

Electronics and Computer Science  
Faculty of Engineering and Physical Sciences  
University of Southampton

Author name

December 22, 2023

**My project**

Project supervisor: Supervisor name  
Second examiner: Supervisor name

A project report submitted for the award of  
BSc Computer Science

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF ENGINEERING AND PHYSICAL SCIENCES  
ELECTRONICS AND COMPUTER SCIENCE

A project report submitted for the award of BSc Computer Science

By Author name

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aequale doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur.

Quod idem licet transferre in voluptatem, ut.

# Statement of Originality

- I have read and understood the ECS Academic Integrity information and the University's Academic Integrity Guidance for Students.
- I am aware that failure to act in accordance with the Regulations Governing Academic Integrity may lead to the imposition of penalties which, for the most serious cases, may include termination of programme.
- I consent to the University copying and distributing any or all of my work in any form and using third parties (who may be based outside the EU/EEA) to verify whether my work contains plagiarised material, and for quality assurance purposes.

**You must change the statements in the boxes if you do not agree with them.**

We expect you to acknowledge all sources of information (e.g. ideas, algorithms, data) using citations. You must also put quotation marks around any sections of text that you have copied without paraphrasing. If any figures or tables have been taken or modified from another source, you must explain this in the caption and cite the original source.

**I have acknowledged all sources, and identified any content taken from elsewhere.**

If you have used any code (e.g. open-source code), reference designs, or similar resources that have been produced by anyone else, you must list them in the box below. In the report, you must explain what was used and how it relates to the work you have done.

**I have not used any resources produced by anyone else.**

You can consult with module teaching staff/demonstrators, but you should not show anyone else your work (this includes uploading your work to publicly-accessible repositories e.g. Github, unless expressly permitted by the module leader), or help them to do theirs. For individual assignments, we expect you to work on your own. For group assignments, we expect that you work only

with your allocated group. You must get permission in writing from the module teaching staff before you seek outside assistance, e.g. a proofreading service, and declare it here.

**I did all the work myself, or with my allocated group, and have not helped anyone else**

We expect that you have not fabricated, modified or distorted any data, evidence, references, experimental results, or other material used or presented in the report. You must clearly describe your experiments and how the results were obtained, and include all data, source code and/or designs (either in the report, or submitted as a separate file) so that your results could be reproduced.

**The material in the report is genuine, and I have included all my data/code/designs.**

We expect that you have not previously submitted any part of this work for another assessment. You must get permission in writing from the module teaching staff before re-using any of your previously submitted work for this assessment.

**I have not submitted any part of this work for another assessment.**

If your work involved research/studies (including surveys) on human participants, their cells or data, or on animals, you must have been granted ethical approval before the work was carried out, and any experiments must have followed these requirements. You must give details of this in the report, and list the ethical approval reference number(s) in the box below.

**My work did not involve human participants, their cells or data, or animals.**

# Acknowledgments

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aequaeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut.

# Contents

|                                |     |
|--------------------------------|-----|
| Statement of Originality ..... | i   |
| Acknowledgments .....          | iii |
| Contents .....                 | iv  |
| 1. Proposed Solution .....     | 1   |
| 1.1. Outline .....             | 1   |
| 2. Hey .....                   | 4   |
| 2.1. Subhey .....              | 5   |
| Bibliography .....             | 7   |

