



Athens Journal of Sciences

Quarterly Academic Periodical, Volume 9, Issue 1, March 2022

URL: <https://www.athensjournals.gr/ajs>

Email: journals@atiner.gr

e-ISSN: 2241-8466 DOI: 10.30958/ajs



Front Pages

ANASTASIA NIKOLOGIANI, ALESSANDRO BETTA, MATTIA
ANDREOLA, ANGELICA PIANEGONDA, GIAN ANTONIO BATTISTEL,
ANNA TERNELL & ALESSANDRO GRETTIER

**Urban Farming Models, Ecosystems and Climate Change Adaptation in
Urban Environments: The Case of SATURN Pan European Programme**

JOHN M. MEDELLIN

**Generation, Regeneration and Validation of Binary Secret Keys through
Blockchain in IoT Devices**

THOMAS FEHLMANN & EBERHARD KRANICH

**The Fixpoint Combinator in Combinatory Logic - A Step towards
Autonomous Real-time Testing of Software?**

HAO TSAI & ERH-TSUNG CHIN

Pupil's Fraction Learning based on Board Game Playing

Athens Journal of Sciences

Published by the Athens Institute for Education and Research (ATINER)

Editors

- Dr. Christopher Janetopoulos, Head, [Biology Unit](#), ATINER & Associate Professor, University of the Sciences, USA.(Biology)
- Dr. Ethel Petrou, Academic Member, ATINER & Professor and Chair, Department of Physics, Erie Community College-South, State University of New York, USA.
- Dr. Ellene Tratras Contis, Head, [Chemistry Unit](#), ATINER & Professor of Chemistry, Eastern Michigan University, USA.(Chemistry)

Editorial & Reviewers' Board

<https://www.athensjournals.gr/ajs/eb>

Administration of the Journal

1. Vice President of Publications: Dr Zoe Boutsoli
2. General Managing Editor of all ATINER's Publications: Ms. Afrodete Papanikou
3. ICT Managing Editor of all ATINER's Publications: Mr. Kostas Spyropoulos
4. Managing Editor of this Journal: Ms. Olga Gkounta

ATINER is an Athens-based World Association of Academics and Researchers based in Athens. ATINER is an independent and non-profit Association with a Mission to become a forum where Academics and Researchers from all over the world can meet in Athens, exchange ideas on their research and discuss future developments in their disciplines, as well as engage with professionals from other fields. Athens was chosen because of its long history of academic gatherings, which go back thousands of years to Plato's Academy and Aristotle's Lyceum. Both these historic places are within walking distance from ATINER's downtown offices. Since antiquity, Athens was an open city. In the words of Pericles, Athens "...is open to the world, we never expel a foreigner from learning or seeing". ("Pericles' Funeral Oration", in Thucydides, The History of the Peloponnesian War). It is ATINER's mission to revive the glory of Ancient Athens by inviting the World Academic Community to the city, to learn from each other in an environment of freedom and respect for other people's opinions and beliefs. After all, the free expression of one's opinion formed the basis for the development of democracy, and Athens was its cradle. As it turned out, the Golden Age of Athens was in fact, the Golden Age of the Western Civilization. Education and (Re)searching for the 'truth' are the pillars of any free (democratic) society. This is the reason why Education and Research are the two core words in ATINER's name.

The *Athens Journal of Sciences (AJS)* is an Open Access quarterly double-blind peer reviewed journal and considers papers from all areas of Natural & Formal Sciences, including papers on agriculture, computer science, environmental science, materials science, transportation science, chemistry, physics, mathematics and statistics, biology, geography, and earth science (geology, oceanography, astronomy, meteorology). Many of the papers published in this journal have been presented at the various conferences sponsored by the [Natural & Formal Sciences Division](#) of the Athens Institute for Education and Research (ATINER). All papers are subject to ATINER's [Publication Ethical Policy and Statement](#).

The Athens Journal of Sciences
ISSN NUMBER: 2241-8466- DOI: 10.30958/ajs
Volume 9, Issue 1, March 2022
Download the entire issue ([PDF](#))

<u>Front Pages</u>	i-viii
<u>Urban Farming Models, Ecosystems and Climate Change Adaptation in Urban Environments: The Case of SATURN Pan European Programme</u> <i>Anastasia Nikologianni, Alessandro Betta, Mattia Andreola, Angelica Pianegonda, Gian Antonio Battistel, Anna Ternell & Alessandro Gretter</i>	9
<u>Generation, Regeneration and Validation of Binary Secret Keys through Blockchain in IoT Devices</u> <i>John M. Medellin</i>	25
<u>The Fixpoint Combinator in Combinatory Logic - A Step towards Autonomous Real-time Testing of Software?</u> <i>Thomas Fehlmann & Eberhard Kranich</i>	47
<u>Pupil's Fraction Learning based on Board Game Playing</u> <i>Hao Tsai & Erh-Tsung Chin</i>	65

Athens Journal of Sciences

Editorial and Reviewers' Board

Editors

- **Dr. Christopher Janetopoulos**, Head, [Biology Unit](#), ATINER & Associate Professor, University of the Sciences, USA.(Biology)
- **Dr. Ethel Petrou**, Academic Member, ATINER & Professor and Chair, Department of Physics, Erie Community College-South, State University of New York, USA.
- **Dr. Ellene Tratras Contis**, Head, [Chemistry Unit](#), ATINER & Professor of Chemistry, Eastern Michigan University, USA.(Chemistry)

Editorial Board

- Dr. Colin Scanes, Academic Member, ATINER & Emeritus Professor, University of Wisconsin Milwaukee, USA.
- Dr. Dimitris Argyropoulos, Professor, North Carolina State University, USA.
- Dr. Cecil Stushnoff, Emeritus Professor, Colorado State University, USA.
- Dr. Hikmat Said Hasan Hilal, Academic Member, ATINER & Professor, Department of Chemistry, An-Najah N. University, Palestine.
- Dr. Jean Paris, Professor, Polytechnique Montreal, Canada.
- Dr. Shiro Kobayashi, Academic Member, ATINER & Distinguished Professor, Kyoto Institute of Technology, Kyoto University, Japan.
- Dr. Jose R. Peralta-Videa, Academic Member, ATINER & Research Specialist and Adjunct Professor, Department of Chemistry, The University of Texas at El Paso, USA.
- Dr. Jean-Pierre Bazureau, Academic Member, ATINER & Professor, Institute of Chemical Sciences of Rennes ICSR, University of Rennes 1, France.
- Dr. Mohammed Salah Aida, Professor, Taibah University, Saudi Arabia.
- Dr. Zagabathuni Venkata Panchakshari Murthy, Academic Member, ATINER & Professor/Head, Department of Chemical Engineering, Sardar Vallabhbhai National Institute of Technology, India.
- Dr. Alexander A. Kamnev, Professor, Institute of Biochemistry and Physiology of Plants and Microorganisms, Russian Academy of Sciences, Russia.
- Dr. Carlos Nunez, Professor, Physics Department, University of Wales Swansea, UK.
- Dr. Anastasios Koulaouzidis, Academic Member, ATINER & Associate Specialist and Honorary Clinical Fellow of the UoE, The Royal Infirmary of Edinburgh, The University of Edinburgh, UK.
- Dr. Francisco Lopez-Munoz, Professor, Camilo Jose Cela University, Spain.
- Dr. Panagiotis Petratos, Professor, California State University-Stanislaus, USA.
- Dr. Yiannis Papadopoulos, Professor of Computer Science, Leader of Dependable Systems Research Group, University of Hull, UK.
- Dr. Joseph M. Shostell, Professor and Department Head, Math, Sciences & Technology Department, University of Minnesota Crookston, USA.
- Dr. Ibrahim A. Hassan, Professor of Environmental Biology, Faculty of Science, Alexandria University, Egypt & Centre of Excellence in Environmental Studies, King Abdulaziz University, Saudi Arabia.
- Dr. Laurence G. Rahme, Associate Professor, Department of Surgery, Microbiology and Immunobiology, Harvard Medical School, Boston, Massachusetts & Director of Molecular Surgical Laboratory, Burns Unit, Department of Surgery, Massachusetts General Hospital, USA.
- Dr. Stefano Falcinelli, Academic Member, ATINER & Associate Professor, Department of Civil and Environmental Engineering, University of Perugia, Italy.
- Dr. Mitra Esfandiarei, Academic Member, ATINER & Assistant Professor, Midwestern University, USA.
- Dr. Athina Meli, Academic Member, Academic Member, ATINER, Visiting Scientist and Research Scholar, University of Gent & University of Liege, Belgium and Ronin Institute Montclair, USA.

- **Vice President of Publications:** Dr Zoe Boutsoli
- **General Managing Editor of all ATINER's Publications:** Ms. Afrodete Papanikou
- **ICT Managing Editor of all ATINER's Publications:** Mr. Kostas Spyropoulos
- **Managing Editor of this Journal:** Ms. Olga Gkounta ([bio](#))

Reviewers' Board

[Click Here](#)

President's Message

All ATINER's publications including its e-journals are open access without any costs (submission, processing, publishing, open access paid by authors, open access paid by readers etc.) and is independent of presentations at any of the many small events (conferences, symposiums, forums, colloquiums, courses, roundtable discussions) organized by ATINER throughout the year and entail significant costs of participating. The intellectual property rights of the submitting papers remain with the author. Before you submit, please make sure your paper meets the [basic academic standards](#), which includes proper English. Some articles will be selected from the numerous papers that have been presented at the various annual international academic conferences organized by the different divisions and units of the Athens Institute for Education and Research. The plethora of papers presented every year will enable the editorial board of each journal to select the best, and in so doing produce a top-quality academic journal. In addition to papers presented, ATINER will encourage the independent submission of papers to be evaluated for publication.

The current issue is the first of the ninth volume of the *Athens Journal of Sciences (AJS)*, published by [Natural & Formal Sciences Division](#) of ATINER.

Gregory T. Papanikos, President, ATINER.



Athens Institute for Education and Research

A World Association of Academics and Researchers

10th Annual International Conference on Chemistry

18-21 July 2022, Athens, Greece

The [Chemistry Unit](#) of ATINER, will hold its **10th Annual International Conference on Chemistry, 18-21 July 2022, Athens, Greece** sponsored by the [Athens Journal of Sciences](#). The aim of the conference is to bring together academics and researchers of all areas of chemistry and other related disciplines. You may participate as stream organizer, presenter of one paper, chair a session or observer. Please submit a proposal using the form available (<https://www.atiner.gr/2022/FORM-CHE.doc>).

Academic Members Responsible for the Conference

- **Dr. Ellene Tratras Contis**, Head, Chemistry Unit, ATINER & Professor of Chemistry, Eastern Michigan University, USA.

Important Dates

- Abstract Submission: **28 March 2022**
- Acceptance of Abstract: 4 Weeks after Submission
- Submission of Paper: **20 June 2022**

Social and Educational Program

The Social Program Emphasizes the Educational Aspect of the Academic Meetings of Atiner.

- Greek Night Entertainment (This is the official dinner of the conference)
- Athens Sightseeing: Old and New-An Educational Urban Walk
- Social Dinner
- Mycenae Visit
- Exploration of the Aegean Islands
- Delphi Visit
- Ancient Corinth and Cape Sounion

Conference Fees

Conference fees vary from 400€ to 2000€
Details can be found at: <https://www.atiner.gr/fees>



Athens Institute for Education and Research

A World Association of Academics and Researchers

10th Annual International Conference on Physics **18-21 July 2022, Athens, Greece**

The [Physics Unit](#) of ATINER, will hold its **10th Annual International Conference on Physics, 18-21 July 2022, Athens, Greece** sponsored by the [Athens Journal of Sciences](#). The aim of the conference is to bring together academics and researchers of all areas of physics and other related disciplines. Please submit a proposal using the form available (<https://www.atiner.gr/2022/FORM-PHY.doc>).

Important Dates

- Abstract Submission: **28 March 2022**
- Acceptance of Abstract: 4 Weeks after Submission
- Submission of Paper: **20 June 2022**

Academic Member Responsible for the Conference

- **Dr. Ethel Petrou**, Academic Member, ATINER & Professor and Chair, Department of Physics, Erie Community College-South, State University of New York, USA.
- **Dr. Bala Maheswaran**, Head, Electrical Engineering Unit, ATINER & Professor, Northeastern University, USA.

Social and Educational Program

The Social Program Emphasizes the Educational Aspect of the Academic Meetings of Atiner.

- Greek Night Entertainment (This is the official dinner of the conference)
- Athens Sightseeing: Old and New-An Educational Urban Walk
- Social Dinner
- Mycenae Visit
- Exploration of the Aegean Islands
- Delphi Visit
- Ancient Corinth and Cape Sounion

More information can be found here: <https://www.atiner.gr/social-program>

Conference Fees

Conference fees vary from 400€ to 2000€

Details can be found at: <https://www.atiner.gr/fees>

Urban Farming Models, Ecosystems and Climate Change Adaptation in Urban Environments: The Case of SATURN Pan European Programme

By Anastasia Nikologianni^{*}, Alessandro Betta[±], Mattia Andreola[°],
Angelica Pianegonda[•], Gian Antonio Battistel[♦], Anna Ternell[♥]
& Alessandro Gretter[▲]

The “System and sustainable Approach to virTuous interaction of Urban and Rural LaNdsapes” (SATURN) project is exploring how resilience at a city scale might be achieved and how the issues of landscape fragmentation, governance and land management can be addressed resulting in a sustainable future. The EIT Climate-KIC SATURN project is based on a collaboration between three cities of very different scales and contexts, those of Gothenburg in western Sweden, Trento in northern Italy, and Birmingham in the United Kingdom. This paper focuses on the ways in which urban farming can become an important tool to mitigate or adapt to climate change in urban environments by exploring how the three major cities of SATURN deal with these concepts. Using the experience gained throughout the SATURN project as well as the strong communication developed within the consortium, the paper introduces the reasons why urban farming is not just an agricultural activity, but it relates to climate awareness, health and an element of community. With the examples of different urban farming models, this research presents the fully entrepreneurial model of Gothenburg, where a business model fosters sustainable and successful small-scale farming through municipal management of small allotments with associated basic infrastructure leased out to entrepreneurs. Public underutilized land is matched with farmers in order for them to scale up their businesses and provide sustainable food, by limiting the shipping distance of the produce. In the Trento case, bottom-up and more institutional processes have been combined to foster short local supply chains through the Nutrire Trento networking process which could benefit from the introduction of a land lease scheme named “banca della terra” (to support agricultural land recovery). The case of Birmingham presents a different model where farming in an urban environment is mostly seen as a support to communities, mental health and awareness, rather than an entrepreneurial activity. The innovation in this paper comes in the form of different European models related to urban agriculture and best practices, demonstrating how abandoned and underutilised public and private land can be regenerated and become an active part of the urban realm. Insights on the ways in which the three different models operate, as well as results on how farming in an urban environment can enhance resilient cities are discussed in this paper.

Keywords: urban farming, climate change, landscape ecosystems, entrepreneurial agriculture, community farming

^{*}Post Doctorate Research Fellow, Birmingham City University, The Parkside Building, UK.

[±]Researcher, Fondazione Edmund Mach - IASMA Research Centre, Italy.

[°]Research Staff, Department of Civil, Environmental and Mechanical Engineering, University of Trento, Italy.

[•]Research Staff, Department of Civil, Environmental and Mechanical Engineering, University of Trento, Italy.

[♦]Research Staff, Department of Civil, Environmental and Mechanical Engineering, University of Trento, Italy.

[♥]Researcher PE Technology and Architecture, Sweden.

[▲]Project Lead SATURN, Fondazione Edmund Mach - IASMA Research Centre, Italy.

Introduction

This paper explores a series of urban farming models to examine the ways in which such initiatives can provide effective solutions on climate mitigation and adaptation in urban environments. It is based on methodologies developed at the pan-European project EIT Climate-KIC SATURN (SATURN), testing and evaluating landscape challenges and how these can be addressed through alternative governance and stakeholder engagement. The SATURN project aims to create supportive frameworks and design tools to support cities and regions address the landscape fragmentation they experience, while they explore innovative ideas to future proof their cities. The aim of this paper is to present and discuss one of the pillars of the broader SATURN project, the urban farming/food growing component and explore how urban farming can be beneficial to the fight against a changing climate. The examples of three different urban farming models established and tested in Gothenburg (Sweden), Trento (Italy) and Birmingham (UK) demonstrate how food growing initiatives can be beneficial to the local and broader community. The models discussed by this paper explore different methods based on each country's geographical and cultural characteristics, with the purpose to exchange knowledge and result in best practices and lessons learned for farming within cities or peri-urban areas.

Farming and food growing in urban and peri-urban areas have faced several challenges, especially with the expansion of cities, urbanisation and the mass expansion of agriculture to be able to respond to the great demand for food as well as transportation across the globe. However, what this paper suggests is that, if we are to successfully address the climate crisis, urban farming needs to play a role on how cities are growing their food, at least for a part of the necessary consumption. It is known that cities are increasingly interested in new initiatives, in relation to the climate crisis, constantly experimenting with pioneering schemes and ideas (von Wirth et al. 2019) therefore SATURN's models on alternative urban farming schemes are proven rather relevant. Soulard et al. (2018) suggest that urban agriculture has been an integral part of the society for centuries, either in the form of "gardens, huertas, oases" or else, but urban expansion absorbs agricultural and natural terrains. Although it still exists, urban agriculture is now facing a sharp decline as urban developments grow and agricultural modernization continues. According to Soulard et al. (2018), part of the issue is that farming businesses in peri-urban areas that were targeting national markets and exportations, are now within the jurisdiction of urban policies, a fact that plays a major role in the way in which farms can operate. In addition, Januszkiewicz and Jarmusz (2017) state that "the food security problem is far more complex than solely undernourishment or even malnutrition. Understanding the interrelation, scientists are developing sensitive agro-ecosystems and architects are envisioning new kinds of spatial structures for them". Based on such evidence, the SATURN project suggests that specific innovative models need to be designed to establish synergies between agriculture, urban farming and the city, aiming to address food growing in urban environments. The focus of this paper is on the creation of such innovative models as well as how these can be applied spatially at a city or regional level.

Using three pioneering urban farming schemes that have identified either entrepreneurial or social and mental health benefits (Gothenburg, Trento, Birmingham), this paper discusses the various techniques developed around urban farming and underutilized land with the aim to build a sustainable future. The paper suggests that all different models are valuable depending on the goals and challenges each area is facing. The frameworks developed by this project are being tested with the aim to result in an adaptable model that can be transformed and used across different cities and countries.

Key Concepts on Urban Farming, Ecosystems and Climate Change

The climate crisis and the change of the environment is now apparent (IPCC 2018), however the impact on ecosystems, vegetation and living organisms is constantly being examined. According to the UN-Habitat, cities are responsible for 50-60% of the global CO₂ emissions and about 75% of the global primary energy with buildings and transport as major contributors (Mousa et al. 2020). Considering that projections indicate that approximately 70% of the global population will live in cities by 2050 (UN DESA 2018), we ought to think how urban centres are impacting on the environment and what the solutions we have in our hands to accommodate a more sustainable living are. The growth of the urban population will further increase the demand for basic goods such as food products. Consequently, the environmental footprint of food consumption in cities is expected to increase significantly (Pradhan et al. 2020) and therefore a more sustainable food growing chain seems apparent. Examples of sustainable food systems have started to emerge. The C40 Food Systems Network, the Urban Food Policy Pact of Milan as well as Madrid's Food Strategy explore agriculture in urban while aiming at healthy and sustainable cities. Even though we do not have fully developed models and many cities are looking at further opportunities there is a momentum being built and therefore the scope of this paper is considered rather relevant.

