockchains:



And the next figure shows the future support of privacy-enhancing technologies[HR17]:



Note that secure computation techniques are yet to be developed and the zero-knowledge proofs only protect the privacy of the transactions, and not the code executed within smart contracts: actually, they are pre-requisites for all future decentralized software architectures.

Encrypted Algorithmic Trading

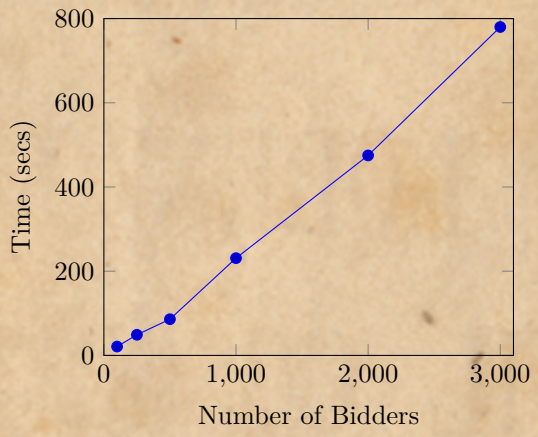
Tracing the execution of any smart contract, including public input and output parameters, is a well-known privacy leakage of current permissionless blockchains. Consider the following example:

These execution traces violate privacy regulations: the "Right to Be Forgotten", the principles of "Privacy by Design" and "Privacy by Default" included on the new European General Data Protection Regulation[PC16]; and the "Financial Privacy Rule" of the Gramm-Leach-Bliley Act[Con99]. Even worse, only a tiny percentage of all the possible smart contracts are being deployed on permissionless blockchains because it's economically irrational to expose so much confidential information: consequently, the crypto-currency space is being held back due to the lack of essential privacy protections. To reach the same level of algorithmic/program trading observed in public exchanges, it will be indispensable to adopt the most efficient secure computation techniques available.

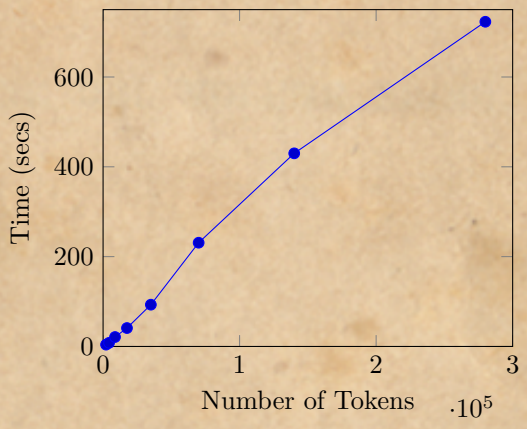
Publications and Patents

The contents of the following publications and patents are incorporated herein by way of reference. Two research publications have been published:

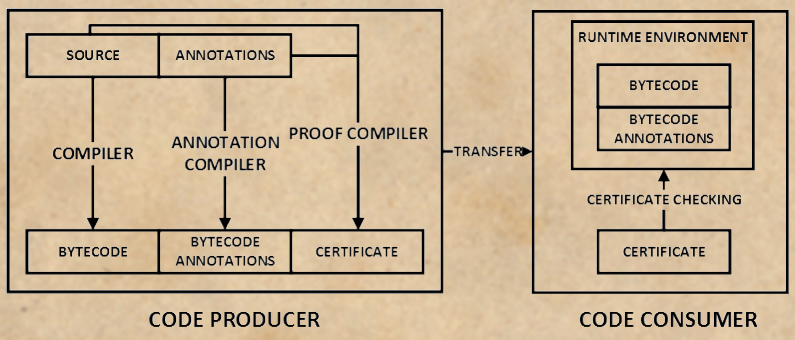
"**An Optimal ICO Mechanism**"[CS17a]: Initial Coin Offerings are raising billions in funding using multiple strategies, none justified from the point of view of mechanism design, resulting in severe underpricing and high volatility. In the present paper, an optimal ICO mechanism is proposed for the first time: a truthful multi-unit Vickrey-Dutch auction of callable tokens (i.e., a new hybrid security of tokens packaged with callable warrants). Truthful bidding is an ex-post Nash equilibrium strategy and the auction terminates with an ex-post efficient allocation; additionally, the callability of the warrants eliminates the winners curse of the auction and its underpricing. An implementation demonstrates its practical viability.