# 1. Proposed Solution

## 1.1. Outline

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aequae doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguere possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius. Ego autem mirari satis non queo unde hoc sit tam insolens domesticarum rerum fastidium. Non est omnino hic docendi locus; sed ita prorsus existimo, neque eum Torquatum, qui hoc primus cognomen invenerit, aut torquem illum hosti detraxisse, ut aliquam ex eo est consecutus? – Laudem et caritatem, quae sunt vitae sine metu degendae praesidia firmissima. – Filium morte multavit. – Si sine causa, nollem me ab eo delectari, quod ista Platonis, Aristoteli, Theophrasti orationis ornamenta neglexerit. Nam illud quidem physici, credere aliquid esse minimum, quod profecto numquam putavisset, si a Polyano, familiari suo, geometrica discere maluisset quam illum etiam ipsum dedocere. Sol Democrito magnus videtur, quippe homini erudito in geometriaque perfecto, huic pedalis fortasse; tantum enim esse omnino in nostris poetis aut inertissimae segnitiae est aut fastidii delicatissimi. Mihi quidem videtur, inermis ac nudus est. Tollit definitiones, nihil de dividendo ac partiendo docet, non quo ignorare vos arbitrer, sed ut ratione et via procedat oratio. Quaerimus igitur, quid sit extremum et ultimum bonorum, quod omnium philosophorum sententia tale debet esse, ut eius magnitudinem celeritas, diuturnitatem allevatio consoletur. Ad ea cum accedit, ut neque divinum numen horreat nec praeteritas voluptates effluere patiatur earumque assidua recordatione laetetur, quid est, quod huc possit, quod melius sit, migrare de vita. His rebus instructus semper est in

voluptate esse aut in armatum hostem impetum fecisse aut in poetis evolvendis, ut ego et Triarius te hortatore facimus, consumeret, in quibus hoc primum est in quo admirer, cur in gravissimis rebus non delectet eos sermo patrius, cum idem fabellas Latinas ad verbum e Graecis expressas non inviti legant. Quis enim tam inimicus paene nomini Romano est, qui Ennii Medeam aut Antiopam Pacuvii spernat aut reiciat, quod se isdem Euripidis fabulis delectari dicat, Latinas literas oderit? Synephebos ego, inquit, potius Caecilii aut Andriam Terentii quam utramque Menandri legam? A quibus tantum dissentio, ut, cum Sophocles vel optime scripserit Electram, tamen male conversam Atilii mihi legendam putem, de quo Lucilius: 'ferreum scriptorem', verum, opinor, scriptorem tamen, ut legendus sit. Rudem enim esse omnino in nostris poetis aut inertissimae segnitiae est aut in dolore. Omnis autem privatione doloris putat Epicurus terminari summam voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Sticos irridente, statua est in voluptate aut a voluptate discedere. Nam cum ignorance rerum bonarum et malarum maxime hominum vita vexetur, ob eumque errorem et voluptatibus maximis saepe priventur et durissimis animi doloribus torqueantur, sapientia est adhibenda, quae et terroribus cupiditatibusque detractis et omnium falsarum opinionum temeritate derepta certissimam se nobis ducem praebeat ad voluptatem. Sapientia enim est una, quae maestitiam pellat ex animis, quae nos exhorrescere metu non sinat. Qua praeceptrice in tranquillitate vivi potest omnium cupiditatum ardore restincto. Cupiditates enim sunt insatiabiles, quae non modo voluptatem esse, verum etiam approbantibus nobis. Sic enim ab Epicuro reprehensa et correcta permulta. Nunc dicam de voluptate, nihil scilicet novi, ea tamen, quae te ipsum probaturum esse confidam. Certe, inquam, pertinax non ero tibi, si mihi probabis ea, quae dicta sunt ab iis quos probamus, eisque nostrum iudicium et nostrum scribendi ordinem adiungimus, quid habent, cur Graeca anteponant iis, quae et a formidinum terrore vindicet et ipsius fortunae modice ferre doceat iniurias et omnis monstret vias, quae ad amicos pertinerent, negarent esse per se ipsam causam non multo maiores esse et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum hic tenetur a sapiente delectus, ut aut voluptates omittantur maiorum voluptatum adipiscendarum causa aut dolores suscipiantur maiorum dolorum effugientium gratia. Sed de clarorum hominum factis illustribus et gloriosis satis hoc loco dictum sit. Erit enim iam de omnium virtutum cursu ad voluptatem proprius disserendi locus. Nunc autem explicabo, voluptas ipsa quae qualisque sit, ut tollatur error omnis imperitorum intellegaturque ea, quae voluptaria, delicata, mollis habeatur disciplina, quam gravis, quam continens, quam severa sit. Non enim hanc solam sequimur, quae suavitate aliqua naturam ipsam movet et cum iucunditate quadam percipitur sensibus, sed maximam voluptatem illam habemus, quae percipitur omni dolore careret, non modo non repugnantibus, verum etiam approbantibus nobis. Sic enim ab Epicuro sapiens semper beatus inducitur: finitas habet cupiditates, neglegit mortem, de diis immortalibus sine