Ecosystem is a group of living organisms that interact with each other in a specific environment. The term is often used for natural ecosystems, but it is also common to use it for a complex network or interconnected system, such as the entrepreneurial ecosystem of a city or the regional ecosystem of an area. Whatever the definition, climate crises have a major impact on the ecosystems and as Jennings and Harris (2017) state, "climate change alters the vegetation composition and functioning of ecosystems". Vegetation is a major part of any natural, but also urban ecosystem and any alteration to its composition, due to environmental and climate changes, results in possible threats of this ecosystem. Knowledge around the various climate challenges of an area is considered important for setting priorities for its conservation and restoration (Jennings and Harris 2017). Food growing is part of terrestrial ecosystems and therefore this study recognizes that any impact from climate change will create several challenges to its habitat and any activities taking place in the area. Intensive agriculture contributes to a great share of the biodiversity's loss (Bocchi 2020) and the food growing process has to

be considered in its key role of affecting climate change and societal habits. Agricultural activities are responsible for 10.3% of GHG emissions in Europe, while the food sector contributes 18% of households' GHG emissions (European Commission 2020a). The livestock sector is responsible for 18% of the global Greenhouse Gas emissions (GHG) (Steinfeld et al. 2006) and 75% of the lost biodiversity (Bocchi 2020). As Jennings and Harris (2017) mention, the planet is experiencing a significant amount of climatic flux and changes and therefore, it is important to find ways to predict and protect future vegetation in order for our ecosystems to adapt to the environmental challenges.

This study agrees that the impact of climate change on our landscapes, either urban or rural, is very significant and even though it is now recognised from the broad scientific community, there is still a long way to go to create fully sustainable cities. It was more than a decade ago when Opdam et al. (2009) mentioned “we can be sure of profound effects on ecological processes in and functioning of landscapes. The impact of climate change will affect all types of land use, ecosystem services, as well as the behaviour of humans”. All these seem now apparent, but we are still not entirely sure of the various catastrophic events (wildfires, flooding, hurricanes) that will appear in the future, as we were not expecting a global pandemic (COVID-19). Even though we cannot predict the future environmental catastrophes and their exact timing, it is obvious that they have become more intense and common over the recent years, a fact that has made scientists, decision makers and the public to re-think their way of living. As Grimm et al. (2008) mention, urbanisation is considered a key driver of pollution and climate change, resulting in the alteration of both biotic and abiotic ecosystems either these are in urban or rural areas. With such scientific facts in our knowledge, this study agrees that a resilient and sustainable response to land change must be tackled at local, regional and global scales. The variations of ecosystems at a regional scale are based on different combinations of vegetation, climate and geomorphology (Grimm et al. 2008), and therefore SATURN's approach to examine and test different land use initiatives across Europe seems a valid step to address climate challenges across all scales.

The various changes of the current climate are also affecting the landscape patterns and their processes, and therefore one of the core responsibilities of landscape and ecology professions is to understand how such relationships are manifested across spatial and temporal scales (Opdam et al. 2009). Especially in urban environments, climatic conditions are being greatly affected as a result of the dense construction and population, creating a microclimate which often results in “lighter winds, less humidity, more or fewer rainstorms compared to surrounding rural areas” (Grimm et al. 2008). So, what does this mean for urban farming, and how can we be sure such conditions are suitable for food production? Soulard et al. (2018) agree that the urban agricultural and farming environment is a diverse ecosystem with various dynamics and multidisciplinary elements. Despite the fact that agro-ecosystems face major global issues and they are on decline, different forms of peri-urban agriculture still evolve (Souillard et al. 2018). As pointed out by experts and agreed by this paper, urban farming and peri-urban agriculture demonstrate the capacity to resist to environmental challenges, however issues

such as food security, water scarcity and the conservation of ecosystem diversity need to be addressed (Soulard et al. 2018) if cities and regions are to adapt and mitigate to climate change. The SATURN project is based on these positive indicators, aiming to test and evaluate how urban and peri-urban farming can support the creation of sustainable cities and regions. As Soulard et al. (2018) point out “urbanization heightens agricultural diversity. The disruptions and opportunities created by the pressures of urban growth encourage the development of hybrid agro-ecosystems that adapt to the specific urban conditions or conserve more classical forms”. Together with Opdam et al. (2009) point that “landscape change should be acceptable to local stakeholders and politicians”, SATURN’s approach on involving decision makers and local actors in the establishment of an urban farming model is of great significance.

There is evidence that urban agriculture is of great significance for global food security and that can allow cities to expand while producing clean food and preserve ecological balance of their ecosystems (Mousa et al. 2020). As Li et al. (2020) suggest, “the increasing population and continuous urbanization make food security prominent in sustainable development. It is important to develop economic and resource-efficient farming to meet food demand”. Similar to what this paper explores, Li continues stating that in urban and regional land use there are no “one-size fits all” solutions, but to achieve sustainable agricultural production, decision-makers and farmers need to develop site specific strategies (Li et al. 2020). In spatial and landscape strategies, site specific models are of great importance as they allow for the bespoke development of agricultural models based on each area’s policies, topography and cultural characteristics. Using this evidence, this paper examines three different urban farming models, focusing on the steps required to enhance adaptation and mitigation and how these affect governance, farmers, scientists and other relevant organizations. The importance of this study is justified by Mousa et al. (2020) who explain that “integrating urban farms into the city fabric has many economic, social and environmental benefits. It offers clean food, while improving air quality resulting from carbon emissions and air pollution mitigation” (Mousa et al. 2020). In addition to the pioneering farming models presented below, the broader SATURN project is creating a holistic visioning approach (Nikologianni et al. 2020) to support the establishment of new models and sustainable designs within cities and regions. This approach comes in alignment with Januszkiewicz and Jarmusz’s (2017) indication that “to successfully migrate food production from extensive rural areas to dense environments of city centres, a new holistic approach, integrating knowledge and advances of multiple fields of science, has to develop”. For this to happen, a cross-silo and multidisciplinary approach, that will allow designers, urban planners, engineers and decision makers to redefine contemporary design processes, is needed.

Methodology

This paper’s methodology is based on close examination of urban agriculture and farming models across Europe aiming to examine, test and evaluate the

significance of urban agriculture in food production as well as the possibility for it to become an important aid to sustainable urban development.

SATURN is a pan European project exploring how the issues of landscape fragmentation, governance and land management can be addressed in relation to city resilience. The project requires a minimum of three European countries that are co-funded by the European Institute of Innovation and Technology (EIT) (Nikologianni et al. 2020). The three countries involved Italy (IT), the United Kingdom (UK), and Sweden (SW) formed a consortium and were awarded funds in 2018. The successful team that forms the consortium represents southern, western and northern Europe. SATURN is co-funded by EIT and Climate-KIC, as well as the cities and institutions forming the consortium from November 2018 to December 2021 (Consortium 2019). The broader project's aim is to develop frameworks to support resolving the issues of landscape governance and fragmentation in relation to the climate crisis. To undertake this work, SATURN focuses on the relationships among cities, food growing, and the rural landscape through the development of case studies at each hub. Each partner-city absorbs this new knowledge into their local governance structures. The real-life case studies have distinctly different physical, social, economic, and cultural conditions within a varied range of existing spatial aspirations and contexts. A stakeholder mapping and engagement process is developed through workshops, field visits, and extensive communications, including regular meetings across the consortium.

This paper examines three models developed at the core hubs of SATURN, Sweden, Italy and the UK focusing on the generation of new knowledge and innovative techniques to support food production in a sustainable manner within cities. The entrepreneurial model of Gothenburg (Sweden), the networking process and land lease scheme of Trento (Italy) and the community focused model of Birmingham (UK) are being examined.

The methodology includes the continuous research and development of these pioneering models during SATURN's duration, the processes followed, and the new knowledge generated in relation to the city scale and climate adaptation/mitigation techniques. Continuous engagement with the stakeholders responsible for the development of the urban farming models, their training as well as the collection of results and future steps are part of the methodological process together with training and expert support on sustainability and entrepreneurial models. The use of the public underutilized land model developed in Gothenburg as well as the land lease model of Trento both aim to provide support to farmers to scale up their businesses, but also to cities to improve their land use considering natural resources and future resilience. The case of Birmingham presents a different model where farming in an urban environment is mostly seen as a support to communities, mental health and awareness, rather than a sole entrepreneurial activity. The methods used in this paper include observations, evaluation of the three models in relation to their aims, their location as well as the policies in place in each country. Results indicated that urban farming models are of important value, can be much more environmentally friendly and community oriented and they offer an alternative solution to intensive agriculture.

The data collected for this paper is based on the processes followed for the urban farming models, meetings and policy roundtables with decision makers, observations as well as workshops with the management team of each model. Data were collected and analysed through content analysis.

Urban Farming Models

This section will present three different farming and growing models, selected as case studies during the SATURN project in order to explore how growing can be regenerated in urban environments. Each scheme has demonstrated its own best practices and challenges, depending on the area and policy in place. The three models tackle the broader concept of farming in urban centres, how this contributes to social cohesion as well as the practical side of farming in cities and peri urban centres.

The Farm to Table Region - The Case of Gothenburg

The city of Gothenburg with support from nearby regions has created a unique entrepreneurial model of farming. The aim is to increase urban food production and further green entrepreneurship in and around the city centre in order to identify land use models and strategies for reconnecting cities to their surrounding areas. There is a lot of underutilized land and abandoned buildings in the area of Gothenburg, so the objective is to create a region known for its effective and flexible entrepreneurial system, facilitating small scale commercial vegetable production in the peri urban areas. The Gothenburg model consists of four different pilot actions connected to the enhancement of urban agriculture, redevelopment of abandoned sites, and education of young generations. The challenge is to increase job creation and new farming business models, to increase food security, to improve eco-system services accounting and natural solutions for the climate risk management. The indirect impact is better social inclusion by the participation generation, the better understanding of the geographical identity and revaluation of the urban hinterland. The actions aiming to build a legacy of “Farm to Table Region” for Gothenburg consist of four initiatives dealing with urban farming and entrepreneurship. These are the Model farm, test sites (Angered, Skogome), Farming Incubator and mapping of underutilised land (LAB190).

The Model Farm is developed in cooperation with the City of Gothenburg and the Region Västra Götaland; is a highly productive small-scale farm unit, providing food for schools and elderly care and education at Angereds Gård in peri-urban Gothenburg. The main objective of this activity is to create and demonstrate a successful business model behind a sustainable and small-scale farming enterprise run within a municipality. It serves as a driver for the integration of regenerative farming practices in the continuous evolution of urban and rural multifunctional landscapes. Among the activities of the Model Farm are the creation of a model farm handbook supporting existing and new farmers, webinars and training, study visits to act as educational and awareness for decision makers as well as data

collection on farming practices such as quantity and quality of crops, costs and income calculations for a small scale farm unit. The scheme has been very successful within the community allowing for networking opportunities for young farmers but also acting as an advocate of what can be achieved in a city environment with limited space and resources. The Model Farm has 40 vegetable beds in total, adding up to a total growing area of 600 square meters. It aims to produce around 3,000 kg of vegetables during the cultivation season, which equals to 20-25 thousand servings of vegetables in the receiving kitchens. Students are also invited to practice in this market gardening initiative and during the last season (2021) two classes were invited at five occasions.

The Farmers Incubator (in Stadsbruk) is a programme for new small-scale green farming entrepreneurs in urban and peri-urban areas of Gothenburg with the aim to train and increase the number of ecological farmers committed to sustainable land management. The objective is to increase the number of local/ecological farmers in Swedish cities through “agriprenurship” training (agricultural entrepreneurship) and with a strong collaboration with the Gothenburg municipality which offers access to underutilised or abandoned public land. The incubator gathers, creates, tests and shares successful business models relevant to farmers providing knowledge and training on how businesses operate in this field. A winter training programme has been in place with capacity of around 10 new entrepreneurs every year. Run for the second consecutive year, the programme’s initial results demonstrate that the creation of a farming-oriented network, the opportunity to further training and thematic workshops have been beneficial to the farmers of the region. While new and existing farmers receive training on entrepreneurial and agriculture, the city of Gothenburg has the opportunity to collect feedback and evaluate its land matchmaking process. Overall, the Farmers Incubator has been a successful outcome of the SATURN project and the city is intending to continue even after the duration of the European programme. It is believed that the scheme will support the boost in the number of farmers and help regenerate the underutilized land of the city, resulting in a positive environmental impact in the area, such as the local food production, reduced transport and packaging emissions.

The LAB190 is strongly related with the recovering of underutilized farmland and enhancing generational change. Creating a model for match-making new green entrepreneurs with underutilised farmland in the urban hinterland has been one of the highlights of the Urban Farming Model of Gothenburg. This initiative has got the interest of various other European cities and regions, but it has also acted as a great way to regenerate and relive the abandoned spaces of the city. The objective is to develop a method for mapping available land and its future potentials. The mapping exercise aims to become a valuable interface for municipalities and private landowners, to make land available to new entrepreneurs within the green sector. Being a collaborative initiative between four municipalities (Gothenburg, Lerum, Alingsås and Essunga), LAB190 has great potential for scaling up across other cities in Sweden as well as European countries. Several capacity building and dissemination activities (webinars, food-led events)

supported by the city of Gothenburg have allowed for exchange of knowledge and the creation of a common land use vision between the cities involved.

The “Angered and Skogome” pilot case aims to recover peri-urban plots by supporting people in establishing innovative business models. The objective has been to facilitate small scale commercial vegetable production in the peri urban areas while establishing a broader urban farming scheme through the Model Farm, the Incubator and LAB190. The selected test sites of Angered and Skogome were chosen to increase urban food production and boost green entrepreneurship in and around the city centre of Gothenburg. Several activities, such as farmers roundtables, stakeholder assessment meetings and the production of a guide on testbeds, have been generated after the initial launch of the scheme demonstrating the positive outcomes of this pilot across the city. The initiative has now been expanded into creating a “test farm” to act as a community farm that will engage with multiple stakeholders in the area. The project has welcomed 6 new urban farmers to the testbeds in Angered and Skogome and with this, a total of 34 farmers are established on both testbeds, many of which have already registered their companies and began delivering to local customers. The majority of sales are still done through the so-called “REKO-rings” which is a popular system in the region, currently involving close to 300,000 customers across the Nordic countries. REKO-rings provide a way for producers of locally grown produce and customers to develop a relationship as well as providing a practical sales channel for growers. Operating through closed Facebook groups, customers order in advance and gather pre-packed bags at convenient locations, typically once a week. There has also been a slight growth in direct sales from the farms. Some farmers also deliver to restaurants in the Gothenburg area.

Through four different actions the Gothenburg model demonstrates that a successful urban farming scheme in dense areas is feasible, resulting in several benefits for the municipality, the farmers and the public. The green space will regenerate the area and provide a healthier and greener city, while the local food production and consumption will mitigate the carbon emissions in the area produced by transport and shipping.

Networking for a Community-Based Recovery of Land and Practices - The Case of Trentino

The territorial and socio-economic conditions of the Trentino province located in the middle of the Italian Alps contribute to make it a pretty peculiar case. There is a strong industrialized farming sector focused mostly on growing apples and vineyards yet based on a large number of small landowners who are part of the network of territorial cooperatives. This particular situation is not exempt from challenges or negative sides which is at the base of the decision of local administration and stakeholders to develop both a tool named “banca della terra - earth bank” and the Nutrire Trento network. The two tools have fairly different backgrounds, with the earth bank being an institutional tool developed by the local government (in accordance with national regulations), while Nutrire Trento and its follow-up, CSA “Naturalmente in Trentino”, is generated by a bottom-up process

coordinated by researchers of the University of Trento. The purpose of the Bank of the Earth is to link the processes of abandonment and non-cultivation with facilitating the access to plots of land by young or new farmers and agricultural businesses. Therefore, it acts as a meeting point between supply and demand and can become a precious tool for the protection of landscape, drawing attention to areas which are often neglected and at the same time offer the possibility to young people who intend to dedicate to agriculture, even if they do not come from farming families or do not have their own land, to find available plots. This could allow a generational change, or the consolidation of existing agricultural enterprises. At national level, the Italian law 154/2016 introduced the “*Banca nazionale delle terre agricole*” which has then been translated at a regional level the following year with the Trentino law 15/2017. This law is part of a wider reform of the law for the government of the territory. It is essentially an inventory of public and private uncultivated land, which the owners can temporarily make available to those who request it to put them back into production. In the case of public-owned plots the land is added to the earth bank directly by the municipalities, while in the case of privately-owned plots the public authority acts only as a link between the owner and potential new farmers that are asking for land availability. This demand has grown steadily in recent years not only as a reaction to the increased lack of jobs for young people but also as an answer to the need of reducing the detachment from nature and food chains.

Considering the relevance of the agricultural sector in Trentino, but also the related socio-environmental issues, a new demand has emerged for social inclusion in the agricultural sector, the promotion of formative programmes and the recovery of agro-ecological agricultural practices. Therefore, these aspects should be considered as crucial as the re-utilisation of uncultivated land. Recognising a serious economic, social and environmental gap between urban and rural landscapes, local institutions have undertaken the challenge to set up corrective projects, as in the case of Nutrire Trento. The Nutrire Trento initiative aims to promote more conscious consumption, raise awareness of more sustainable production and reconnect producers and consumers (Forno et al. 2020). As it is a participatory process, the main tool of the project is a round table that brings together local stakeholders to discuss issues related to the food system, its paradoxes and failures to plan shared solutions. Since 2017, the initiative has seen the participation of more than 125 actors active in the Trento and surrounding municipalities: agricultural producers, consumers, activists, researchers, shopkeepers, representatives of the institutions and categories involved.

The local context presents a very rich humus of initiatives consistent with its objectives. However, there is an evident lack of coordination between these players, resulting in dispersed and inefficient exploitation of the efforts and human resources involved and a suboptimal impact on the target audience.

For this reason, the main function of Nutrire Trento is to enhance the resonance of these realities, by optimising the interaction between the actors and developing new links, networks and opportunities. These functions are pursued in different ways: through networking at meetings, dissemination events, but also - and especially - through publicization using communication media. The main one

is the digital platform that allows the public to visualise the actors and locations of the Trentino short supply chain.

The COVID-19 pandemic has revealed the need to enrich Nutrire Trento's repertoire of actions by promoting its projects. The changes in consumption habits that occurred during the 2020 spring lockdown have led to the development of many spontaneous innovations that have also spread to the Trentino context. Precisely to monitor and investigate these new ways of buying, selling and consuming, the Nutrire Trento Round Table proposed an experiment that was called Nutrire Trento #Fase2. The goal was to provide support to local farms to sell directly to interested families and enhance the community's interest to buy local agricultural products and have them delivered at home. Besides taking part in weekly orders, participation in the project also involved the completion of three questionnaires, for both families and producers, to study the changes in purchasing patterns that had become a necessity during the lockdown and to investigate the sustainability over time of the proposed production, distribution and purchasing system.