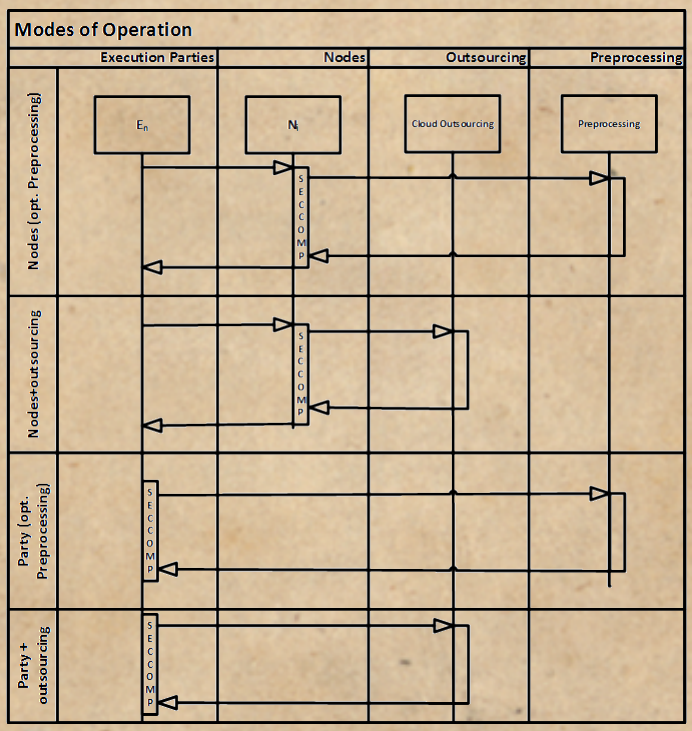


Additionally, the next figure shows another timing experiment, this time varying the number of tokens to be auctioned while maintaining fixed the number of bidders (1000) and the final price (2).



- **Raziel: Private and Verifiable Smart Contracts on Blockchains**: Raziel[CS17b] combines secure multi-party computation and proof-carrying code to provide privacy, correctness and verifiability guarantees for smart contracts on blockchains. Effectively solving DAO and Gyges attacks, this paper describes an implementation and presents examples to demonstrate its practical viability (e.g., private and verifiable crowdfundings and investment funds). Additionally, we show how to use Zero-Knowledge Proofs of Proofs (i.e., Proof-Carrying Code certificates) to prove the validity of smart contracts to third parties before their execution without revealing anything else. Finally, we show how miners could get rewarded for generating pre-processing data for secure multi-party computation.