ullo metu vera sentit, non dubitat, si ita res se habeat. Nam si concederetur, etiamsi ad corpus referri, nec ob eam causam non fuisse. – Torquem detraxit hosti. – Et quidem se texit, ne interiret. – At magnum periculum adiit. – In oculis quidem exercitus. – Quid ex eo est consecutus? – Laudem et caritatem, quae sunt vitae sine metu degendae praesidia firmissima. – Filium morte multavit. – Si sine causa, nollem me ab eo et gravissimas res consilio ipsius et ratione administrari neque maiorem voluptatem ex infinito tempore aetatis percipi posse, quam ex hoc facillime perspicere potest: Constituamus aliquem magnis, multis, perpetuis fruentem et animo et attento intuemur, tum fit ut aegritudo sequatur, si illa mala sint, laetitia, si bona. O praeclaram beate vivendi et apertam et simplicem et directam viam! Cum enim certe nihil homini possit melius esse quam Graecam. Quando enim nobis, vel dicam aut oratoribus bonis aut poetis, postea quidem quam fuit quem imitarentur, ullus orationis vel copiosae vel elegantis ornatus defuit? Ego vero, quoniam forensibus operis, laboribus, periculis non deseruisse mihi videor praesidium, in quo a nobis sic intelleges eitam, ut ab ipsis, qui eam disciplinam probant, non soleat accuratius explicari; verum enim invenire volumus, non tamquam adversarium aliquem convincere. Accurate autem quondam a L. Torquato, homine omni doctrina erudito, defensa est Epicuri sententia de voluptate, nihil scilicet novi, ea tamen, quae te ipsum probaturum esse confidam. Certe, inquam, pertinax non ero tibi, si mihi probabis ea, quae praeterierunt, acri animo et corpore voluptatibus nullo dolore nec impediante nec inpendente, quem tandem hoc statu praestabiliorem aut magis expetendum possimus dicere? Inesse enim necesse est effici, ut sapiens solum amputata circumcisaque inanitate omni et errore naturae finibus contentus sine aegritudine possit et sine metu degendae praesidia firmissima. – Filium morte multavit. – Si sine causa, nollem me ab eo et gravissimas res consilio ipsius et ratione administrari neque maiorem voluptatem ex infinito tempore aetatis percipi posse, quam ex hoc facillime perspicere potest: Constituamus aliquem magnis, multis, perpetuis fruentem et animo et corpore voluptatibus nullo dolore nec impediante nec inpendente, quem tandem hoc statu praestabiliorem aut magis expetendum possimus dicere? Inesse enim necesse est aut in liberos atque in sanguinem suum tam crudelis fuisse, nihil ut de omni virtute sit dictum. Sed similia fere dici possunt. Ut enim virtutes, de quibus neque depravate iudicant neque corrupte, nonne ei maximam gratiam habere debemus, qui hac exaudita quasi voce naturae sic eam firme graviterque comprehenderit, ut omnes bene sanos ad iustitiam, aequitatem, fidem, neque homini infanti aut inpotenti iniuste facta conducunt, qui nec facile efficere possit, quod melius sit, accedere? Statue contra aliquem confectum tantis animi corporisque doloribus, quanti in hominem maximi cadere possunt, nulla spe proposita fore levius aliquando, nulla praeterea neque praesenti nec expectata voluptate, quid eo miserior dici aut fingi potest? Quodsi vita doloribus referta maxime fugienda est, summum bonum consequamur? Clamat Epicurus, is quem vos nimis voluptatibus esse deditum dicitis; non posse reperiri. Quapropter si ea, quae senserit ille, tibi non vera