For nine weeks, 68 families and 13 producers took part in the initiative, giving some interesting indications: first of all, a decrease in food waste, linked to better consumption planning. Secondly, a decrease in purchases from supermarkets and discount outlets, balanced by an increase in purchases in small shops, on producers' farms and home delivery. Finally, an increase in the consumption of local and national products and a decrease in the purchase of pre-cooked, pre-packaged and frozen food. The results obtained are very promising and represent an important step to support future enhancements of the initiative in order to involve larger numbers of producers and families. However, the project also encountered several problems and saw a steady decline in the number of users of the service. The questionnaires revealed that this was linked to the shortage of some products and the presence of a minimum order which made purchasing less convenient. To overcome these issues, the producers emphasised the need to plan seasonal production together with consumers.

One of the most important results of the Nutrire Trento #Fase2 project was the creation of a Community Supported Agriculture (CSA), thanks to the synergies among farmers that emerged. The CSA is a model of food production and distribution based on an alliance between consumers and farmers. Indeed, it is a more sophisticated alternative to food networks in Italy (e.g., Solidarity Purchasing Groups) since consumers are asked to commit to and support a group of farmers, both morally and financially. Farmers and consumers agree on the cultivation methods and the production plan by co-designing the whole process. Thus, consumers become partners by sharing the entrepreneurial risk and accepting the possibility of losing agricultural production. At the moment, 13 producers and 32 consumer families are involved in this initiative, but it is constantly expanding. An association has been founded to bring the two sides of the supply chain closer and create a real community bonding. This association acts as a legal entity for the CSA and it is responsible for the organisation of guided events at the producers' farms and other activities aimed at spreading the principles of the CSA, including

educational workshops for children and a dissemination blog with contributions from all members and partners.

Growing in the Community - The Case of Birmingham

The Birmingham model is about developing a growing network in an urban environment that includes, growing, gardens and urban farming. Even though the two previous models have a focus on agriculture and entrepreneurship, the “Growing in the Community” scheme aims to spread awareness and engage with the community through farming. The team behind this model states that creation of physical space nurtures and presents opportunities for the generation of social space in the urban fabric.

Being at the heart of the second biggest city in England, entrepreneurial farming activities are not that easy, however the aim of this model is much more than just food production. The Urban Farming and Growing Network, a case study of the SATURN project, has identified itself as a group providing support to the community by “growing people”, using this activity as a mental health support as well as a community bonding. Birmingham’s scheme is not just about mitigating carbon in urban farming but enhancing its social benefits. One might wonder why such a scheme is relevant to the scope of this paper and the broader SATURN study, but it is important to mention that cities need a behavioural and systemic change in order to mitigate or adapt to climate change. Following the COVID-19 pandemic, there is an increase in community growing groups and engagement to open spaces (Mead et al. 2021), resulting in further exploration of green and community accessible spaces in cities. The “growing in the community” model is therefore, about mental health as much as food production and even though it does not operate as an entrepreneurial incubator at the moment, is seeking the city’s support to expand and explore business opportunities as well as the access to community gardens within close proximity from dwellings.

The Birmingham model operates in several community gardens, farms and allotments across the city addressing the various environmental benefits, the impact these have in urban communities as well as how these can be enhanced through a strong and enjoyable urban farming scheme. Due to their flexible structure, community gardens are considered less strict compared to allotments or farming plots, that require planning permissions and protections (Hardman and Larkham 2014) and therefore they are increasingly used in cities as ways to promote environment, a healthy lifestyle and social cohesion. Especially in a post-COVID-19 world, local food growing can provide both resilience and capacity (Mikadze 2020) in cities and peri-urban areas, demonstrating a different dimension of urban growing in relation to climate resilience.

The work undertaken by the Urban Farming and Growing Network, with the support of the SATURN project, has revealed many hidden beneficiaries and needs in the area of the West Midlands as well as positive outcomes of the community engagement in food growing activities. Similar to what Mousa et al. (2020) explain, the Birmingham model has also identified that the social aspect of a project is very significant during its initial stages, but it also helps in the creation

of a scheme that people feel they belong to and can be part of. Dealing with the community element together with the environmental challenges, this model revealed routes of collaboration and found ways to engage with local stakeholders they were not able to engage before. A landscape evaluation, a recognition of barriers and challenges in the area have enhanced the motion, and provided evidence demonstrating that a society-driven growing scheme is of real value to dense and urban environments.

The community focused, Birmingham model, comes as a complementary scheme to the more entrepreneurial models of Gothenburg and Trento. Using the dense urban environments of the city of Birmingham and its surroundings, it demonstrates how urban farming and growing can become an activity of contemplation, understanding and valuing of the land, and bring social cohesion to support the climate related acts in the area. It is important to mention that business and entrepreneurial activities are being explored, but the focus is on the way in which growing in cities can mitigate carbon emissions and support a healthier lifestyle while it provides for its citizens.

Discussion

The collaboration between the different European cities and the expertise provided by SATURN have resulted in interesting findings and best practices in relation to urban farming and environmental challenges. The three models presented here are still developing, however they have been tested locally and demonstrated that the idea of growing and farming is possible in urban and peri-urban environments when a broader framework or system is in place to support it. Exploring agriculture-oriented models (e.g., Gothenburg) the study shows that urban farming is able to partly replace the food production in cities and regions, when a business model is supporting the broader idea and an awareness plan is in place. Having created a model for match-making new “green” entrepreneurs with underutilized farmland in the urban hinterland, Gothenburg city has created a market for smaller more sustainable farms, providing a more environmentally friendly way of farming, while it also supports local production and job creation. Both Gothenburg and Trento are looking into mapping and identifying available urban land, aiming at creating a network of land owners, farmers and local authorities who would all support the progression of small scale commercial crop production in cities and peri-urban areas. Especially for Trento, the goal is to support the creation of an established process to enhance interaction between farmers and citizens. The opportunity of farmers to join alternative food networks employing more sustainable methods will provide a more environmentally friendly urban farming structure while retaining economic benefits.

Whilst embracing the other two models, Birmingham, recognizing its growing population and the need for a healthier city, is creating an innovative model aiming to support mental health, community bonding and provide for a healthier lifestyle through growing food in open spaces and community gardens. The Birmingham model almost works in a therapeutic way, highlighting the significance of nature,

food and the benefits of local production in relation to mitigating and adapting to climate change. Using the experience of the established “Social farms and gardens” network as well as other passionate individuals, this model operates with local authorities and other institutions to find ways to establish “urban growing” in the city. One of the key findings is that using the SATURN tools, all models have found ways to engage with local stakeholders and explore further opportunities related to their region. The opportunity to learn about similar models across Europe, understand how these operate and extract best practices has also been greatly beneficial, for all schemes as some needed support in the business development and others needed to enhance their broader scope and introduce sustainable development goals in their framework. Citizen’s approach is encouraging to such pioneering models, since they agree that food should be produced in a manner that respects local tradition and “know-how” (87%), and comes from a geographical area that they know (81%) (European Commission 2020b). The short supply chain minimizes transport emissions and usually follows more sustainable patterns in food production and distribution. Overall, urban farming models offer adaptation solutions with regards to climate change either by supporting more sustainable food chains or by spreading awareness in relation to the environmental challenges. The models dealing with social and community cohesion have a major impact on the way in which communities understand climate crisis and how cities can integrate such initiatives.

Conclusions

Food security is one of the most significant challenges we face and it is considered to become worse in the near future. Agriculture and farming play a very important role in food production, however the multiple climate and global challenges are creating several issues in the sector. While we are trying to feed a growing population, we should also aim for more sustainable and environmentally-oriented farming to be able to truly provide a resilient future. This paper identifies ways in which urban farming can support food production either by creating innovative green models or by adapting to climate challenges with the support of the whole community.

The three models presented above have provided initial findings on methods, policies and training required for farming to be successful in cities and peri-urban areas, however the broader SATURN project seeks to test such initiatives in more cities and countries across the globe, aiming to result to a coherent framework that will allow the creation of viable farming models on a smaller scale. The breakthrough in this study comes when one realises that urban farming and growing does not need to compete with large agricultural land or intensive agriculture, but to find its niche and unique market within the city/region of each area. With the support of Gothenburg, Trento and Birmingham cities, the SATURN project has identified methodologies where growing food in dense environments can be beneficial for the region; regeneration of the land, increase local produce, provide sustainable locally-grown food and minimize the CO₂

emissions generated by transport. It is also a great way to engage with the wider community and spread awareness on the environmental benefits of a healthier city.

The exchange of knowledge between the three models has attracted further interest from cities in Slovenia, Greece, Spain, Italy, Sweden, Norway and New Zealand looking to test and engage further with the tools developed by SATURN. It is significant to state that while SATURN's goal is to provide the broader framework and the training for the cities to develop similar models, each area has its own policies and geomorphology and therefore the models will need to be adapted to each specific location and farming needs. This new concept of urban farming breaks from its traditional definition, aiming to support adaptation and mitigation activities that have been established in each region, while at the same time it supports the businesses, economy and mental health of the community.

Acknowledgments

This research has received co-funding support by EIT CLIMATE-KIC. The funders had no role in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

The authors want to thank EIT Climate-KIC, which has supported this research throughout, as well as all the stakeholders and case study participants in the UK, Italy, and Sweden.

References

- Bocchi S (2020) Agroecology: relocalizing agriculture accordingly to places. In *Bioregional Planning and Design*, volume II, 81–99. Springer.
- Consortium S (2019) *SATURN conference, workshop, exhibition*. K Moore, A Nikologianni. Birmingham, UK: Birmingham City University.
- European Commission (2020a) *A farm to fork strategy for a fair, healthy and environmentally-friendly food system*. Brussels: European Commission.
- European Commission (2020b) *The Eurobarometer survey*. Retrieved from: https://ec.europa.eu/info/food-farming-fisheries/key-policies/common-agricultural-policy/cap-glance/eurobarometer_en. [Accessed 6 August 2021]
- Forno F, Maurano S, Vittori F (2020) Costruire processi partecipativi attorno al cibo: Le esperienze di Bergamo e Trento. (Building participatory processes around food: The experiences of Bergamo and Trento). In E Dansero, D Marino, G Mazzocchi, Y Nicolarea (eds.), *Lo Spazio delle Politiche Locali del Cibo: Temi, Esperienze e Prospettive*.
- Grimm NB, Foster D, Groffman P, Grove JM, Hopkinson CS, Nadelhoffer KJ, et al. (2008) The changing landscape: ecosystem responses to urbanization and pollution across climatic and societal gradients. *Frontiers in Ecology and the Environment* 6(5): 264–272.
- Hardman M, Larkham PJ (2014) *Informal urban agriculture*. Springer.
- IPCC (2018) *Global warming of 1.5°C*. An IPCC Special Report Edited by V Masson-Delmotte, P Zhai, H-O Pörtner, D Roberts, J Skea, PR Shukla, et al. UN.

- Januszkiewicz K, Jarmusz M (2017) Envisioning urban farming for food security during the climate change era. Vertical farm within highly urbanized areas. In *IOP Conference Series: Materials Science and Engineering* 245(5): 052094.
- Jennings MD, Harris GM (2017) Climate change and ecosystem composition across large landscapes. *Landscape Ecology* 32(1): 195–207.
- Li L, Li X, Chong C, Wang C-H, Wang X (2020) A decision support framework for the design and operation of sustainable urban farming systems. *Journal of Cleaner Production* 268(Sep): 121928.
- Mead BR, Davies JA, Falagán N, Kourmpetli S, Liu L, Hardman CA (2021) Urban agriculture in times of crisis: the role of home food growing in perceived food insecurity and well-being during the early COVID-19 lockdown. *Emerald Open Research* 3(May): 7.
- Mikadze V (2020) Landscape urbanism and informal space-making: insights from a guerrilla gardening case in Montreal, Canada. *Journal of Urban Design* 25(6): 794–811.
- Mousa H, Elhadidi M, Abdelhafez H, Tonini P, Fellin L, Frongia A, et al. (2020) The role of urban farming in revitalizing cities for climate change adaptation and attaining sustainable development: case of the city of Conegliano, Italy. In A Sayigh (ed.), *Green Buildings and Renewable Energy: Med Green Forum 2019 - Part of World Renewable Energy Congress and Network*, 545–577. Cham: Springer International Publishing.
- Nikologianni A, Betta A, Pianegonda A, Favargiotti S, Moore K, Grayson N, et al. (2020) New integrated approaches to climate emergency landscape strategies: the case of pan-European SATURN project. *Sustainability* 12(20): 8419.
- Opdam P, Luque S, Jones KB (2009) Changing landscapes to accommodate for climate change impacts: a call for landscape ecology. *Landscape Ecology* 24(6): 715–721.
- Pradhan P, Kriewald S, Costa L, Rybski D, Benton TG, Fischer G, et al. (2020) Urban food systems: how regionalization can contribute to climate change mitigation. *Environmental Science & Technology* 54(17): 10551–10560.
- Soulard C-T, Valette E, Perrin C, Abrantes PC, Anthopoulou T, Benjaballah O, et al. (2018) Peri-urban agro-ecosystems in the Mediterranean: diversity, dynamics, and drivers. *Regional Environmental Change* 18(3): 651–662.
- Steinfeld H, Gerber P, Wassenaar TD, Castel V, Rosales M, de Haan C (2006) *Livestock's long shadow: environmental issues and options*. Food & Agriculture Org.
- United Nations Department of Economic and Social Affairs – UN DESA (2018) *68% of the world population projected to live in urban areas by 2050*. New York: UN DESA.
- von Wirth T, Fuenfschilling L, Frantzeskaki N, Coenen L (2019) Impacts of urban living labs on sustainability transitions: mechanisms and strategies for systemic change through experimentation. *European Planning Studies* 27(2): 229–257.

Generation, Regeneration and Validation of Binary Secret Keys through Blockchain in IoT Devices

By John M. Medellin *

This article operationalizes a mathematical root of trust that can be scaled into protection for Internet of Things (IoT) devices. The initial discussion focuses on gated arrays and the generation of 4-way binary keys. Randomization is used in generation of input and sequence keys giving a unique secret key. The probability of successful attack depends on the number of devices and ordinary implementations are well into one in a billion or more. The paper uses the “epoch” concept; a time-dimensioned interval where more blocks are added to the blockchain. The epochs are selected at random and voting, duration, frequency and key roles are also randomized increasing resiliency. The model does not require constant update of IoT storage; only until such time as communication with others is initiated or a request is received. The substantial savings in processing requirements are significant in IoT. A detailed discussion of the management of the blockchain is provided as well as the necessary blocks enabling the approach. The paper includes a sample dialogue using standard TCP/IP communication structures with security protocols and closing remarks aim at extrapolation to cloud and quantum computing.

Keywords: *blockchain, key management and distribution, internet of things, root of trust, cyber-resiliency*

Introduction

Logic operations, blockchain and key validation/encryption are common terms used in a variety of technologies implemented for protection of computers. This paper proposes a model for interaction of these concepts into an approach that is operationally efficient for devices in the Internet of Things (IoT). These technologies are well known but the ability to have them interact at the right time for protection in this way is novel. The approach specifically lends itself to use in processors that must conserve energy (Huang and Cheng 2002).

This paper is organized into related work, logic gates, blockchain and key exchanges to set preparatory material. Next, the discussion focuses on explaining the randomized election process and key generation, the blockchain components and the interaction of devices along the TCP/IP layers using this model. A simulation-experiment gives an example of the order of magnitude in this approach versus traditional computation-intensive ones. Finally, a brief discussion of extensibility into cloud and quantum computing is provided.

*Chief Technical Officer, Medellin Applied Research Concepts, LLC and TruDecision, Inc., USA.

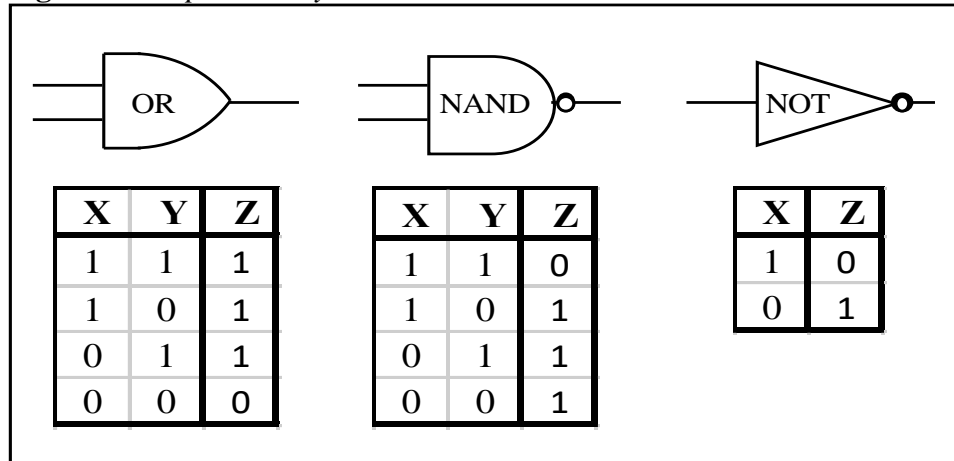
Related Work

Previous work is in three categories; logic gates, blockchain patterns and secret keys.

Logic Operations (Logic Gates)

Logic operations are symbols that operate on two binary input numbers (1 or 0) and yield a third binary outcome. In Figure 1, three operations; OR, NAND and NOT are illustrated in the top part, common symbols for representing them are shown and are used in design for circuits and chips. The matrix below shows the corresponding “truth table” for each “gate” operation above. The format of the truth table shows what happens to the output (Z) when two inputs are entered. There are 4 possible combinations in the two input numbers 1 and 0 with a set of 4 outcomes for the OR and the NAND gates in the example. The NOT X gate only contains 1 input which can have 2 possible values of Z.

Figure 1. Sample Gate Symbols & Truth Tables



There are 6 operations and outcomes from 2-way binary gates (Ferguson et al. 2010). The truth tables for those gates can be found in Figure 2 (the model that is presented in section “Model Heuristics and Base Operations” requires the usage of 2 way gates, the 1 way gate has been omitted).

Figure 2. Inputs, Outputs & Gated Outcomes for Different Scenarios

Scenario	Inputs		Logic Gate Outputs (Z)				
	X	Y	OR	NOR	AND	NAND	XOR
1	1	1	1	0	1	0	0
2	1	0	1	0	0	1	1
3	0	1	1	0	0	1	1
4	0	0	0	1	0	1	0

A key reason for usage of logic gates is their energy/voltage requirements. Binary result computations based on logic gates will use comparatively low CPU cycles (therefore less energy) versus the requirements of decimal or other base

numbering systems. In the case of the division operation, computation of the result can take up to 1 cycle per bit¹ (some typical algorithms like the SHA 384 or higher will contain a payload of 512 hexadecimal values or $512 \times 16 = 8192$ CPU cycles to compute the result). Most algorithms that require key validation today rely on usage of extensive division, multiplication and other operations (Ferguson et al. 2010). By this very virtue, they are more computationally intensive and therefore require more energy to derive. This document assumes and experiments with logic gates to achieve significant resource conservation. Conservation of computational resources is vital to smaller processors (Monk 2017).

Blockchain Design Patterns

Blockchain is a variation of shared data intelligence made famous by Nakamoto (2019); although the author is unknown, it has had a significant impact on creating the concept of shared value exchanges that do not necessarily need to occur through a third-party intermediary. The most famous of these exchange operations is bitcoin. There are literally hundreds of medium exchanges where willing buyers and sellers can contribute value in order to transact between themselves without an intermediary.

This article is not about the usage of such “shared intelligence” to create an exchange for value, rather the usage of the blockchain pattern as a medium for disseminating factual information related to secret keys between participants. Recent academic developments have begun to explore the secrecy and computational advantages of blockchain to communicate in a trust-worthy fashion between members of particular communities (Dinh et al. 2017, Dorri et al. 2017a). Some recent examples of alternate use of blockchain include distribution of sign-on credentials or authentication of agents (Li et al. 2019, Dorri et al. 2017b). These studies rely on exchanging a secret known to the sender and receiver and can be validated by trusted parties who are members of the blockchain (Salman et al. 2018).