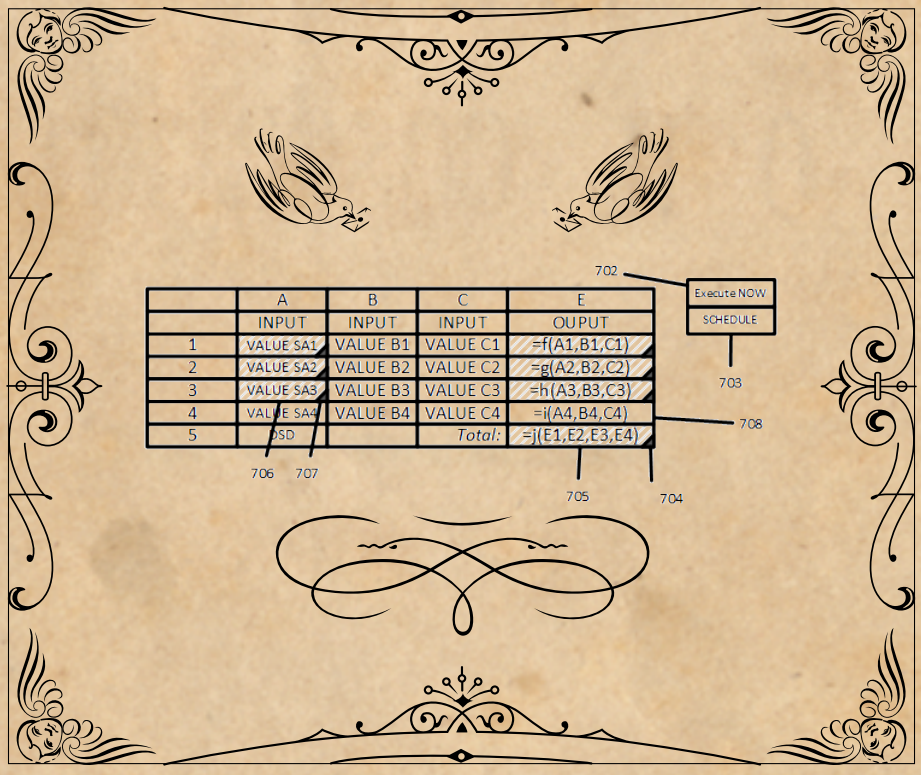


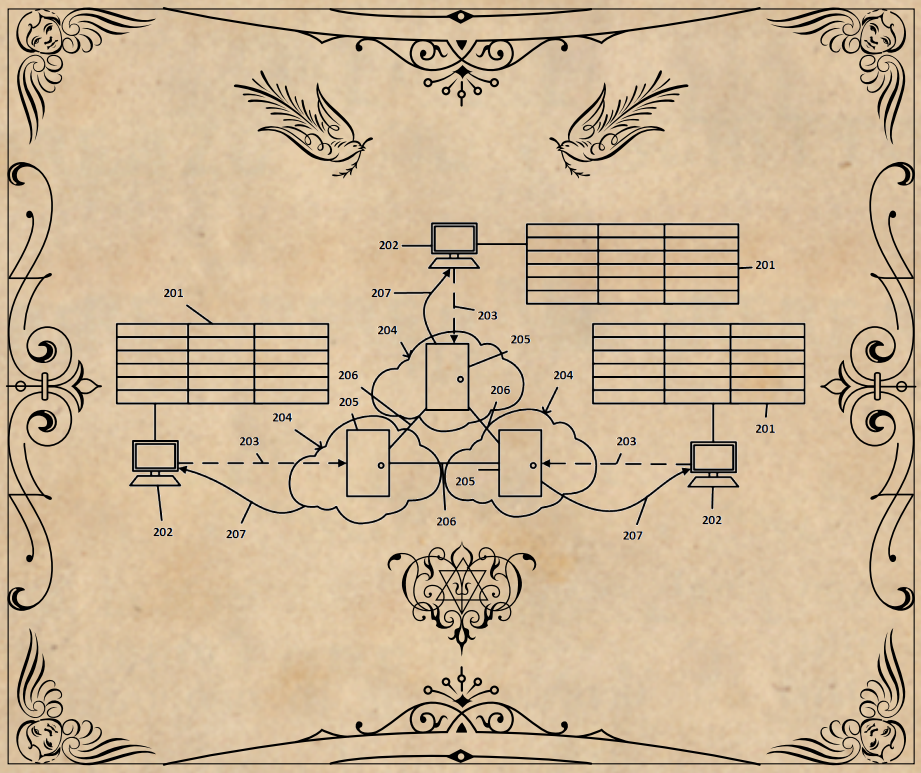


Two patents have been filed:

"**Secure Computation on Spreadsheets**"[CS14]: Systems, computer-readable media and methods for enabling secure computation on spreadsheet software. A secure spreadsheet is implemented as an add-in to an existing spreadsheet program, or as a new spreadsheet program/web application, to allow secure computations on private input data (and also optionally with private functions) without the parties learning anything about them, via the familiar spreadsheet interface and its formula language. Automatic conversion of previous spreadsheet data and formulas is provided whenever possible, or assisted via a helper. The secure computation can be executed between the computers of the involved parties, or outsourced to a third-parties, or outsourced to a third-party -cloud-computing system-: the secure cryptographic calculation module automatically optimizes for the best performing technique of secure computation (for example, homomorphic encryption, garbled circuits, oblivious transfers, secret sharing, oblivious random machines and/or a combination of the previous crypto-primitives).

The Secure Spreadsheet is the first program to offer provably-secure state-of-the-art cryptographically secure secure computation to the general public: for the first time, joint secure calculations between potentially distrusting parties can now be used for very profitable purposes in accounting/finance/banking while maintaining the privacy of the input data. The Secure Spreadsheet is fully functional and already available on the webpage: its strongest points are the easiness of use and retro-compatibility with previously available spreadsheet files. Future developments will integrate it with Private and Verifiable Smart Contracts.





- **Cryptographically Secure Financial Instruments**[CS15]: Systems, methods and financial instruments enhanced with secure computation. A financial instrument management system is implemented with secure computation capabilities, respecting the privacy and secrecy rights during computation of the information contained within financial instruments, external datasets and/or secure computation programs. Automatic conversion and aggregation of conventional financial instruments is also disclosed. Furthermore, secure computation programs can be certified with mathematical proofs about very advantageous and valuable properties such as their correct termination, conformance to a specification, or any other pre-conditions, post-conditions and invariants on their inputs and outputs, encrypted or in plaintext form.

  Note that these Cryptographically Secure Financial Instruments are a specific case of the Private and Verifiable Smart Contracts, in the sense that smart contracts can be of a more general class than the more specific financial instruments. Additional features not discussed on the Raziel paper[CS17b] but available on the patent[CS15] include: storage of the encrypted smart contracts in standard formats; conversion of insecure financial instruments to private financial instruments; packaging financial instruments and interoperability between exchanges.

Cætera desunt

All the technologies hereby mentioned are results of very recent research: future developments are expected and we'll collaborate to be part of their development.