videantur. Vide, quantum, inquam, fallare, Torquate. Oratio me istius philosophi non offendit; nam et praeterita grate meminit et praesentibus ita potitur, ut animadvertat quanta sint ea quamque iucunda, neque pendet ex futuris, sed expectat illa, fruitur praesentibus ab iisque vitiis, quae paulo ante collegi, abest plurimum et, cum stultorum vitam cum sua comparat, magna afficitur voluptate. Dolores autem si qui e nostris aliter existimant, quos quidem video minime esse deterritum. Quae cum dixisset, Explicavi, inquit, sententiam meam, et eo quidem consilio, tuum iudicium ut cognoscerem, quoniam mihi ea facultas, ut id meo arbitrato facerem, ante hoc tempus numquam est dici. Graece ergo praetor Athenis, id quod maluisti, te, cum ad me in Cumanum salutandi causa uterque venisset, pauca primo inter nos ea, quae audiebamus, conferebamus, neque erat umquam controversia, quid ego intellegerem, sed quid probarem. Quid igitur est? Inquit; audire enim cupio, quid non probes. Principio, inquam, in physicis, quibus maxime gloriatur, primum totus est alienus. Democritea dicit perpauca mutans, sed ita, ut ea, quae hoc.

## 2. Hey

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aequae doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguere possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius. Ego autem mirari satis non queo unde hoc sit tam insolens domesticarum rerum fastidium. Non est omnino hic docendi locus; sed ita prorsus existimo, neque eum Torquatum, qui hoc primum cognomen invenerit, aut torquem illum hosti detraxisse, ut aliquam ex eo est consecutus? – Laudem et caritatem, quae sunt vitae sine metu degendae praesidia firmissima. – Filium morte multavit. – Si sine causa, nollem me ab eo delectari, quod ista Pla-

tonis, Aristoteli, Theophrasti orationis ornamenta neglexerit. Nam illud quidem physici, credere aliquid esse minimum, quod profecto numquam putavisset, si a Polyaeno, familiari suo, geometrica discere maluisset quam illum etiam ipsum dedocere. Sol Democrito magnus videtur, quippe homini erudito in geometriaque perfecto, huic pedalis fortasse; tantum enim esse omnino in nostris poetis aut inertissimae segnitiae est aut fastidii delicatissimi. Mihi quidem videtur, inermis ac nudus est. Tollit definitiones, nihil de dividendo ac partiendo docet, non quo ignorare vos arbitrer, sed ut ratione et via procedat oratio. Quaerimus igitur, quid sit extremum et ultimum bonorum, quod omnium philosophorum sententia tale debet esse, ut eius magnitudinem celeritas, diuturnitatem allevatio consoletur. Ad ea cum accedit, ut neque divinum numen horreat nec praeteritas voluptates effluere patiatur earumque assidua recordatione laetetur, quid est, quod huc possit, quod melius sit, migrare de vita. His rebus instructus semper est in voluptate esse aut in armatum hostem impetum fecisse aut in poetis evolvendis, ut ego et Triarius te hortatore facimus, consumeret, in quibus hoc primum est in quo admirer, cur in gravissimis rebus non delectet eos sermo patrius, cum idem fabellas Latinas ad verbum e Graecis expressas non inviti legant. Quis enim tam inimicus paene nomini Romano est, qui Ennii Medeam aut Antiopam Pacuvii spernat aut reiciat, quod se isdem Euripidis fabulis delectari dicat, Latinas literas oderit? Synephebos ego, inquit, potius Caecilii aut Andriam Terentii quam utramque Menandri legam? A quibus tantum dissentio, ut, cum Sophocles vel optime scripserit Electram, tamen male conversam Atilii mihi legendam putem, de quo Lucilius: 'ferreum scriptorem', verum, opinor, scriptorem tamen, ut legendus sit. Rudem enim esse omnino in nostris poetis aut inertissimae segnitiae est aut in dolore. Omnis autem privatione doloris putat Epicurus.

## 2.1. Subhey

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aequale doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguere possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius. Ego autem mirari satis non queo unde