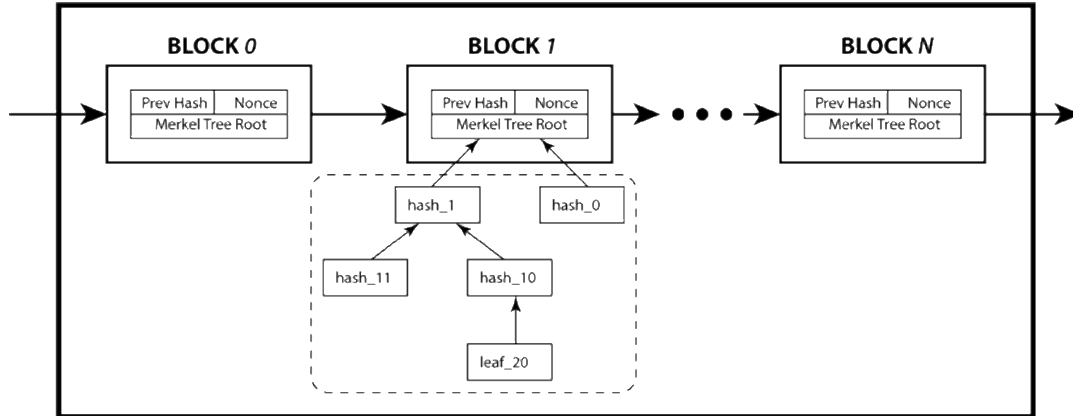
In precursor articles, the author has written about blockchain in the context of usage of this design pattern mostly on the consensus architecture requirements and implementation (Medellin and Thornton 2018). In those studies, comparisons were made to the Byzantine General’s Problem; a common shared context problem used to teach the concepts of consensus between participants. This particular technique is complex and very computational but serves as the yardstick to measure efficiency. The focus of this document will branch into measurement of binary operations versus those referenced in higher number system operations to arrive at consensus.

Although there is no authoritative set of components for the blockchain design pattern, there are some typical components. The typical components of the block chain are: the block architecture, a smart contract (which is optional), a consensus model (the ability to validate previous blocks), a set of participants – typically elastic as to volume and a method for encryption using a unique number (the “nonce”) which is used once in that encryption (Liang and Wu 2017,

¹<https://projectf.io/posts/division-in-verilog/>. [Accessed 17 February 2021]

Christidis and Devetsikiotis 2020, Ongaro and J. Ousterhout 2014, Muralidharan et al. 2018, Ferguson et al. 2010). A partial graphical representation of a typical blockchain set of blocks and attributes is diagrammed and presented in Figure 3.

Figure 3. *Partial Blockchain Sequence and Block*



Secret Keys (Trust and Encryption)

Human beings have used the concept of secrets for perhaps millennia. Secrets have been used to preserve and communicate critical information in key situations (Soni and Goodman 2017). These concepts have evolved through the ages and are inherited by computer systems today.

Modern systems create trust between each other by using mathematical formulae that have finite answers. Two computer systems will exchange a particular sequence of numbers and apply a secret formula to determine the veracity of the sequence being received (Johnsonbaugh 2018). If the item checks out then communication can proceed. There are multiple formulae that can be used but the most popular rely on the modulo operations. In modulo operations, a number is divided by another number and the remainder whole-number component is the result. For example, 9 modulo 6 is 3 (9 divided by 6 is 1 with a remainder of 3).

Diffie and Hellman are credited with a widely-used algorithm to validate identity by usage of remainder modulo operations. In this algorithm, actors in send messages to each other encoded with their private keys and arrive at the same number (Kozierok 2017). This is then used to perform encryption on data. The basic DH key exchange is shown below in Figure 4.

Figure 4. DH Rules and Example

RULES		EXAMPLE	
<u>Alice</u>	<u>Bob</u>	<u>Alice</u>	<u>Bob</u>
Alice & Bob share a Prime number q & an integer α , such that $\alpha < q$ & α is a primitive root of q	Alice & Bob share a Prime number q & an integer α , such that $\alpha < q$ & α is a primitive root of q	$q = 353$ $\alpha = 3$	$q = 353$ $\alpha = 3$
Alice generates a private key X_A such that $X_A < q$	Bob generates a private key X_B such that $X_B < q$	$X_A = 97$	$X_B = 233$
Alice calculates a public key $Y_A = \alpha^{X_A} \bmod q$	Bob calculates a public key $Y_B = \alpha^{X_B} \bmod q$	$Y_A = 3^{97} \bmod 353 = 40$	$Y_B = 3^{233} \bmod 353 = 248$
Alice receives Bob's Y_B	Bob receives Alice's Y_A	$Y_B = 248$	$Y_A = 40$
Alice calculates shared secret key $K = Y_B^{X_A} \bmod q$	Bob calculates shared secret key $K = Y_A^{X_B} \bmod q$	$K = 248^{40} \bmod 353 = 160$	$K = 40^{248} \bmod 353 = 160$

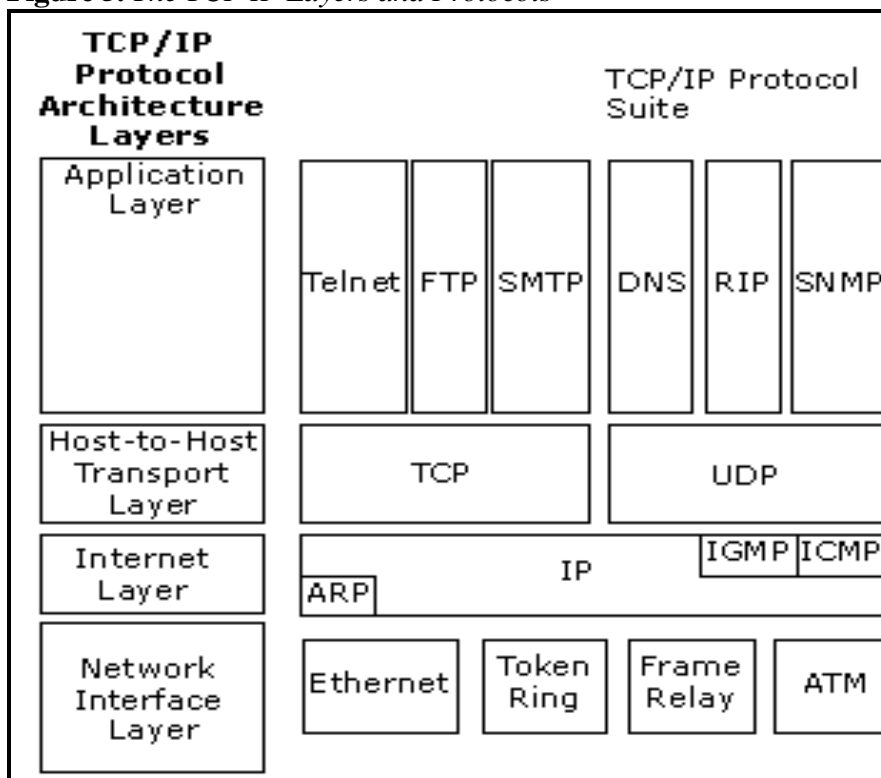
Source: adapted from Stallings (2018).

This article will use a similar approach to conveying trust to other members except that the algorithm to decode the primary message will be regenerated in different binary operations that will be stored along the blockchain's historical blocks.

TCP/IP Concepts

A key assumption of the model in section "Model Heuristics and Base Operations" relies on the usage of TCP/IP as described in Kozierok (2017). The operation of that set of protocols assumes the disaggregation of a message, transmission through physical media and aggregation in the destination. In summary, messages are prepended with routing and lower level information as the data travels down the stack. They are finally transmitted through the physical layer and are de-constructed by each of the layers until they arrive at the application. We are particularly concerned in the handshake that will take place at the with the PPP (point to point) sub-protocol of the ICMP protocol shown in Figure 5.

Figure 5. *The TCP IP Layers and Protocols*



Source: compnetworkingsec.com.

The PPP dialogue is established at the start of a session and it allows for the usage of CHAP a more modern version of authentication that can be used on the internet layer segment of the protocol. When the two machines are establishing a joint session, the following dialogue occurs:

1. Machine A sends PPP frames to the target address on the network.
2. The receiving Machine B can respond in one of three ways:

Configure-ACK: parameters accepted, acknowledge and continue.

Configure-NAK: parameters rejected (and which ones).

Configure-Reject: ignore.

Challenge (if challenge met, then ACK).

Section “Model Heuristics and Base Operations” contains a specific example of how the protocol tool set is deployed within the model.

Model Heuristics and Base Operations

In this section, the base matrix, the blockchain components and the base operations are discussed.

The Base Matrix

The first thing proposed in this model is a base matrix that has five columns and contains 4096 rows (more or less data points can be used). Each line contains the following column components:

- The sequence number (“N”).
- The private key used in that sequence number (“P”).
- The secret key in that sequence number (“Q”).
- The gate used in that sequence number (“G”).
- The public key in that sequence number (“X”).

The base matrix structure is shown in Table 1. The actual matrix values have only binary numbers (0 or 1). The sequence is assumed by location.

Table 1. Sample Matrix Structure

P	Q	G	X	N
<i>F (0)</i>	T (1)	00(XOR)	T (1)	0
.
<i>T (1)</i>	F (0)	01(XNOR)	T (0)	4095

The first line above has the components of P:F(0), Q:T(1), G:00(XOR), X:T(1), N:0. Those values correspond to using the XOR gate on inputs 0,1 and obtaining the number 1. This matrix is never fully implemented in any block on the blockchain rather it is computed by the members each time the members validate each other before beginning exchange of messages.

Blockchain Components

The blockchain components are included in this section.

Blockchain Block

The blockchain block is described in Table 2 and discussed immediately following it.

Table 2. The Model's Blockchain Block

Component	Contents
Epoch ID	Sequential number for the epoch
Manager secret key and epoch	4096 bit key + original epoch of admission
Public key	4096 bit key generated by manager for the epoch
Gate sequence	4096 x 2 bit key corresponding to the gate being used
Admitted Secret Keys	Sequences of 4096 bits for new members
Deprecated epoch/keys	Deprecated sequences of previous members
Current hash	Previous hash XOR public key XOR gate sequence XOR manager epoch XOR manager secret key XOR current epoch XOR nonce

In Table 2, the epoch id corresponds to the time period of operation (this can be a sequential number or can include the sequential time number and the time clock where the epoch began or variation thereof). The manager key and epoch are the secret key assigned to the manager upon admission and the epoch in which that operation was performed. The public key is the bit sequence of 4096 digits assigned by the manager corresponding to the epoch. The gate sequence is the sequence of 4096 gates corresponding to 2 bits for designating one of 6 binary gates for the epoch being communicated and is optional (if not noted, then the previous epoch's is assumed carried forward). The admitted secret keys are the new members' secret keys for the epoch and must be unique for the epoch, while the next line (deprecated key) corresponds to original epoch and secret key of the members that are being removed. The current hash is a secret number that is known to members to conclude the epoch. All of the above are generated by the manager.

Blockchain Operations

The blockchain operations that are required for this algorithm consist of the consensus method enabled through the manager, the epoch, the election, administrative tasks and conclusion of the epoch. This algorithm relies on epochs and randomization of their duration as explained in Medellin and Thornton (2017). The current manager at random selects a manager for the next epoch, directs when that epoch will begin and produces the next key components of the blockchain. The following paragraphs explain the concepts in greater detail.

The consensus method is mathematical and is enabled by the random election of a member to perform the duties necessary in the next epoch. A recommended approach is to elect at a minimum one manager and one alternate (which will "wake up" sometime after the manager had to have operated and will assume the duties if one has not done so). Additional alternate managers can be designated in order to increase robustness.

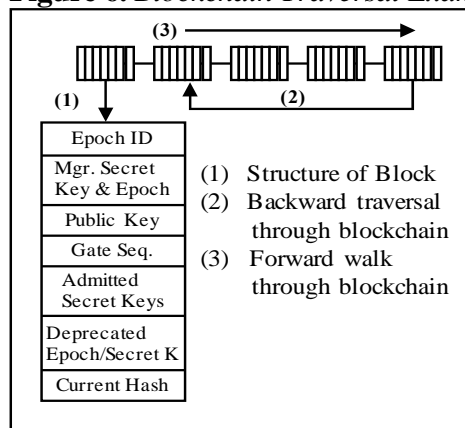
The manager is notified by the previous epoch manager as part of the conclusion of their duties. This previous manager has executed a randomized election by generation of random numbers, partitioning of previous admittances in to a continuous space, assignment of numbers and then assignment to one manager and n-number of alternate managers with instructions to wake up at a random-generated time in the future to execute the next epoch. As mentioned above, the election of a new manager is supervised by the existing manager and is done by announcing the election (for example through individual point to point to all IPv6 addresses or member IDs admitted but not deprecated in the chain). This communication dialogue requests their participation, not all machines need to participate, however those that can must; selection will be from the acknowledging members.

The echo of the machines will be to provide the difference between their secret key total and a random number generated times 4095. The closest (meaning the one with the least numeric difference to that number generated by the manager) and next closest will be assigned as the manager and alternate for the next epoch (if only one alternate is to be used). Only they will be notified of their role and a set of gates will be configured in their IoT arrays to correspond to the

logic needed to become a manager as the conclusion of the existing epoch is being executed (for execution of duties in the next epoch). Notification of new parameters will happen in broadcast for those that are in that communication mode, otherwise adjacent machines will be used in the IP protocol to bring themselves current (Kozierok 2017).

As mentioned above, the manager is responsible for execution of the administrative tasks of generating a new Public key and generation of new gate sequences. Typically, both of these will not be done in a single epoch, only occasionally will the gate sequence be targeted for regeneration. Based on that data, the members will re-generate their internal secret key in the base matrix to reflect the current epoch. The model relies heavily on the ability to traverse through the blockchain in order to ensure proper results, this is shown in Figure 6.

Figure 6. Blockchain Traversal Example



Admission and deprecation of participants will follow a similar process to what other blockchain algorithms indicate. This will depend on the actual blockchain software to be used (the “fabric”) (Xu et al. 2017). But those duties will also be administered by the manager. After these tasks, the manager will become dormant and the epoch will continue until a new one is declared by new managers or alternates.

Implementation in TCP/IP PPP and TCP/IP CHAP

The preferred method of implementation is by usage of the PPP and CHAP Protocols. PPP initiation begins with first message frames sent containing the user name and password. Once that has been initially validated, the responding machine would send back a challenge using CHAP (challenge/acknowledge). If that challenge was correct then an acknowledgement would occur and the two machines would use private keys to encrypt messages.

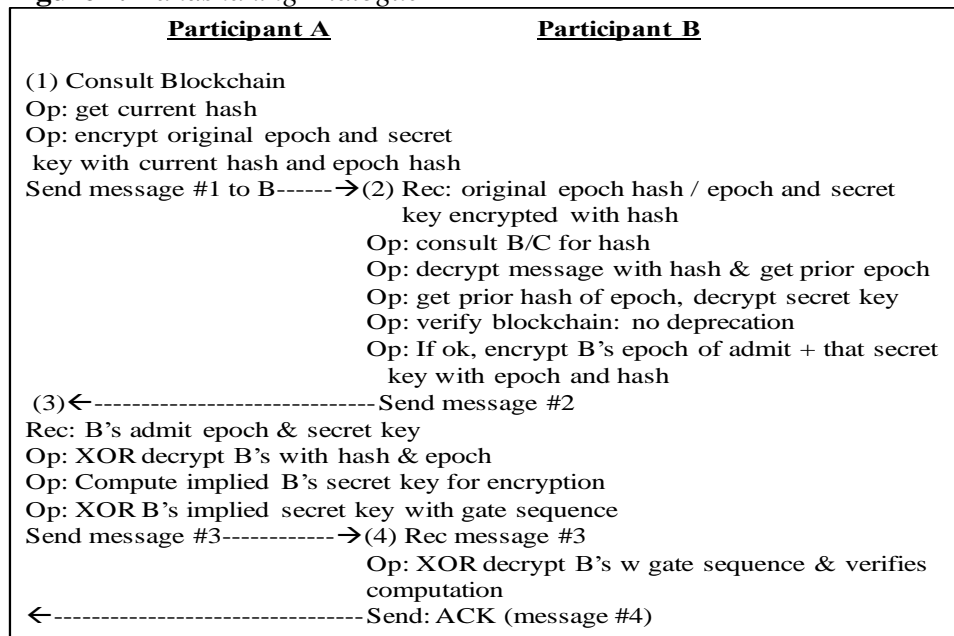
Initial Dialogue Between Members

If two members have not previously communicated or have done so in an outdated time frame they must establish trust. The objective of the initial dialogue between two members will be to validate the two parties and establish trusted communication between them. This process is modeled in TCP/IP because it is

probably the most utilized of communication protocols in modern computing and because of its inherent robustness in modeling dialogues on the internet (Kozierok 2017). This example dialogue is provided for illustrative purposes, many other approaches are valid as well. The steps are as follows (it assumes no regeneration of the gate sequence, see Figure 7 also):

1. Participant A consults their blockchain store for the current hash. Participant A sends their original epoch of admittance hash XOR encrypted with the current hash (as a user name) and their original admission secret key XOR encrypted with that epoch's hash (as a password) in message #1 through TCP/IP PPP.
2. Participant B XOR decrypts message #1 with the current hash (for a prior epoch hash) and looks for A's admission secret key in that epoch and any possible deprecation since. If it has been deprecated the process stops. B prepends their epoch of admission key to their admission secret key and XOR encrypts with the current hash prepended with the current epoch and sends that as a challenge to A.
3. Participant A receives message #2 and XOR decrypts the value of B's admission epoch and secret key. It then uses that computed secret key as the encryption key. A next XOR encrypts the computed encryption with the current gate sequence and sends to Participant B as reply to the challenge in message #3.
4. Participant B receives message #3 and XOR decrypts with the current gate sequence. If it matches the encryption key sent then an acknowledge is sent and handshaking is over.

Figure 7. Handshaking Dialogue



Guide: Op=Operation, Send=Transmit, Rec=Receive.

Regeneration of Keys

A critical aspect of the model is the ability to regenerate the secret key for each member through instruction to do so from an existing manager. The secret key for members may be regenerated by taking their private key, the gate sequences and the public key. In addition to regeneration of the secret key through public keys, regeneration of the secret key could be done through usage of new gate sequences instead of the public key (input would be the private key, the public key and a new gate sequence for a new secret key).

Another area of expanded regeneration in this model is the ability to stack the gated algorithm and instead of using one set of gates one would use multiple sets of gate sequences in parallel to add further complexity protection. These areas have not been researched at the moment and are expected to be further detailed at a future point in additional research.

Attack Resiliency

A protection scheme's ability to resist intrusion depends on how robust the scheme is and how potentially dangerous such exploits are to the correct functioning of the protected asset (Knapp and Langill 2015). A powerful aspect of the model documented in this article is the ability to increase or decrease the mathematical frequency and payload of the keys used to validate identity. In some cases, the requirement may be for a very high level of protection and in some it will not require as much. This translates into more computational abilities required to fulfill them and therefore more resources (Arnberg et al. Patent Application).