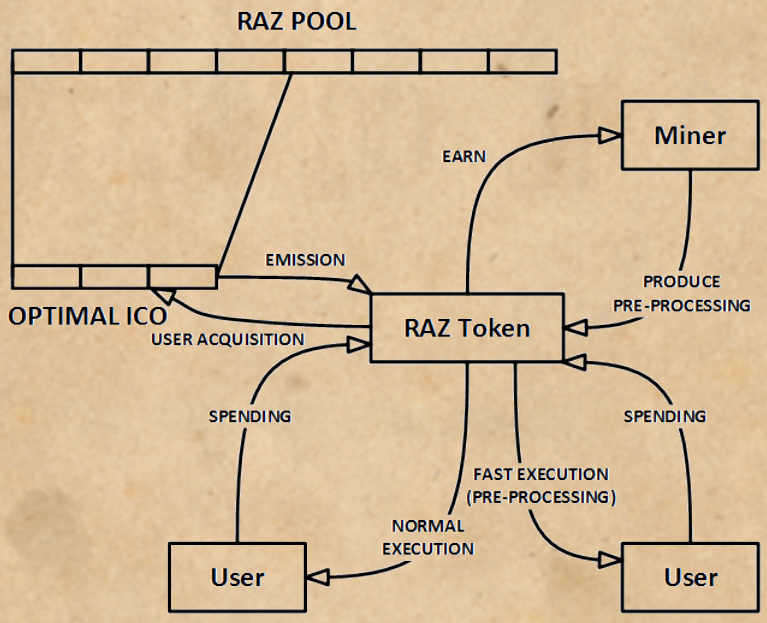
ICO

Details

Role of Token	Utility token for Raziel Smart Contracts
Token Name	RAZ
Maximum supply	500 billion of RAZ Tokens
Offered on ICO	10% (50 billion)
Accepted Currencies	ETH
ICO Mechanism	Described in An Optimal ICO Mechanism (Only auction)
If minimum not met	Funds not called/refunded

Token Lifecyle

The ultimate objective for the creation of the RAZ token is to boostrap a market for the execution rights of private and verifiable smart contracts, including the production and sale of pre-processing data for secure multi-party computation (up to 100x execution speed-up).



Note that the utility of this token intentionally resembles the legally authorised ETH[SC17] (i.e., qualifies as virtual currency), plus the option to speed-up secure computations using acquired pre-processing.

Unoffered Tokens

Tokens that have not been offered in the ICO will become reserved and could be offered later in a controlled way (i.e., preventing dumping the price of quoted tokens).

Minimum Contribution Goal

A minimum contribution goal has been set: if it's not achieved, the individual contributions will not be called and/or refunded.

Use of Funds

Research & Development	80%
Legal	10%
Marketing	10%

Exchanges

After the finalization of the ICO, tokens will be listed on at least one major exchange.

Agreement

Note that before contributing to the ICO, you must read, understand and agree to the crowdsale agreement.

Current Status

1. The Secure Spreadsheet is perfectly functional and available on the web.

2. "An Optimal ICO Mechanism" will be open-sourced after the ICO.

3. Raziel is being developed: the purpose of the ICO is to solve the chicken-and-egg problem by jump-starting a market for its smart-contracts and their pre-processing, and to finance its development to completion.

References

[Ass16] Greenwich Associates. Securing the Blockchain. 2016. https://www.greenwich.com/fixed-income-fx-cmds/securing-blockchain.

[Cha17] ChainAnalysis. The Rise of Cybercrime on Ethereum. 2017. https://blog.chainalysis.com/the-rise-of-cybercrime-on-ethereum/.

[Con99] United States Congress. GrammLeachBliley Act - Financial Services Modernization Act. 1999. https://www.gpo.gov/fdsys/pkg/STATUTE-113/pdf/STATUTE-113-Pg1338.pdf.

[CS14] David Cerezo-Sánchez. Secure Computation on Spreadsheets (PCT/IB2014/065970). 2014. https://www.calctopia.com/papers/secSpreadsheets.pdf.

[CS15] David Cerezo-Sánchez. Cryptographically Secure Financial Instruments (PCT/IB2015/055776). 2015. https://www.calctopia.com/papers/csfi.pdf.

[CS17a] David Cerezo-Sánchez. An Optimal ICO Mechanism. 2017. http://econpapers.repec.org/paper/pramprapa/81285.htm.

[CS17b] David Cerezo-Sánchez. Raziel: Private and Verifiable Smart Contracts on Blockchains. 2017. https://eprint.iacr.org/2017/878.

[GK13] Morton Glantz and Robert Kissell. *Multi-Asset Risk Modeling: Techniques for a Global Economy in an Electronic and Algorithmic Trading Era*. Academic Press, 2013. https://www.calctopia.com/papers/csfi.pdf.

[HR17] Garrick Hileman and Michel Rauchs. Global Blockchain Benchmarking Study. 2017. https://ssrn.com/abstract=3040224.

[PC16] European Parliament and Council. Regulation (EU) 2016/679. 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[SC17] Securities and Exchange Commission. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO. 2017. https://www.sec.gov/litigation/investreport/34-81207.pdf.

[Tec17] Parity Tech. Security Alert - Parity Wallet (multi-sig wallets). 2017. https://paritytech.io/blog/security-alert.html.