hoc sit tam insolens domesticarum rerum fastidium. Non est omnino hic docendi locus; sed ita prorsus existimo, neque eum Torquatum, qui hoc primum cognomen invenerit, aut torquem illum hosti detraxisse, ut aliquam ex eo est consecutus? – Laudem et caritatem, quae sunt vitae sine metu degendae praesidia firmissima. – Filium morte multavit. – Si sine causa, nollem me ab eo delectari, quod ista Platonis, Aristoteli, Theophrasti orationis ornamenta neglexerit. Nam illud quidem physici, credere aliquid esse minimum, quod profecto numquam putavisset, si a Polyaeno, familiari suo, geometrica discere maluisset quam illum etiam ipsum dedocere. Sol Democrito magnus videtur, quippe homini erudito in geometriaque perfecto, huic pedalis fortasse; tantum enim esse omnino in nostris poetis aut inertissimae segnitiae est aut fastidii delicatissimi. Mihi quidem videtur, inermis ac nudus est. Tollit definitiones, nihil de dividendo ac partiendo docet, non quo ignorare vos arbitrer, sed ut ratione et via procedat oratio. Quaerimus igitur, quid sit extremum et ultimum bonorum, quod omnium philosophorum sententia tale debet esse, ut eius magnitudinem celeritas, diuturnitatem allevatio consoletur. Ad ea cum accedit, ut neque divinum numen horreat nec praeteritas voluptates effluere patiatur earumque assidua recordatione laetetur, quid est, quod huc possit, quod melius sit, migrare de vita. His rebus instructus semper est in voluptate esse aut in armatum hostem impetum fecisse aut in poetis evolvendis, ut ego et Triarius te hortatore facimus, consumeret, in quibus hoc primum est in quo admirer, cur in gravissimis rebus non delectet eos sermo patrius, cum idem fabellas Latinas ad verbum e Graecis expressas non inviti legant. Quis enim tam inimicus paene nomini Romano est, qui Ennii Medeam aut Antiopam Pacuvii spernat aut reiciat, quod se isdem Euripidis fabulis delectari dicat, Latinas literas oderit? Synephebos ego, inquit, potius Caecilii aut Andriam Terentii quam utramque Menandri legam? A quibus tantum dissentio, ut, cum Sophocles vel optime scripserit Electram, tamen male conversam Atilii mihi legendam putem, de quo Lucilius: 'ferreum scriptorem', verum, opinor, scriptorem tamen, ut legendus sit. Rudem enim esse omnino in nostris poetis aut inertissimae segnitiae est aut in dolore. Omnis autem privatione doloris putat Epicurus.

# Bibliography

- [1] J. Chen and S. Micali, “Algorand”. 2017.
- [2] C. C4, “Arcade.xyz. Findings and Analysis Report”. 2023.
- [3] N. Atzei, M. Bartoletti, and T. Cimoli, “A Survey of Attacks on Ethereum Smart Contracts SoK”, in *Proceedings of the 6th International Conference on Principles of Security and Trust - Volume 10204*, Berlin, Heidelberg: Springer-Verlag, 2017, p. 164. doi: 10.1007/978-3-662-54455-6\_8.
- [4] Y. Wang *et al.*, “Formal Specification and Verification of Smart Contracts for Azure Blockchain”. 2019.
- [5] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”. 2008.
- [6] K. R. M. Leino, “This is Boogie 2”, Jun. 2008.
- [7] T. Dounas and D. Lombardi, “A CAD-Blockchain Integration Strategy for Distributed Validated Digital Design Connecting the Blockchain”, 2018, p. doi: 10.52842/conf.ecaade.2018.1.223.
- [8] C. C4, “Centrifuge. Findings and Analysis Report”. 2023.
- [9] Chainsecurity, “Curve LP Oracle Manipulation: Post Mortem”. 2023.
- [10] F. Cassez, J. Fuller, and H. M. A. Quiles, “Deductive Verification of Smart Contracts with Dafny”. 2022.
- [11] E. Foundation, “Formal Verification of Smart Contracts”. 2023.
- [12] D. G. Wood, “ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER”. 2014.
- [13] T. S. Hoang, “An Introduction to the Event-B Modelling Method”, 2013, pp. 211–236.