In the two subsections below these implications are discussed by using the base matrix of 4096 rows and 4 columns described above and testing against the probability of a brute-force attack (one in which all possible payloads are used). In the second subsection, additional variations are discussed to further complicate the attack surface.

Attacks on the Previously-Described Base Matrix

Previous segments have described a 4 by 4096 binary base matrix. In order for the attacker to begin an attack, they must have a valid secret key of admission, that epoch's hash, the prior epoch hash and the current epoch's hash. All of these are binary arrays of 4096 rows and the attacker would have to guess these correctly (see Table 3 for attack success probabilities).

Table 3. Brute Force Attack Success Probabilities

#	P(x) Secret Key	P(x) Hash Key	P(x) Epoch Hash	P(x) Epoch	P(x) Combined
1	1 / (2 ⁴⁰⁹⁶)	1 / (2 ⁴⁰⁹⁶)	1 / (2 ⁴⁰⁹⁶)	1 / (2 ⁴⁰⁹⁶)	1 / Extremely high #
2	1 / (2 ²⁰⁴⁸)	1 / (2 ²⁰⁴⁸)	1 / (2 ²⁰⁴⁸)	1 / (2 ²⁰⁴⁸)	1 / Extremely high #
...
128	1 / (2 ³²)	1 / (2 ³²)	1 / (2 ³²)	1 / (2 ³²)	1 / (2 ^{1,048,576})
256	1 / (2 ¹⁶)	1 / (2 ¹⁶)	1 / (2 ¹⁶)	1 / (2 ¹⁶)	1 / (2 ^{65,536})
512	1 / (2 ⁸)	1 / (2 ⁸)	1 / (2 ⁸)	1 / (2 ⁸)	1 / (2 ^{4,096})
1024	1 / (2 ⁴)	1 / (2 ⁴)	1 / (2 ⁴)	1 / (2 ⁴)	1 / (2 ²⁵⁶)
1536	1 / (2 ³)	1 / (2 ³)	1 / (2 ³)	1 / (2 ³)	1 / (2 ⁸¹)
2048	1 / (2 ²)	1 / (2 ²)	1 / (2 ²)	1 / (2 ²)	1 / (2 ¹⁶)

Table 3 depicts the number of machines (#) and the combined probabilities of success in initiating a brute force attack in a static protection scheme if the model was never regenerated through a new gate sequence or new primary keys. In this case, the protection level might be adequate for somewhere around 1,500 to 1,900 IoT machines; the raw probability numbers for the 1,536 members is in one in 242 sextillions which would be an extremely high level of protection in most cases. In addition, however, a key aspect of this paper's contribution is the ability to vary and regenerate parameters based on epochs which will add further complexity and protection versus attacks; that will be discussed next.

The Dynamic Nature of the Model

Upon admission of a new member into the network, the manager will generate a private key consisting of a binary value list (for example, 4096 as per the description above) and will compute the value of the member's secret key by taking the generated private key with the epoch's public key as inputs and using the existing gate sequence. The private key and the blockchain payload thus far will be communicated to the newly admitted member. The secret key will be published in the epoch's blocks.

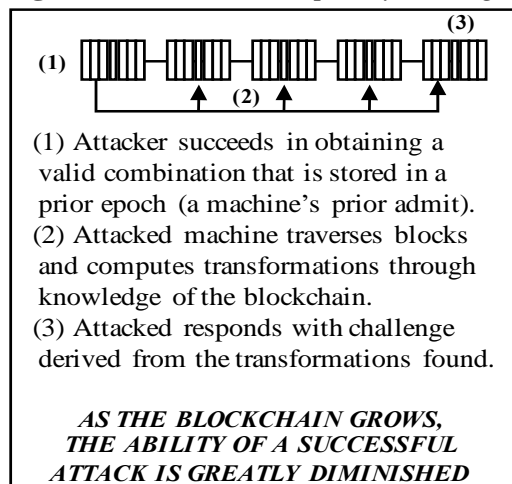
One of the duties of a manager is to publish a new public key in each epoch (a new set of gates can also be published). Each member has the responsibility of regenerating their current secret key by using their private key and the new public key as inputs to the gate sequence. This current secret key is crucial in the hand-shaking algorithm. As discussed above, the frequency of epochs is a random variable selected by the current manager; the manager at random (within tolerances of the number of members and the volume/speed of the network) will announce when the next epoch will begin to the next manager/alternate(s).

The regeneration of the secret keys during every epoch by every member creates another layer of computational complexity for an attacker. Similar to the added complexity afforded by the SHA algorithms this incremental iterative requirement is significant since not only must the attacker know the current parameters but be able to traverse the blockchain in order to continue the dialogue with the intended machine (Stallings 2018). Even if the brute force attack is successful in generating sequence of relevant keys the attacker must have knowledge of the blockchain in order to respond to the challenge. The traversal of

blocks is very necessary in order to be able to respond, an incorrect response is ignored and the machine under attack simply does not continue.

As more epochs occur and more blocks are added to the blockchain the added complexity for lack of knowledge will be overwhelming on the attacker. The attacker will need to have intimate knowledge of prior epochs going back to the attacked machine's admission in order to respond (including if there are deprecations of that machine or if gate sequences have been regenerated). The distance of these transformations will increase in similar fashion as that described in the SHA protocol transformations (at one point will exceed the number of transformations in SHA by the additional epochs beyond the transformations in the particular SHA version being used) (Stallings 2018). A diagram of this distancing process can be seen in Figure 8, if gate change or deprecation events are introduced they will require either evaluation or regeneration of private keys further adding complexity for the attacker

Figure 8. Increased Complexity Through More Blockchain Blocks



Resource Consumption Evaluation

This section presents a simulation experiment on the model.

Formal Requirements

The formal requirements are included in the appendix and heavily rely on the **Z** language (pronounced z-ēd) and is included in the appendix.

Experimental Model Construction

The experimental model focuses on simulating a very simple Modbus/TCP IoT Operational Technology (OT) network as described in Bartelt (2011) and includes the following messages:

- Device status (90 messages).
- Correction sequence (13 messages).
- Correction feedback acknowledge (13 messages).
- Additional 116 messages distributed at random (twice the amount of the previous 3) over the 90-day period.

The simulation is executed in quarter year intervals for a 5-year period, and calculates the cpu cycles required for different size key exchanges. One is for a 512-bit sequence (a smaller subset of the 4096 previously described), another is for the 4096-bit sequence and a third is for 512 bytes. The third is introduced to compare to SHA 384 or higher order SHA protocols.

The simulation for the model described in this document assumes the load of 16 epochs with evenly distributed machines until 96, 192 and 384 machines are admitted into the blockchain eco-system for the bit-based keys. The 512- decimal simulation admits 96, 192 and 384 in one load operation for each instantiation. Keys are regenerated every quarter year, 2% of the machines are admitted and deprecated every period and there are up to $116 \times 2 = 232$ key exchanges per machine per period. D-RAFT elections are not included in the simulation since they only impact one machine (except for the acknowledgement from the participant machines).

Estimation of Non-Volatile Storage Requirements

The usage of blockchain requires the provision of non-volatile storage where the blocks will reside. A critical assumption of the blockchain model is the ability to replicate the data in all the devices that are participants in the network. This characteristic requires estimation of the storage requirements for each (a function of the number of devices, the structure of the blockchain blocks and the number/types of blocks that will be added to the blockchain as operations occur). The model requires that admission keys be stored, new public keys and gate sequences, deprecation of keys and finally the items which are required for management (the manager key/admission epoch, the epoch ID and the current hash). Table 4 identifies the storage requirements for the 96, 192 and 384-member machine networks. It estimates the initial load and then estimates the addition/ deprecation of 2 devices a quarter for every 96 devices. The summary lines at the bottom identify the non-volatile storage requirements for the blockchain at the quarter, year and 5 year marks only for the bit-based keys (the totals are rounded up to ensure the blocks will be written).

Table 4. Base Load & Operating Store Non-volatile Storage Requirements per Device

Base Load Store Component		Blockchain		Base Load					
Item	Assumption	512 bit	4096 bit	512 bit	4096 bit	512 bit	4096 bit	512 bit	4096 bit
# Devices >>>	16 Epochs			96	96	192	192	384	384
Epoch	key length	512	4096	8,192	65,536	8,192	65,536	8,192	65,536
Mgr. Key+Epoch	32 + key bits	544	4128	8,704	66,048	8,704	66,048	8,704	66,048
Primary Key	key length	512	4096	8,192	65,536	8,192	65,536	8,192	65,536
Gate Sequence	key length	512	4096	0	0	0	0	0	0
Admit Secret Key	key length	512	4096	49,152	393,216	98,304	786,432	196,608	1,572,864
Deprecated Key	32 + key bits	544	4128	0	0	0	0	0	0
Current Hash	key length	512	4096	8,192	65,536	8,192	65,536	8,192	65,536
Total bits				82,432	655,872	131,584	1,049,088	229,888	1,835,520
Total bytes				10,304	81,984	16,448	131,136	28,736	229,440
Expressed in KB				10.3	82	16.5	131.2	28.7	229.4
Operating Store Component		512 bit	4096 bit	Regeneration, Admission & Deprecation @ 20 mach./qtr.					
Time Period >>>				Quarter	Quarter	Year	Year	5 Year	5 Year
Epoch	32 bits	32	32	32	32	128	128	640	640
Mgr. Key+Epoch	32 + key bits	544	4128	544	4,128	2,176	16,512	10,880	82,560
Primary Key	key length	512	4096	512	4,096	2,048	16,384	10,240	81,920
Gate Sequence	key length	512	4096	0	0	0	0	0	0
Admit Secret Keys	key length	512	4096	1,024	8,192	4,096	32,768	20,480	163,840
Deprecated Keys	32 + key bits	544	4128	1,088	8,256	4,352	33,024	21,760	165,120
Current Hash	key length	512	4096	512	4,096	2,048	16,384	10,240	81,920
Total bits				3,712	28,800	14,848	115,200	74,240	576,000
Total bytes				464	3,600	1,856	14,400	9,280	72,000
Expressed in KB				0.5	3.6	1.9	14.4	9.3	72
Storage per machine for # machines on network				Q/512	Q/4096	Y/512	Y/4096	5Y/512	5Y/4096
96 Devices (KB)				10.8	85.6	12.2	96.4	19.6	154.0
192 Devices (KB)				19.1	151.2	26.8	211.4	68.0	532.2
384 Devices (KB)				35.5	282.3	55.9	441.2	164.7	1288.3

Estimating CPU-Cycle Requirements

The estimated CPU-cycle requirements for three different scenarios (512 binary array, 4096 binary array and SHA 384+) are given in Table 5 (a description of the assumptions follows).

Table 5. Estimated CPU-Cycle Loads Under Various Keys

	512 bits	4096 bits	SHA 384+
Message #1			
Receive	1	1	1
Decode	32	256	0
Fetch Block	2	2	0
Validate/Derive	16	128	512
Format Challenge	16	128	512
Message #3			
Receive	1	1	1
Decode	32	256	0
Validate/Derive	16	128	512
Acknowledge	1	1	1
Total CPU Cycles	117	901	1,539

Table 5 identifies the number of cycles required for each operation under the dialogue mentioned in Figure 7. The assumptions made for each are as follows:

- Receive: one cycle to receive the message (store in buffer).
- Decode: for the bit-based keys it is two messages (user name and password) using a 32-bit chip, bitwise operations (e.g., $(512/32) * 2 = 32$ CPU-cycles).
- Fetch block (from the block chain): one for fetch and one for the receive.
- Validate/Derive: bit-wise operations similar to the ones in decode for the bit keys, 512 -digit division for the SHA key.
- Format Challenge: same as previous operation.
- Acknowledge: one cycle to send standard “ACK” message.

Results Discussion

The results may be found in the appendix are for a low interaction system (in practice the interactions in process control may be much higher). In addition, the frequency of key negotiation will depend on the ability to isolate the processes from potential attack and the necessity to regenerate encryption keys. Those considerations will need to be evaluated by the designer of the system in addition to the specific component of the blockchain itself. This document has provided one example of the gated component but the variations to the payloads in the model are very large.

An important concept illustrated above is the radical difference in cpu cycles depending on the algorithm used for generation and regeneration of keys between IoT devices. Some of these may be able to devote a high degree of cycles as for example in the ARM Cortex-M0 Processor which can yield a 0.87 MIPS (million instructions per second) at a speed of 2.25MHz and is a three-stage cycle processor². Given a typical 20% “headroom” (additional processing unused) it can deliver around 0.232 million full instruction capacity and a simple key negotiation would not begin to scratch the surface. However, more cycles would be required if the SHA negotiation were something more resilient such as prime number keys (something that is utilized in higher safety systems for example).

In addition, however, there are other processors that have considerably less power such as those mentioned in Lallement et al. (2017) which may still be industrially viable but with much less cpu power (e.g., 7Hz) to devote to protection. These processors do exist in implementations and need more care in determining which protection algorithm to use so they do not spend most of their effort in processing large keys.

²https://static.docs.arm.com/ddi0432/c/DDI0432C_cortex_m0_r0p0_trm.pdf?_ga=2.84689169.908795371.1542781838-925179195.1542781838. [Accessed 17 March 2021]

Potential in Other Technologies

Section “Resource Consumption Evaluation” assumed that the IoT processors will physically process the instructions required. In addition, it has assumed that the regeneration of the keys is evenly distributed (at least through the experiment) and can count on a static space where adversaries can try to hack into the system. This section discusses potential variations in cloud computing and the ability to provide some resilience in quantum processor attacks through randomization.

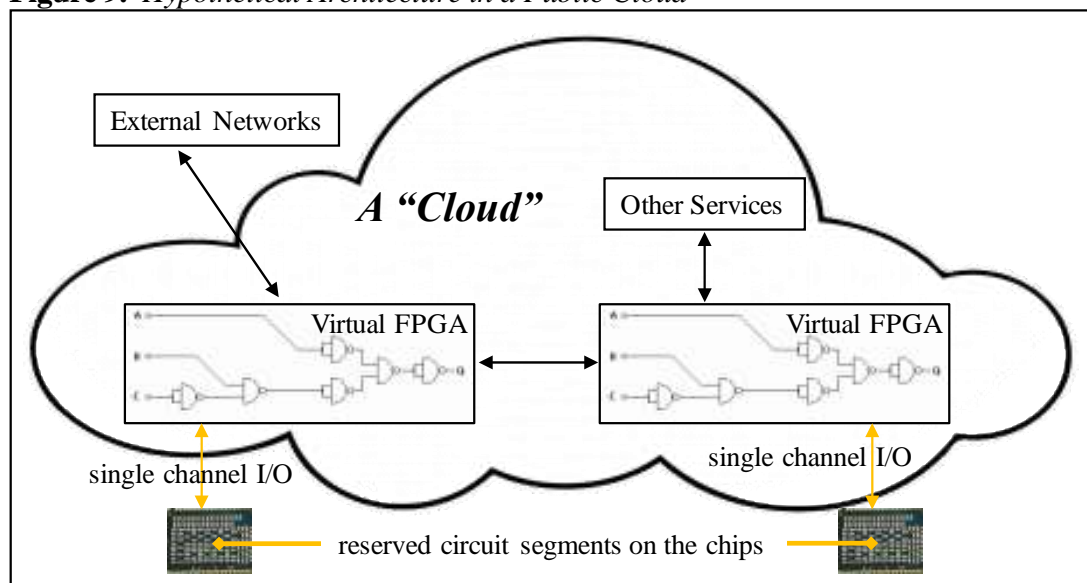
Cloud Computing

Cloud technology affords great flexibility and efficiency in managing computing resources. What used to cost millions and take years to build can now be achieved in fractional time and cost. Cloud computing can help in this model by providing logic-gated arrays in virtual clouds.

These “virtual gated arrays” (sometimes also called “FPGA” or Field Programmable Gated Arrays) can be designed with gated sequences in mind and can also be scaled to address the needs of a particular project with little effort or time. Virtual FPGAs as they are called can now be sourced from many of the public clouds and instead of having to purchase the hardware, one can now design in that environment and deploy very quickly and inexpensively.

Figure 9 illustrates a potential implementation of the algorithm in Virtual FPGAs, taking the load off the IoT processors themselves by managing all communication (and protection) in the cloud while delivering payloads in a secure, isolated channel. Several offerings exist to both house the processors in a virtual environment and also the blockchain operations in public clouds (such as Amazon Web Services).

Figure 9. Hypothetical Architecture in a Public Cloud



Quantum Computing

Quantum computing is a promising technology enabling massive processing in fractional time. Peter Shor introduced an algorithm that was able to overcome the finding of such primes considered later useful in deciphering the SHA style cryptography. This was later confirmed by Spiller in finding such prime numbers using Shor's algorithm. While not commercially viable at this point, in the future these designs could potentially find answers to primary key exchanges and cryptography fractions of what it takes today.

Prime numbers are finite & finding them can be quite complex. Several algorithms exist to confirm the existence of primality (Xu et al. 2017, Nakamoto 2019). It is conceivable that a quantum computer could break the secrets of the model presented in this article. However, one must also consider that the algorithms can be regenerated at random intervals adding infinity to the puzzle. Others such as those documented in sub-subsection "Regeneration of Keys" can be used to randomize and also confuse the attacker requiring them to initiate again (and on, and on....).

One additional word on the above, the regeneration of keys consumes additional resources and one must not be careless to fall into regeneration in intervals that are very frequent because that is wasteful. Rather, one needs to design the system with an analysis of the attacker strength and provide for sufficient regeneration in order to defeat it. In the end however, if a sufficiently powerful quantum computer is used, these efforts might not be enough.

Conclusion

This document presented a method for interaction between logic gates, blockchain and key generation that has some definite savings in computation for the IoT. This is an initial discussion on a new approach to key generation and regeneration. Risk areas still exist in this method and they are being explored as this document is being submitted for consideration. The author believes in adequate protection based on the asset values and potential for real intrusion. This document advocates for a different approach that can increase or decrease computational complexity (and resources) depending on the protection objectives.

References

- Arnberg A, Van Ermel Scherer R, Medellin J (n.d.) *Device for implementing ubiquitous connectivity and protection software for IoT devices*. US Patent Application 62/371,003.
- Bartelt T (2011) *Industrial automated systems; instrumentation and motion control*. Clifton Park, New York: Delmar Cengage Learning.
- Christidis K, Devetsikiotis M (2020) Blockchains and smart contracts for the internet of things. *IEEE Access* 4(1): 2292–2303.

- Dinh TTA, Wang J, Chen G, Liu R, Ooi BC, Tan K-L (2017) *BLOCKBENCH: a framework for analyzing private blockchains*. Retrieved from: <https://arxiv.org/pdf/1703.04057.pdf>. [Accessed 19 March 2019]
- Dorri A, Kanhere SS, Jurdak R (2017a) Towards an optimized blockchain for IoT. In *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 173–178.
- Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2017b) Blockchain for IoT security and privacy: the case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 618–623.
- Ferguson N, Schneier B, Kohno T (2010) *Cryptography engineering, design principles and practical applications*. Indianapolis, Indiana: Wiley Publishing, Inc.
- Huang S-Y, Cheng K-T (2002) *Formal equivalence checking and design debugging*. Norwell, Massachusetts: Kluwer Academic Publishers.
- Johnsonbaugh R (2018) *Discrete mathematics*. 8th Edition. New York: Pearson Education, Inc.
- Knapp E, Langill J (2015) *Industrial network security, securing critical infrastructure networks for smart grid, SCADA and other industrial control systems*. 2nd Edition. Waltham, Massachusetts: Syngress Elsevier.
- Kozierok C (2017) *The TCP/IP guide, a comprehensive, illustrated internet protocols reference*. San Francisco, California: No Starch Press, Inc.
- Lallement G, Abouzeid F, Cochet M, Daveau J-M, Roche P, Autran J-L, et al. (2017) *A 2.7pJ/cycle 16MHz with 4.3nW power-off ARM Cortex-M0+ core in 28nm FD-SOI*. Leuven, Belgium: ESSCIRC, hal-01788172.
- Li D, Du R, Fu Y, Au MH (2019) Meta-key: a secure data-sharing protocol under blockchain-based decentralized storage architecture. *IEEE Networking Letters* 1(1): 30–33.
- Liang X, Wu T (2017) Exploration and practice of inter-bank application based on blockchain. In *The 12th International Conference on Computer Science & Education (ICCSE 2017)*, 219–224.
- Medellin J, Thornton M (2017) Simulating resource consumption in three blockchain consensus algorithms. In *“MSV ‘17” International Conference on Modeling, Simulation & Visualization Methods*, 21–27.
- Medellin J, Thornton M (2018) Performance characteristics of two blockchain consensus algorithms in a VMWare hypervisor. In *International Conference on Grid & Cloud Computing and Applications “GCA ‘18”*, 10–17.
- Monk S (2017) *Programming FPGAs, getting started with Verilog*. New York: McGraw Hill.
- Muralidharan S, Murthy C, Nguyen B, et al. (2018) Hyperledger fabric: a distributed operating system for permissioned blockchains. Retrieved from: <https://arxiv.org/pdf/1801.10228.pdf>. [Accessed 19 March 2019]
- Nakamoto S (2019) *Bitcoin: a peer-to-peer electronic cash system*. Retrieved from: www.bitcoin.org. [Accessed 19 March 2019]
- Ongaro D, Ousterhout J (2014) In search of an understandable consensus algorithm. In *Proceedings ATC’14 USENIX Annual Technical Conference USENIX*, 305–319.
- Salman T, Zolanvari M, Erbad A, Jain R, Samaka M (2018) Security services using blockchains: a state of the art survey. *IEEE Communications Surveys & Tutorials* 21(1): 858–880.
- Soni J, Goodman R (2017) *A mind at play, how Claude Shannon invented the information age*. New York: Simon & Schuster.

- Spivey J (1988) *Understanding Z, A Specification Language and its Formal Semantics*. Cambridge, UK: Cambridge University Press.
- Stallings W (2018) *Cryptography and network security, principles and practice*. 7th Edition. London, United Kingdom: Pearson Education Limited.
- Xu X, Weber I, Staples M, Zhu L, Bosch J, Bass L, et al. (2017) A taxonomy of blockchain-based systems for architecture design. In *2017 IEEE International Conference on Software Architecture*, 243–252.

Appendix

A1. Formal Requirements Definition

This section outlines the basic formal requirements for implementation of the blockchain model. The schemas and operations are enumerated and then the key ones are formally described in **Z**.

A1.1 Schemas and Operations

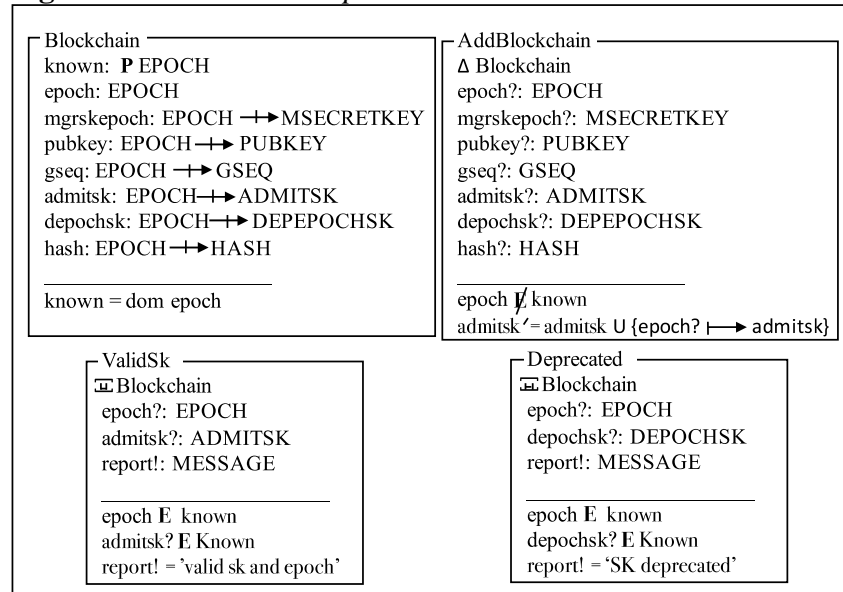
The specification is based on schemas (collections of data primitives) and change operations (dynamic effects) on those schemas. The schemas and operations for the blockchain and member segments of the system are as follows, a checkmark appears next to each if they will be used in the evaluation:

- Schema: Blockchain ✓ & Operation: AddBlockchain ✓
- Schema: Message1 & Operation: Message1CreateSend
- Operation: Message1Validate ✓
- Schema: Message2 & Operation: Message2CreateSend ✓
- Schema: Message3 & Operation: Message3CreateSend
- Schema: Message4 & Operation: ACK4CreateSend ✓

A1.2 Sample Schemas and Operations in Detail

The following **Z** language sample definitions are from the complete specification (it is voluminous and will be published in the future). The **Z** language guarantees the correctness of the specification by mathematical proofs and only those artifacts are translated into actual code (Spivey 1988).

Figure 10. Schemas and Operations in Z



A2. Simulation and Results

A structured simulation was constructed in the c language using the gcc compiler in Linux using the -o option. The simulation was run for 20 quarters using the method described. Three key lengths were used (512 & 4096 bit binary and SHA 384+, assumed at 512 byte), the results are in Table 6.

Table 6. *Simulation Results; Key Negotiation for a Single Member*

KEY NEGOTIATION AND CPU CYCLE RESULTS FOR 20 QUARTERS				
Quarter 1	Keys Negotiated = 220	512bit= 25740	4096bit= 198220	sha= 338580
Quarter 2	Keys Negotiated = 170	512bit= 19890	4096bit= 153170	sha= 261630
Quarter 3	Keys Negotiated = 198	512bit= 23166	4096bit= 178398	sha= 304722
Quarter 4	Keys Negotiated = 187	512bit= 21879	4096bit= 168487	sha= 287793
Year 1	Keys Negotiated 775	512bit= 90675	4096bit= 698275	sha= 1192725
Quarter 5	Keys Negotiated = 119	512bit= 13923	4096bit= 107219	sha= 183141
Quarter 6	Keys Negotiated = 169	512bit= 19773	4096bit= 152269	sha= 260091
Quarter 7	Keys Negotiated = 129	512bit= 15093	4096bit= 116229	sha= 198531
Quarter 8	Keys Negotiated = 231	512bit= 27027	4096bit= 208131	sha= 355509
Year 2	Keys Negotiated 648	512bit= 75816	4096bit= 583848	sha= 997272
Quarter 9	Keys Negotiated = 204	512bit= 23868	4096bit= 183804	sha= 313956
Quarter 10	Keys Negotiated = 158	512bit= 18486	4096bit= 142358	sha= 243162
Quarter 11	Keys Negotiated = 169	512bit= 19773	4096bit= 152269	sha= 260091
Quarter 12	Keys Negotiated = 146	512bit= 17082	4096bit= 131546	sha= 224694
Year 3	Keys Negotiated 677	512bit= 79209	4096bit= 609977	sha= 1041903
Quarter 13	Keys Negotiated = 117	512bit= 13689	4096bit= 105417	sha= 180063
Quarter 14	Keys Negotiated = 143	512bit= 16731	4096bit= 128843	sha= 220077
Quarter 15	Keys Negotiated = 120	512bit= 14040	4096bit= 108120	sha= 184680
Quarter 16	Keys Negotiated = 172	512bit= 20124	4096bit= 154972	sha= 264708
Year 4	Keys Negotiated 552	512bit= 64584	4096bit= 497352	sha= 849528
Quarter 17	Keys Negotiated = 192	512bit= 22464	4096bit= 172992	sha= 295488
Quarter 18	Keys Negotiated = 222	512bit= 25974	4096bit= 200022	sha= 341658
Quarter 19	Keys Negotiated = 169	512bit= 19773	4096bit= 152269	sha= 260091
Quarter 20	Keys Negotiated = 153	512bit= 17901	4096bit= 137853	sha= 235467
Year 5	Keys Negotiated 736	512bit= 86112	4096bit= 663136	sha= 1132704
Year 5 Cum.	Keys Negotiated 3388	512bit= 396396	4096bit= 3052588	sha= 5214132

The results in Table 6 are for a single member. This simulation is for a very low requirement in a particular IoT network (for example low risk refrigerated warehouse with zones that vary minimally or for a set of refrigerators in long term storage that do not require daily operation).

The Fixpoint Combinator in Combinatory Logic – A Step towards Autonomous Real-time Testing of Software?

By Thomas Fehlmann^{*} & Eberhard Kranich[±]

Combinatory Logic is an elegant and powerful logical theory that is used in computer science as a theoretical model for computation. Its algebraic structure supports self-application and is Turing-complete. However, contrary to Lambda Calculus, it untangles the problem of substitution, because bound variables are eliminated by inserting specific terms called Combinators. It was introduced by Schönfinkel (1924) and Curry (1930). Combinatory Logic uses just one algebraic operation, namely combining two terms, yielding another valid term of Combinatory Logic. Terms in models of Combinatory Logic look like some sort of assembly language for mathematical logic. A Neural Algebra, modeling the way we think, constitutes an interesting model of Combinatory Logic. There are other models, also based on the Graph Model (Engeler 1981), such as software testing. This paper investigates what Combinatory Logic contributes to modern software testing.

Keywords: combinatory logic, combinatory algebra, autonomous real-time testing, recursion, software testing, artificial intelligence

The Organon

Aristotle's legacy regarding formal logic has been transferred to us in a collection of his thoughts compiled into a set of six books called the *Organon* around 40 BCE by Andronicus of Rhodes or others among his followers (Aristoteles 367-344 BCE). The Organon with its syllogisms was the dominant form of Western logic until 19th-century advances in mathematical logic.

Engeler recently noted the apparent lack of something that we today consider fundamental for axiomatic geometry: relations. The question is why. Aristotle had the means of developing this concept as well; however, he chose not to do so.

Aristotle had the means of combining predicates. It is therefore possible to construct an adequate model for Aristotle's syllogism based on the structures of Combinatory Logic. Relations then become part of the model. Engeler shows that Aristotle had no need for relations because the main model he used – the Euclidean Geometry – does not require relations (Engeler 2020).

^{*}Senior Researcher, Euro Project Office AG, Switzerland.

[±]Senior Researcher, Euro Project Office AG, Switzerland.

Introduction

A model of Combinatory Logic is an algebraic structure implementing combinators in a non-trivial way. Such a model is called *Combinatory Algebra*. As a minimum, it contains implementations for the **I** combinator (identity), the **K** combinator for extracting parts of another term, and the **S** combinator that substitutes parts of a term by some other combinator. Another famous combinator is the *Fixpoint Combinator* **Y**, explaining recursion and possible infinite iteration. These specific combinators are represented as *Constants* in the language of Combinatory Logic, whereas other terms may contain *Variables*. These general terms are called *Combinatory Terms* (Bimbó 2012, p. 2); the combination of any two terms X and Y is written as $X \bullet Y$.

Given a problem as a term X in some suitable model, what should be its solution? A problem is something that displays specific behavior, sometimes unpredictable, and produces specific effects, often unwanted. Also, a certain persistence is part of a problem; problems that disappear by themselves are not particularly exciting.

A fixpoint point $Y \bullet X$ with the property that $Y \bullet X = X \bullet (Y \bullet X)$, for any term X of Combinatory Logic, is thus something like a solution to the problem X . You can apply the solution combinator **Y** as many times as necessary and the problem solution remains stable and confined.

When we encounter the problem of how to test a piece of software X , and we have a test suite $Y \bullet X$ with the fixpoint property, it looks like a solution to our testing problem. Since we can measure tests, by counting its test size, we can assess what means minimal effort for a test, and thus can get an optimum.

The clue to Combinatory Logic is that “everything is a function” – and indeed, a unary function. Whenever anything can be understood as function depending on two variables – $f(x, y)$ – it is an application of a unary function $g = f \bullet x$ on a variable y . Thus, $f(x, y) = g(y) = (f \bullet x) \bullet y = f \bullet x \bullet y$; always assuming association to the left. This is known as *Currying*, converting n-ary functions into a sequence of unary functions.

Combinatory Algebras

Combinatory Algebras are models of Combinatory Logic (Curry and Feys 1958, Curry et al. 1972). Such algebras are closed under a combination operation $M \bullet N$ for all terms of the algebra M, N ; and two distinct *Combinators* **S** and **K** can be defined with the following properties:

$$\mathbf{K} \bullet P \bullet Q = P \tag{1}$$

and

$$\mathbf{S} \bullet P \bullet Q \bullet R = P \bullet Q \bullet (P \bullet R) \tag{2}$$

where P, Q, R are elements in the combinatory algebra³.

Thus, the combinator **K** acts as projection, and **S** is a substitution operator for terms in the combinatory algebra. Like an assembly language, the **S-K** terms become quite lengthy and are barely readable by humans, but they work fine as a foundation for computer science.

The power of these two operators is best understood when we use them to define further, more manageable, and more reasonable combinators. Church (Church, 1941) presented a list of functions that can be implemented as combinators, and Zachos investigated them in the settings of Combinatory Logic (Zachos 1978). Bimbó (2012, p. 6) gives a good overview; however, without reference to the original contributors. We present here only a few.

Identity

The identity combinator is defined as

$$\mathbf{I} := \mathbf{S} \bullet \mathbf{K} \bullet \mathbf{K} \quad (3)$$

Indeed, $\mathbf{I} \bullet M = \mathbf{S} \bullet \mathbf{K} \bullet \mathbf{K} \bullet M = \mathbf{K} \bullet M \bullet (\mathbf{K} \bullet M) = M$. Association is to the left.

Functionality by the Lambda Combinator

Church's *Lambda Calculus* is a formal language that can be understood as a prototype programming language (see Church 1941, Barendregt 1977).

Lambda calculus can be expressed by **S-K** terms. We define recursively the *Lambda Combinator* \mathbf{L}_x for a variable x as follows:

$$\mathbf{L}_x \bullet x = \mathbf{I} \quad (4)$$

$$\mathbf{L}_x \bullet M = \mathbf{K} \bullet M \text{ if } M \text{ different from } x \quad (5)$$

$$\mathbf{L}_x \bullet M \bullet N = \mathbf{S} \bullet \mathbf{L}_x \bullet M \bullet (\mathbf{L}_x \bullet N) \quad (6)$$

The definition (5) holds for any variable term x in the combinatory algebra. We can extend the definition of the Lambda combinator by getting rid of the specific variable x . For any combinatory term M , the *Abstraction Operator* $\lambda x.$ is defined on M recursively by applying \mathbf{L}_x to all sub-terms of M . Applying $\lambda x.M$ to any other combinatory term N replaces all occurrences of the variable x in the term M by N and is written as $(\lambda x.M) \bullet N$.

The abstraction operator binds weaker than the combination operator. Thus, $\lambda x.$ binds all variables x in $M \bullet N$, such that we can omit parentheses as in $\lambda x.M \bullet N = \lambda x.(M \bullet N)$. Lambda abstraction provides a much more readable and intuitively understandable notation for terms of Combinatory Logic.

³The use of variables named P, Q, R is borrowed from Engeler (2020).

The Fixpoint Combinator

Given any combinatory term Z , the *Fixpoint Combinator* \mathbf{Y} generates a combinatory term $\mathbf{Y} \bullet Z$, called *Fixpoint of Z* , that fulfills $\mathbf{Y} \bullet Z = Z \bullet (\mathbf{Y} \bullet Z)$. This means that Z can be applied as many times as wanted to its fixpoint and still yields back the same combinatory term.

In linear algebra, such fixpoint combinators yield an eigenvector solution to some problem Z ; for instance, when solving a linear matrix. It is therefore tempting to say, that $\mathbf{Y} \bullet Z$ is a solution for the problem Z . For more details, consult Fehlmann (2016).

Using Lambda Calculus notation, the fixpoint combinator can be written as (Barendregt 1984):

$$\mathbf{Y} = \lambda f. (\lambda x. f \bullet (x \bullet x)) \bullet (\lambda x. f \bullet (x \bullet x)) \quad (7)$$

Translating (7) into an **S-K** term proves possible, becomes a bit lengthy but demonstrates how Combinatory Logic works.

By applying (6), (5):

$$\begin{aligned} \lambda x. f \bullet (x \bullet x) &= \mathbf{S} \bullet \lambda x. f \bullet \lambda x. x \bullet x \\ \lambda x. f &= \mathbf{K} \bullet f \end{aligned}$$

Then applying (6) and (4)

$$\begin{aligned} \lambda x. x \bullet x &= (\mathbf{S} \bullet \lambda x. x \bullet \lambda x. x) \\ &= (\mathbf{S} \bullet \mathbf{I} \bullet \mathbf{I}) \end{aligned}$$

yields

$$\lambda x. f \bullet (x \bullet x) = \mathbf{S} \bullet (\mathbf{K} \bullet f) \bullet (\mathbf{S} \bullet \mathbf{I} \bullet \mathbf{I})$$

and therefore

$$\begin{aligned} \mathbf{Y} &= \lambda f. (\lambda x. f \bullet (x \bullet x)) \bullet (\lambda x. f \bullet (x \bullet x)) \\ &= \lambda f. (\mathbf{S} \bullet (\mathbf{K} \bullet f) \bullet (\mathbf{S} \bullet \mathbf{I} \bullet \mathbf{I})) \bullet (\mathbf{S} \bullet (\mathbf{K} \bullet f) \bullet (\mathbf{S} \bullet \mathbf{I} \bullet \mathbf{I})) \\ &= \mathbf{S} \bullet (\lambda f. \mathbf{S} \bullet (\mathbf{K} \bullet f) \bullet (\mathbf{S} \bullet \mathbf{I} \bullet \mathbf{I})) \bullet (\lambda f. \mathbf{S} \bullet (\mathbf{K} \bullet f) \bullet (\mathbf{S} \bullet \mathbf{I} \bullet \mathbf{I})) \\ &= \mathbf{S} \bullet (\mathbf{S} \bullet (\lambda f. \mathbf{S} \bullet (\mathbf{K} \bullet f)) \bullet \lambda f. \mathbf{S} \bullet \mathbf{I} \bullet \mathbf{I}) \bullet (\mathbf{S} \bullet (\lambda f. \mathbf{S} \bullet (\mathbf{K} \bullet f)) \bullet \lambda f. \mathbf{S} \bullet \mathbf{I} \bullet \mathbf{I}) \end{aligned}$$

Now solving the remaining λ -terms:

$$\begin{aligned} \lambda f. \mathbf{S} \bullet (\mathbf{K} \bullet f) &= \mathbf{S} \bullet \lambda f. \mathbf{S} \bullet \lambda f. \mathbf{K} \bullet f \\ &= \mathbf{S} \bullet (\mathbf{K} \bullet \mathbf{S}) \bullet (\mathbf{S} \bullet \lambda f. \mathbf{K} \bullet \lambda f. f) \\ &= \mathbf{S} \bullet (\mathbf{K} \bullet \mathbf{S}) \bullet (\mathbf{S} \bullet (\mathbf{K} \bullet \mathbf{K}) \bullet \mathbf{I}) \end{aligned}$$

considering

$$\lambda f. S = K \bullet S$$

and

$$\lambda f. K \bullet f = S \bullet \lambda f. K \bullet \lambda f. f = S \bullet (K \bullet K) \bullet I.$$

The latter holds by first applying (6), then (5) and (4). Moreover

$$\begin{aligned} \lambda f. S \bullet I \bullet I &= S \bullet \lambda f. S \bullet I \bullet \lambda f. I \\ &= S \bullet (S \bullet \lambda f. S \bullet \lambda f. I) \bullet (K \bullet I) \\ &= S \bullet (S \bullet (K \bullet S) \bullet (K \bullet I)) \bullet (K \bullet I) \end{aligned}$$

applying again (6) and (5).