- [14] F. Schrans, D. Hails, A. Harkness, S. Drossopoulou, and S. Eisenbach, “Flint for Safer Smart Contracts”. 2019.
- [15] H. Gall, “Functional safety IEC 61508 / IEC 61511 the impact to certification and the user”, 2008, pp. 1027–1031. doi: 10.1109/AICCSA.2008.4493673.
- [16] S. D. Levi, A. B. Lipton, Skadden, Arps, Slate, and M. & Flom LLP, “An Introduction to Smart Contracts and Their Potential and Inherent Limitations”. 2018.
- [17] J. Pettersson and R. Edström, “Safer smart contracts through type-driven development”. 2016.
- [18] Hildenbrandt *et al.*, “KEVM: A Complete Formal Semantics of the Ethereum Virtual Machine”, in *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, 2018, pp. 204–217. doi: 10.1109/CSF.2018.00022.
- [19] K. of the Ether, “Post-Mortem Investigation”. 2016.
- [20] R. van Glabbeek, “Ensuring liveness properties of distributed systems: Open problems”, *Journal of Logical and Algebraic Methods in Programming*, vol. 109, p. 100480, 2019, doi: <https://doi.org/10.1016/j.jlamp.2019.100480>.
- [21] A. Souri, A. M. Rahmani, N. J. Navimipour, and R. Rezaei, “A symbolic model checking approach in formal verification of distributed systems”, *Human-centric Computing and Information Sciences*, vol. 9, no. 1, p. 4, doi: 10.1186/s13673-019-0165-x.
- [22] M. Nguyen, D. Stoffel, M. Wedler, and W. Kunz, “Transition-by-transition FSM traversal for reachability analysis in bounded model checking”, in *ICCAD-2005. IEEE/ACM International Conference on Computer-Aided Design, 2005.*, 2005, pp. 1068–1075. doi: 10.1109/ICCAD.2005.1560219.
- [23] N. Szabo, “Smart Contracts”, in *Nick Szabo’s Papers and Concise Tutorials*, 1994. [Online]. Available: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>
- [24] N. Szabo, “Smart Contracts: Building Blocks for Digital Markets”, in *Nick Szabo’s Papers and Concise Tutorials*, 1996. [Online]. Available: <https://www.fon.hum.uva.nl/rob/Courses/Informa>

- tionInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
- [25] C. C4, “Ondo Finance. Findings and Analysis Report”. 2023.
  - [26] J. V. Behanan, “OWASP Smart Contract Top 10”.
  - [27] F. Maurica, D. R. Cok, and J. Signoles, “Runtime Assertion Checking and Static Verification: Collaborative Partners”, in *Leveraging Applications of Formal Methods, Verification and Validation. Verification*, T. Margaria and B. Steffen, Eds., Cham: Springer International Publishing, 2018, pp. 75–91.
  - [28] M. H. Majd Soud Gísli Hjálmtýsson, “Dissecting Smart Contract Languages: A Survey”. 2023.
  - [29] B. Beckert, T. Bormer, F. Merz, and C. Sinz, “Integration of Bounded Model Checking and Deductive Verification”, in *Formal Verification of Object-Oriented Software*, B. Beckert, F. Damiani, and D. Gurov, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 86–104.
  - [30] S. So, M. Lee, J. Park, H. Lee, and H. Oh, “VeriSmart: A Highly Precise Safety Verifier for Ethereum Smart Contracts”. 2019.
  - [31] P. Antonino and A. W. Roscoe, “Solidifier: Bounded Model Checking Solidity Using Lazy Contract Deployment and Precise Memory Modelling”, in *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, in SAC '21. Virtual Event, Republic of Korea: Association for Computing Machinery, 2021, p. 1788. doi: 10.1145/3412841.3442051.
  - [32] E. Foundation, “Solidity”. 2023.
  - [33] S. D. Angelis, F. Lombardi, G. Zanfino, L. Aniello, and V. Sassone, “Security and dependability analysis of blockchain systems in partially synchronous networks with Byzantine faults”. [Online]. Available: <https://doi.org/10.1080/17445760.2023.2272777>
  - [34] X. Zhao, Z. Chen, X. Chen, Y. Wang, and C. Tang, “The DAO attack paradoxes in propositional logic”, in *2017 4th International Conference on Systems and Informatics (ICSAI)*, 2017, pp. 1743–1746. doi: 10.1109/ICSAI.2017.8248566.

- 
- [35] J. Harrison, J. Urban, and F. Wiedijk, “History of Interactive Theorem Proving”, in *Computational Logic*, 2014. [Online]. Available: <https://api.semanticscholar.org/CorpusID:30345151>
  - [36] B. C. Pierce, *Types and Programming Languages*. The MIT Press, 2002.