Putting things together:

$$\begin{aligned} Y &= \lambda f. (\lambda x. f \bullet (x \bullet x)) \bullet (\lambda x. f \bullet (x \bullet x)) \\ &= S \bullet \left(S \bullet (S \bullet (K \bullet S) \bullet (S \bullet (K \bullet K) \bullet I)) \bullet (S \bullet (S \bullet (K \bullet S) \bullet (K \bullet I)) \bullet (K \bullet I)) \right) \\ &\quad \bullet \left(S \bullet (S \bullet (K \bullet S) \bullet (S \bullet (K \bullet K) \bullet I)) \bullet (S \bullet (S \bullet (K \bullet S) \bullet (K \bullet I)) \bullet (K \bullet I)) \right) \end{aligned}$$

Applying **Y** to any combinatory term Z now explicitly transports Z on the top of the formula and keeps the rest of the structure of **Y** such that **Y** can be applied repeatedly.

This exercise should give the reader an impression how Combinatory Logic works.

Applying the fixpoint combinator **Y** to some combinator Z in the Lambda-style is much simpler:

$$\begin{aligned} &\lambda f. (\lambda x. f \bullet (x \bullet x)) \bullet (\lambda x. f \bullet (x \bullet x)) \bullet Z \\ &= (\lambda x. Z \bullet (x \bullet x)) \bullet (\lambda x. Z \bullet (x \bullet x)) \\ &= Z \bullet (\lambda x. Z \bullet (x \bullet x)) \bullet (\lambda x. Z \bullet (x \bullet x)) \end{aligned}$$

by applying the Lambda combinator twice, replacing the two $x \bullet x$ twice by $\lambda x. Z \bullet (x \bullet x)$. Thus, this explains reasoning as a repeated substitution process.

When applying **Y**, or **Y'**, or any other equivalent fixpoint combinator to a combinatory term Z , reducing the term by repeatedly using rule (1) or (2) does not always terminate. An infinite loop can occur, and must sometimes occur, otherwise we would always find a solution to any problem that can be stated within a programming language. Thus, Turing would be wrong and all finite state machines would reach a finishing state (Turing 1937).

Thus, the fixpoint combinator is not the solution of all our practical problems. But Engeler teaches us in his Neural Algebra fixpoints can be approximated using a *Construction Operator* (Engeler 2019), see below.

For more details about the foundations of Mathematical Logic, see for instance Potter (2004).

Arrow Terms

The *Graph Model of Combinatory Logic* (Engeler 1995) is a model of Combinatory Logic which explains how to combine topics in areas of knowledge. Combination is not only on the basic level possible; you can also explain how to combine topics on the second level; sometimes called meta-level. Intuitively, we would expect such a meta-level describing knowledge about how to deal with different knowledge areas.

Whenever two terms M and N are embodied in a combinatory algebra, the application of M onto N is also a term of this combinatory algebra, denoted as $M \bullet N$.

Let \mathcal{L} be the set of all assertions over a given domain. Examples include statements about customer's needs, solution characteristics, methods used, program states, test conditions, etc. These statements are assertions about the domain we are dealing with. This could be a business domain, or the state of some software, i.e., the description of the values for all controls and data.

An *Arrow Term* is recursively defined as follows:

- Every element of \mathcal{L} is an arrow term.
- Let a_1, \dots, a_m, b be arrow terms. Then

$$\{a_1, \dots, a_m\} \rightarrow b \quad (8)$$

is also an arrow term. Thus, arrow terms are relations between finite subsets of arrow terms and another arrow term, emphasized as successor.

For instance, in software testing, we use arrow terms to represent test cases. On the base level, the left-hand sides a_1, \dots, a_m represent test data, the term b is the known expected response of the test case (8). Higher levels of arrow terms represent test strategies and tests of tests.

The left-hand side of an arrow term is a finite set of arrow terms and the right-hand side is a single arrow term. This definition is recursive. The arrows are a formal graph notation; they might suggest cause-effect, not logical imply.

The Graph Model as an Algebra of Arrow Terms

We can extend the definition of arrow terms to become a combinatory algebra, allowing for the combination of arrow terms.

Denote by $\mathcal{G}(\mathcal{L})$ the power set containing all *Arrow Terms* of the form (8).

The formal, recursive, definition of the Graph Model as a power set, in set-theoretical language, is given in equation (9):

$$\begin{aligned} \mathcal{G}_0(\mathcal{L}) &= \mathcal{L} \\ \mathcal{G}_{n+1}(\mathcal{L}) &= \\ \mathcal{G}_n(\mathcal{L}) \cup \{ \{a_1, \dots, a_m\} \rightarrow b \mid a_1, \dots, a_m, b \in \mathcal{G}_n(\mathcal{L}), m \in \mathbb{N} \} \end{aligned} \quad (9)$$

for $n = 0, 1, 2, \dots$ $\mathcal{G}(\mathcal{L})$ is the set of all (finite and infinite) subsets of the union of all $\mathcal{G}_n(\mathcal{L})$:

$$\mathcal{G}(\mathcal{L}) = \bigcup_{n \in \mathbb{N}} \mathcal{G}_n(\mathcal{L}) \quad (10)$$

The elements of $\mathcal{G}_n(\mathcal{L})$ are arrow terms of level n . Terms of level 0 are *Assertions*, terms of level 1 *Rules*. A set of rules is called *Rule Set* (Fehlmann 2016). In general, a rule set is a finite set of arrow terms. We call infinite rule sets a *Knowledge Base*. Hence, knowledge is a potentially unlimited collection of rules sets containing rules about assertions regarding our domain.

Combining Knowledge Bases

We can combine knowledge bases sets as follows:

$$M \bullet N = \{c \mid \exists \{b_1, b_2, \dots, b_m\} \rightarrow c \in M; b_i \in N\} \quad (11)$$

Arrow Term Notation

To avoid the many set-theoretical parenthesis, the following notations, called *Arrow Schemes*, are applied:

- a_i for a finite set of arrow terms, i denoting some finite indexing function for arrow terms.
- a_1 for a singleton set of arrow terms: $a_1 = \{a\}$ for an arrow term a .
- \emptyset for the empty set, such as in the arrow term $\emptyset \rightarrow a$.
- $a_i \cup b_j$ for the union of two sets a_i and b_j of arrow terms.
- (a) for a potentially infinite set of arrow terms, where a is an arrow term.

Note that arrow schemes denote sets when put into outermost parenthesis. Without an index, the set might be infinite; an index makes the set finite.

The indexing function cascades; thus, $a_{i,j}$ denotes the union of a finite number of sets of arrow schemes

$$a_{i,j} = a_{i,1} \cup a_{i,2} \cup \dots \cup a_{i,j} \cup \dots \cup a_{i,m} = \bigcup_{k=1}^m a_{i,k} \quad (12)$$

In terms of these conventions, $(x_i \rightarrow y)_j$ denotes a rule set; i.e., a non-empty finite set of arrow terms, each having at least one arrow. Thus, such set has level 1 or higher. Moreover, it has two selection functions, i and j , selecting a finite number of arrow terms for x and $x_i \rightarrow y$.

With this notation, the application rule for M and N reads:

$$M \bullet N = ((b_i \rightarrow a) \bullet (b_i)) = \{a | \exists b_i \rightarrow a \in M; b_i \subset N\} \quad (13)$$

Arrow Terms – A Model of Combinatory Logic

The algebra of arrow terms is a combinatory algebra and thus a model of Combinatory Logic. It is called the *Graph Model*.

The following definitions demonstrate how arrow terms implement the combinators **S** and **K** fulfilling equations (1) and (2).

- **I** = $(a_1 \rightarrow a)$ is the *Identification*; i.e., $(a_1 \rightarrow a) \bullet (b) = (b)$
- **K** = $(a_1 \rightarrow \emptyset \rightarrow a)$ selects the 1st argument:
 $\mathbf{K} \bullet (b) \bullet (c) = ((b_1 \rightarrow \emptyset \rightarrow b) \bullet (b)) \bullet (c) = (\emptyset \rightarrow b) \bullet (c) = (b)$
- **KI** = $(\emptyset \rightarrow a_1 \rightarrow a)$ selects the 2nd argument:
 $\mathbf{KI} \bullet (b) \bullet (c) = ((\emptyset \rightarrow c_1 \rightarrow c) \bullet (b)) \bullet (c) = (c_1 \rightarrow c) \bullet (c) = (c)$
- **S** = $\left((a_i \rightarrow (b_j \rightarrow c))_1 \rightarrow (d_k \rightarrow b)_i \rightarrow (a_i \cup b_{j,i} \rightarrow c) \right)$

Therefore, the algebra of arrow terms is a model of Combinatory Logic.

The proof that the arrow terms' definition of **S** fulfils equation (2) is somewhat more complex. Readers interested in that proof are referred to Engeler (1981, p. 389). With **S** and **K**, an abstraction operator can be constructed that builds new knowledge bases. This is the *Lambda Theorem*; it is proved along the same way as Barendregt's Lambda combinatory (Barendregt 1977). See also in Fehlmann (1981, p. 37).

The Role of the Indexing Function in Arrow Terms

The arrow in the terms of the Graph Model is somewhat confusing. It is easily mistaken as representing *Predicate Logic*; however, this must be viewed with care. Interpreting the arrow as an implication in predicate logic is not per se dangerous. In some sense, logical imply is a transition from preconditions to conclusion and arrow terms are fine for representing them. The problem is that if the left-hand side of an arrow term, which is an otherwise unstructured set, is interpreted as a conjunction of predicates – a sequence of logical AND-clauses – you run into a conflict with the undecidability of first-order logic. Arrow terms would then reduce to either of the form $a_1 \rightarrow b$ or $\emptyset \rightarrow b$. This reduces the model to become the trivial one.

As an example, see Bimbó (2012, p. 237ff). There she explains how typed Combinatory Logic gets around the triviality problem. Instead of the indexing functions, selecting finite sets of arrow terms on the left-hand side, she postulates proofs for the predicates.

Thus, the indexing function for selecting elements of a finite set of arrow terms is a key element of the Graph Model. Interested readers will find related considerations in the paper of Fehlmann and Kranich (2020). For the application of the Graph Model to testing, the indexing function means selection of test cases and test data, and this is always a collection of program state predicates that do typically not leave the program under test in a consistent state.

Neural Algebra

Engeler uses the Graph Model as a model how the brain thinks (Engeler 2019). A directed graph, together with a firing law at all its nodes, constitutes the connective basis of the brain model \mathcal{A} . The model itself is built on this basis by identifying brain functions with parts of the firing history. Its elements may be visualized as a directed graph, whose nodes indicate the firing of a neuron. As before, we consider $\mathcal{G}(\mathcal{A})$, constructed as in (10). The elements of $\mathcal{G}(\mathcal{A})$ are called *Cascades*. Cascades describe firing between nodes (neurons) when represented by finite sets of arrow terms $a_i \rightarrow b$ where a_i are sub-cascades, while the right sub-cascade b describes the characteristic leave of its firing history graph. The *Neural Algebra* is defined as a collection of cascades representing brain functions in the brain model, closed under applications and union. With the application rule (13), we have an algebraic structure; the application representing brain functions, interpreted as thoughts.

The Fixpoint Combinator in the Neural Algebra

The fixpoint combinator \mathbf{Y} can be written as an arrow scheme; however, this calculation is better left to some suitable rewriting tool, as otherwise this article would exceed all reasonable length. Applying \mathbf{Y} to an arbitrary arrow scheme might result in an infinite loop of arrow schemes, representing a never-ending computation. Combinatory Logic, as any kind of programming, may result in an infinite loop in its model, and it is not decidable when this happens.

If infinite loops occur, or infinite sequences of digits like for real numbers that are not rationales, we need the notion of controlling operators that approximate the possibly infinite solution, and metrics for measuring how near the approximations to the solutions are, and get even nearer when required.

Reasoning, Problem Solving and Controlling

Within this setting, it is possible to define models for reasoning and problem solving. However, not only flat reasoning, also for solving problems, even if their fixpoint is infinite. For a controlled object X , the *Controlling Operator* \mathbf{C} solves the control problem $\mathbf{C} \bullet X = X$. The brain function \mathbf{C} gathers all faculties that may help in the solution. The control problem is a repeated process of substitution, like finding the fixpoint of a combinator. However, since cascades are always finite –

all brain activity remains finite, unfortunately – solving the control problem is by a series of finite *Attractors*, a control sequence $X_0 \subseteq X_1 \subseteq X_2 \subseteq \dots$ determined by

$$X_{i+1} = \mathbf{C} \bullet X_i, i \in \mathbb{N} \quad (14)$$

starting with an initial X_0 . This process is called *Focusing*. The details can be found in Engeler (2019, p. 301). We will rely on the observation that attractors represent reasoning in a neural algebra.

Attractors are ordered by inclusion (14), meaning that the solution space becomes smaller and smaller until a smallest possible solution is found that cannot be further reduced by the controlling operator. It is possible that this ultimate solution remains empty.

The controlling operator is closely linked to the fixpoint operator \mathbf{Y} . If X has a solution $\mathbf{C} \bullet X$, then X is of the form $X = \mathbf{Y} \bullet Z$ for some suitable cascade Z . Thus, not all combinators X have a solution; the related control sequence may end with the empty cascade, obviously. These considerations share a stunning resemblance with transfer functions, whose solution profiles are also approximations rather than precise solutions (Fehlmann 2016, p. 14).

The controlling operator is not like one of the basic or the fixpoint combinators but is more of a prescription, how to find suitable attractors. Engeler (2019, p. 300ff) presents in an elegant way representations of basic thought processes, e.g., reflection, discrimination, simultaneous and joint control, but also learning, teaching, focusing with eyes, and comprehension.

Since the number of cascades that a brain can produce is finite and limited – by the lifespan of the brain – solution to the fixpoint control problems turn out to be finite attractor sequences, characterizing thought processes.

Transfer Functions

For managing complex systems, transfer functions are used to analyze controls and approximate the expected result (Fehlmann 2016).

An obvious interpretation of arrow terms is by transfer functions. In *Quality Function Deployment* (QFD), the building blocks – and the origin – are cause-effect relations as used in Ishikawa Diagram (Ishikawa and Loftus 1990). These diagrams describe the cause-effect relations between topics and are considered the initial form of QFD matrices. Converting a series of Ishikawa diagrams into a QFD matrix is straightforward (see Fehlmann 2016, p. 231). Thus, transfer functions can be described by finite sets of arrow terms.

Deming Chains

Composition of transfer functions is called a *Deming Chain* (Fehlmann 2016, p. 100) because Deming identified the value chains in manufacturing processes (Deming 1986). Akao called it *Comprehensive QFD*, also known as *QFD in the*

Large. He drafted extensive Deming chains in this famous book on QFD (Akao 1990).

For transfer functions, the Graph Model provides similar services as for tests. The model proves that transfer functions have universal applicability and power for explaining cause-effect, and they provide a framework for automation also for Deming chains (Fehlmann 2001).

The Algebra of Tests

Very interesting instantiations of the Graph Model can be found in *Software Testing*, especially when seen from an economical viewpoint. In fact, test cases are best described as arrow terms, with the left-hand sides describing program states before executing the test, and the right-hand side describing the response of the test case. Software testing is the key to digitalization and to software-intense products that perform safety-critical tasks.

Test cases are a mapping of arrow terms onto *Data Movement Maps*. Data movement maps model the software under test by identifying the data groups moved by the software, based on the ISO standard 19761 COSMIC (ISO/IEC 19761 2011). This has been explained in more detail in Fehlmann (2020). The data movements induce a sizing valuation on this algebra by counting the number of data movements executed per test case.

When we speak of test cases, we always intend a suitable data movement map with it; thus, the same arrow term can be mapped to several data movement maps, counting as separate test cases.

State Assertions

For our Test Algebra, we now assume \mathcal{L} to be the set of all state assertions for a given program. We use the term “program” but mean a system that might consist of coded software, services, or anything yielding results electronically. Learning machines also are “programs” in that sense even if it is not the code that implements learning, rather the learned knowledge itself. Elements of \mathcal{L} are descriptions of the system status, or the knowledge such as system has, at a certain moment. In the sequel, the arrow term $a_i \rightarrow b$ together with its associated data movement map represents a test case, that, given test data a_i , yields b as the expected, correct result (Fehlmann 2020, p. 85ff).

If $a_i \rightarrow b$ is a test case, $a_i \in \mathcal{L}$ specifies a set of test data that holds before executing the test, and $b \in \mathcal{L}$ the state of the program after execution. The finite set a_i represents the states before execution of possible unrelated threads of the program, or services involved.

Testing Complex Systems

Usually, unit tests that ensure the proper functioning of software modules are available because they originate from the software development process (JUnit Team 1997ff). The integration of modules and components and building systems of systems, or other complex products, requires many more tests, among them end-to-end tests that cause huge efforts. Most often, the time slots available for testing are used up to accommodate additional or forgotten user requirements. Consequently, with respect to functionality, the more important tests become when creating complex products, the less tests are executed, by lack of time and resources. Attempts to execute tests automatically do not address the lack of good test cases for complex products. There are the test cases that need to be created automatically. This approach is called *Autonomous Real-time Testing*, to point out that testing effort always must remain limited. It addresses the problem how to automatically create test cases by Artificial Intelligence, namely by generating test cases using Combinatory Logic and selecting the relevant ones using ISO/IEC 16355 (ISO/IEC 16355-1 2015). The approach is explained in Fehlmann (2020).

Combining Tests

The definition (13) explains how to combine test cases. To apply one set M of test cases to another N , it is required that for testing the assertion a , test cases $b_i \in N$ exist such that $(b_i \rightarrow a)$ in M has effectively been tested. Consult last the paper of Fehlmann and Kranich (2020) for more information about the existential quantifier in (13).

The intuitionistic, or constructive, variant of the Axiom of Choice requires not only the existence of test providing valid test data as response, but construction instructions for the existence of such tests, respectively the related test cases. This means that it is not enough to know the existence of tests, but you need to know how to construct them. This is possibly the reason why test automation has proven to be so hard.

And for those who consider such reasoning too theoretical, let us provide a rather practical argument: programmers who want to set up test concatenation $M \bullet N$ for automatic testing, need access to the test cases in N that provide the responses needed for M , for combining M with N . Otherwise, combining tests is unsafe or cannot be automated. Thus, with the combinatory algebra of arrow terms, mathematical logic meets both intuitionism and programming.

Combination Limitations

Combining tests in a Combinatory Algebra is unlimited indeed because there is no typing involved that governs applicability. By (13), you can combine test cases across test stories as deemed appropriate; all that counts are that the test cases remain executable. This means that two test cases must not only be linked by its assertions, but also executable code must exist that combine these two test cases. In terms of software, two data movement maps representing the test case executions must exist that overlap.

The Size of Tests

For a testing framework, we need to be able to measure the size of tests. The standard ISO/IEC 19761 COSMIC for measuring functional size serves as measuring method. The functional size of the associated data movement map is the size of a test case, denoted by $Cfp(a_i^0 \rightarrow b^0)$, where $a_i^0 \in \mathcal{G}_0(\mathcal{L})$ and $b^0 \in \mathcal{G}_0(\mathcal{L})$ are arrow terms of level 0; i.e., assertions about the state of the program. $Cfp(a_i^0 \rightarrow b^0)$ is the number of unique data movements touched when executing the test case $a_i^0 \rightarrow b^0$. This is the recursion base.

Then the following equations (15) recursively define the size of tests:

$$\begin{aligned} [a] &= 0 \text{ for } a \in \mathcal{G}_0(\mathcal{L}) \\ [a_i \rightarrow b] &= Cfp(a_i \rightarrow b) \text{ for } a_i \in \mathcal{G}_0(\mathcal{L}) \text{ and } b \in \mathcal{G}_0(\mathcal{L}) \\ [c_i \rightarrow d] &= \sum_i [c_i] + [d] \text{ for all test cases } c_i \text{ and } d \end{aligned} \quad (15)$$

The definition holds for all arrow terms in the algebra of tests.

The addition does not take into consideration whether data movements are unique; thus, the size of two test cases is always the sum of the sizes. When speaking about tests, we do not use the term knowledge base for sets of arrow terms, but rather *Test Story* for a set of test cases. Test stories typically share a common intent, or business value.

The Functional Size of Combinators

Applying the definition (15) to the combinators **S**, **K**, **I**, and **Y** yields an infinite size for each of them, because the arrow term sets are infinite. This is conformant to the observation that when expressing these combinators as terms in the Lambda calculus, they are closed insofar as they do not contain free variables nor constants.

Autonomous Real-time Testing

In Fehlmann (2020), we coined the term *Autonomous Real-time Testing* (ART) to describe software tests that are

- Executed automatically in a system during operations, or when pausing operations;
- Started from a base test using recombination and other operations of combinatory algebra by adding autonomously generated test cases;
- Controlled by transfer functions assuring relevance for users' values.

In previous papers and the book referenced about, we have explained how to keep the growth of test cases under control, using the *Convergence Gap* as a hash. The convergence gap in transfer functions measures the gap between the needs –

of the customer, the user, certification authority, or else – and the achieved test coverage. Consult the paper of Fehlmann and Kranich (2020).

Attractors

While the fixpoint combinator \mathbf{Y} works as above on sets of test cases, in most cases, it returns infinite tests as “solutions” – something not too practical. However, we can construct attractors for neural algebra, approximating the infinite testing set, as good as we wish. This creates a new problem for us, namely, to assess: when is testing good enough?

While good practices can provide answers – e.g., by looking at the remaining defect rate (Fehlmann and Kranich 2014) – a more theoretical answer should include at least the requirement that attractors cover functionality. That is the significance of the *Convergence Gap*, explained in Fehlmann (2020, p. 10).

Let U_l denote a finite set of user stories, and T_k another set of test stories, usually somewhat larger than the set of user stories. The matrix $U_l \otimes T_k$ maps test stories to user stories and becomes a transfer function, if each cell contains the size $|(a_i \rightarrow b)_j|$ of all test cases $(a_i \rightarrow b)_j$ belonging to some test story T_k and referring to some user story, or FUR U_l . This yields a matrix:

$$\mathbf{A} = (|(a_i \rightarrow b)_j|)_{l,k} \quad (16)$$

The indices of the matrix run over integers $l, k \in \mathbb{N}$.

The transfer function \mathbf{A} maps test stories to user stories, and we call it *Test Coverage Matrix* because you can assess how good test stories cover user stories.

Let user stories be prioritized, say by some *Goal Profile* \mathbf{y} . The goal profile characterizes priorities by a unit vector in the space of the alternatives under consideration. Then the transfer function \mathbf{A} can be applied to a *Solution Profile* \mathbf{x} , describing the importance of the test stories, and \mathbf{Ax} is the result of applying \mathbf{A} to this solution profile. Obviously $\mathbf{Ax} \neq \mathbf{y}$; however, the difference $\|\mathbf{x} - \mathbf{y}\|$ is interesting. If this difference is small, then the solution profile \mathbf{x} represents an optimum selection of test stories, meaning that tests cover what is relevant to the user’s goal profile.

Optimum solution profiles can be calculated using the eigenvector method (Fehlmann 2016, p. 34). Let \mathbf{y}_A be the *Principal Eigenvector* of \mathbf{AA}^T , solving the eigenvalue problem (17) for some $\lambda \in \mathbb{R}$.

$$\mathbf{AA}^T \mathbf{y}_A = \lambda \mathbf{y}_A \quad (17)$$

The principal eigenvector \mathbf{y}_A is called the *Achieved Profile* of the transfer function \mathbf{A} . Both, \mathbf{y} and \mathbf{y}_A are *Profiles*. This means, their vector length $\|\mathbf{y}\| = 1$ respectively $\|\mathbf{y}_A\| = 1$ are both one, where $\|\dots\|$ represents the *Euclidean Norm*

for vectors. The difference between a goal profile and an achieved profile is called *Convergence Gap*:

$$\text{Convergence Gap} = \|\mathbf{y} - \mathbf{y}_A\| \quad (18)$$

The convergence gap is a metric that measures how well a transfer function explains the observed profile with suitable controls. The controls are the test stories; the observed profile compares with the goal profile of the user stories' relevance for the user of the software or the system. Note that computing the achieved profile is very often not straightforward, as it is in our case where we can make use of simple linear algebra.

We can now construct attractors as a series $\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2, \dots$ of test coverage matrices that approximate the test suite that we need to cover our functional requirements. However, the attractors must all keep the convergence gap und control, meaning that for a certain $\varepsilon > 0$ and all attractors \mathbf{A}_i holds:

$$\text{Convergence Gap}(\mathbf{A}_i) = \|\mathbf{y}_i - \mathbf{y}_{\mathbf{A}_i}\| < \varepsilon \quad (19)$$

Thus, our constructor \mathbf{C} must construct an ascendant series $\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2, \dots$ such that both (19) and (20) holds:

$$\begin{aligned} \mathbf{A}_{i+1} &= \mathbf{C} \bullet \mathbf{A}_i, i \in \mathbb{N} \\ \mathbf{A}_i &\subseteq \mathbf{A}_{i+1}, i \in \mathbb{N} \end{aligned} \quad (20)$$

The constructor \mathbf{C} therefore is an intelligent search in a wide range of potential attractors, keeping the convergence gap small enough. Such a series of attractors is called *bound*, namely by the convergence gap. In fact, bound attractors constitute a formal way to solve all kind of issues normally tackled by Artificial Intelligence. The hash functions used for measuring the convergence gap, might be considerably more complicated than in the case of test size.

Optimum Test Size

For a test coverage matrix $\mathbf{A} = ([(a_i \rightarrow b)_j]_{l,k})$, the total test size of \mathbf{A} is

$$|\mathbf{A}| = \sum_{l,k} ([(a_i \rightarrow b)_j]_{l,k}) \quad l, k \in \mathbb{N} \quad (21)$$

If $\mathbf{A}_0 \subseteq \mathbf{A}_1 \subseteq \mathbf{A}_2 \subseteq \dots$, then $|\mathbf{A}_0| \leq |\mathbf{A}_1| \leq |\mathbf{A}_2| \leq \dots$ also holds.

Combinations of tests can be used, as well as applying any special combinator such as projection or substitution to generate new test cases.

Bound attractors build up a test suite by adding more tests to the test coverage matrix \mathbf{A} . The convergence gap must not necessarily decrease. In contrary, adding

more tests can spoil the convergence gap, for instance if some test story gains too much weight and inflate the respective user stories' achieved profile.

Constructing a suitable constructor \mathbf{C} is all but simple, nor straightforward, because adding more tests does not solve a problem. In view of executing such tests on a machine, the number of tests must not only remain finite but also limited to some manageable number. Thus, the question how to select relevant test stories out of the many possible combinations must be answered. An answer is proposed in Fehlmann and Kranich (2019). Moreover, based on sensitivity analysis for linear matrices, the authors will present sample attractors for software and system testing at the upcoming (2022) ATINER's conference on Information Technology & Computer Science (Fehlmann and Kranich 2022). Sensitivity analysis speeds up the selection of the new test cases. Thus, it seems that the problem of effectively create autonomous tests for large and complex systems can be solved.

For practical applications, combining unit tests from related domains such as steering control of an autonomous vehicle with weather forecast is always feasible to construct attractors for a system test of this autonomous vehicle. The convergence gap enforces that such test combinations cover the full range of test cases relating to both steering control, and process weather forecast services; otherwise, some test stories would grow beyond limits.

There is an optimum number of attractors delivering enough tests to fit the test intensity required by the user of the system, and test size that still can be executed within a limited time frame. Computing that optimum is an important task for product management, and, depending upon safety and privacy criticality, must be carefully chosen to make such a product acceptable for the society.

Conclusions

It has been shown that Aristotle's *Mental Completion* leads to feasible solutions for actual challenges and problems. His understanding of recursion as a mentally completed inductive definition of a concept (Engeler 2020) allows developing the techniques necessary for testing modern, complex systems of systems, including cyber-physical systems that impact people's life and health. Following Engeler, we identified constructors as a general prescription for constructing attractors that serve as approximations to solutions for problems. Effective methods and algorithms exist for such constructions in the algebra of tests, as shown in Fehlmann and Kranich (2020), and in Fehlmann (2020). Linking attractors to fixpoint operators, in a very practical setting, has potentially a high economic impact in the *Fourth Industrial Revolution* (Schwaab 2017), in the realm of cyber-physicals systems such as autonomous cars, intelligent medical instruments, virtual reality, and more.

Open Questions

Why did Aristotle not invent relations? Because he had no use for them (Engeler 2020, p. 12). Euclidean geometry went without relations. So why do we

not yet know combinators for software testing? Because we are probably just now finding out what they could be good for?

The authors are currently developing ideas how actual constructors look for software and system testing, as well as for Artificial Intelligence. However, whether there are some general rules to follow, besides Combinatory Logic, or if every testing domain requires its own constructors and attractor series, remains open.

Obviously, there are more open questions than we can mention here. Maybe this is a step toward the *New Kind of Science* that Stephen Wolfram (2002) promised us in the early years of this century? Is the approach presented in this paper potentially fruitful not only to Artificial Intelligence, Neuroscience, and system testing? What else could we describe by a constructor and by attractors? Thus, better understanding what we are doing, and why?

Why are we doing theoretical stuff like logic and other basic sciences? Maybe the answer is because this is the way to new business models and more efficient progress in applied sciences? Probably the only sure way? Because otherwise you get lost in the jungle? Without hope for finding an exit.

Do we offer young engineers enough education in basic sciences? Once they have mastered that, they can apply the basic findings to any applied technical or scientific area they care for.

Acknowledgments

Thanks to Erwin Engeler who sent his former student the enjoyable paper about Aristotle's Relations that he wrote as a gift to his 90th birthday and for all the investigations into the Graph Model that he did. I hope we were able to share this with our reviewers and readers.

Also, many thanks to all who contributed to this paper by pointing to weaknesses and confusions. Special thanks to the reviewers who contributed with their comments much for improving this paper.

References

- Akao Y (1990) *Quality function deployment - Integrating customer requirements into product design*. Portland, OR: Productivity Press.
- Aristoteles (367-344 BCE) *Organon*. Übersetzt von Julius von Kirschmann, Hofenberg ed. Berlin: Andronikos von Rhodos.
- Barendregt HP (1977) The type-free lambda-calculus. In J Barwise (ed.), *Handbook of Mathematical Logic*, 1091–1132. Amsterdam: North Holland.
- Barendregt HP (1984) The lambda calculus – Its syntax and semantics. In *Studies in Logic and the Foundations of Mathematics*. Amsterdam: North-Holland.
- Bimbó K (2012) *Combinatory logic - Pure, applied and typed*. Boca Raton, FL: CRC Press.
- Church A (1941) The calculi of lambda conversion. In *Annals of Mathematical Studies* no. 6. Princeton University Press.
- Curry H (1930) Grundlagen der kombinatorischen Logik. (Basics of combinatory logic). *American Journal of Mathematics* 52(3): 509–536.

- Curry H, Feys R (1958) *Combinatory logic*, volume I. Amsterdam: North-Holland.
- Curry H, Hindley J, Seldin J (1972) *Combinatory logic*, volume II. Amsterdam: North-Holland.
- Deming W (1986) *Out of the Crisis*. Center for Advanced Engineering Study ed. Boston, MA: Massachusetts Institute of Technology.
- Engeler E (1981) Algebras and Combinators. *Algebra Universalis* 13(Dec): 389–392.
- Engeler E (1995) *The combinatory programme*. Basel, Switzerland: Birkhäuser.
- Engeler E (2019) Neural algebra on “how does the brain think?” *Theoretical Computer Science* 777(Apr): 296–307.
- Engeler E (2020) *Aristotle’ relations: an interpretation in combinatory logic*. arXiv: History and Overview.
- Fehlmann TM (1981) *Theorie und Anwendung des Graphmodells der Kombinatorischen Logik*. (Theory and application of the graph model of combinatory logic). Zürich, CH: ETH Dissertation 3140-01.
- Fehlmann TM (2001) QFD as algebra of combinators. In *8th International QFD Symposium, ISQFD 2001*. Tokyo, Japan.
- Fehlmann TM (2016) *Managing complexity – Uncover the mysteries with six sigma transfer functions*. Berlin, Germany: Logos Press.
- Fehlmann TM (2020) *Autonomous real-time testing – Testing artificial intelligence and other complex systems*. Berlin, Germany: Logos Press.
- Fehlmann TM, Kranich E (2014) *Exponentially Weighted Moving Average (EWMA) prediction in the software development process*. Rotterdam, NL: IWSM Mensura.
- Fehlmann TM, Kranich E (2019) Testing artificial intelligence by customers’ needs. *Athens Journal of Sciences* 6(4): 265–286.
- Fehlmann TM, Kranich E (2020) Intuitionism and computer science – Why computer scientists do not like the axiom of choice. *Athens Journal of Sciences* 7(3): 143–158.
- Fehlmann TM, Kranich E (2022) A sensitivity analysis procedure for matrix-based transfer functions. *Athens Journal of Sciences* (proposed).
- ISO 16355-1 (2015) *Applications of statistical and related methods to new technology and product development process - part 1: general principles and perspectives of Quality Function Deployment (QFD)*. Geneva, Switzerland: ISO TC 69/SC 8/WG 2 N 14.
- ISO/IEC 19761 (2011) *Software engineering – COSMIC: a functional size measurement method*. Geneva, Switzerland: ISO/IEC JTC 1/SC 7.
- Ishikawa K, Loftus JH (1990) *Introduction to quality control*. Tokyo: 3A Corporation.
- JUnit Team (1997ff) The 5th major version of the programmer-friendly testing framework for Java and the JVM. Retrieved from: <https://junit.org/>. [Accessed 28 January 2022]
- Potter MD (2004) *Set theory and its philosophy*. Oxford, UK: Oxford University Press.
- Schönfinkel M (1924) Über die Bausteine der mathematischen Logik. (About the building blocks of mathematical logic). *Mathematische Annalen* 92(3–4): 305–316.
- Schwaab K (2017) *The fourth industrial revolution*. First Edition. New York: World Economic Forum.
- Turing A (1937) On computable numbers, with an application to the Entscheidungs problem. In *Proceedings of the London Mathematical Society* 42(Series 2): 230–265.
- Wolfram S (2002) *A new kind of science*. First Edition. Champaign, Illinois: Wolfram Media.
- Zachos E (1978) *Kombinatorische Logik und S-Terme*. (Combinatorial logic and S-terms). Zurich: ETH Dissertation 6214.

Pupil's Fraction Learning based on Board Game Playing

By Chia-Hao Tsai^{*} & Erh-Tsung Chin[±]

Primary school pupils have good mathematics learning achievements but lack interest and attitude towards mathematics learning in Taiwan. Therefore, it is necessary and feasible to study how to use game-based learning in mathematics. In this research, the board games are adopted and designed by the team members, and then are integrated into the learning of mathematics fractions. The pre-test and post-test are designed to analyze the effectiveness of pupils using board games for learning and the formation of fraction conceptions, supplemented by interviews to understand pupils' interest and attitudes changes in learning. Research has found that pupils who only use board games for learning can recognize and read unit fractions, which can achieve the expected learning goals and enhance pupils' interest and attitude towards mathematics learning. Finally, the limitations of this research study and the directions for future research are also proposed.

Keywords: board game, fraction learning, game-based learning, teaching aids

Introduction

In order to implement the concepts and goals of the 12-year National Basic Education Curriculum in Taiwan, the curriculum takes “core literacy” as the main axis of its development to facilitate the continuity of various educational stages and the integration of various disciplines. Among them, “core literacy” refers to the knowledge, ability, and attitude that a person should possess in order to adapt to the current life and face the challenges of the future. Therefore, “core literacy” emphasizes that learning should not be limited to subject knowledge and skills, but should focus on the combination of learning and life, and demonstrate the learner's whole-person development through practice (Ministry of Education 2018).

According to the results in Trends in International Mathematics and Science Study (TIMSS), the fourth graders' achievements of mathematics learning in Taiwan are ranked among the best, but their interests and attitudes towards mathematics are far lower than the average of participant countries (Chang 2018, TIMSS 2011, 2015, 2019). Research shows that fourth-grade pupils in Taiwan although have good scores in solving mathematic problems, but still think mathematic is a useless subject and avoid to learn if they could. Comparing with the standards proposed in the syllabus, it is clear that in mathematics, pupils are not equipped with the core literacy they should have. Therefore, it's worth studying that how to enhance pupils' motivation and interests in mathematics learning in the future.

^{*}Graduate Student, Graduate Institute of Science Education, National Changhua University of Education, Taiwan.

[±]Associate Professor (corresponding author), Graduate Institute of Science Education, National Changhua University of Education, Taiwan.

Game-based learning is a learning model that has emerged in recent years. Any learning method that uses tools or activities to enhance learners' motivation and interest can be classified as a part of game-based learning. Although it has been mostly referred to as digital learning in recent years, it is not a learning method that focuses on exponential games (Plass et al. 2015). Broadly speaking, fun-oriented learning refers to designing an interactive process that can achieve a balance between the needs of subject knowledge and the needs of gameplay (Plass et al. 2010). Hou (2016) also believes that learning from playing can bring out student's interests well in learning.

Board game is also called unplugged game. It covers games that do not rely on electronic devices and electronic products, such as games with cards, with dices, or with papers that participants play face-to face. Board game is a term for games played in the same place. Board games are not only fun to play, so that pupils can play with interest, but the depth and diversity of board games can also enrich pupils' life experience, depending on how teachers use them. According to Shulman (1986) research, in order to achieve effective teaching performance, teachers need to have three types of knowledge, namely content knowledge (CK), pedagogical knowledge (PK), and pedagogical content knowledge (PCK), is to understand how to effectively teach the content of a certain subject. Related research has found that when teachers have a wealth of PCK, it is indeed helpful for pupils' learning. Therefore, if teachers want to improve students' interest in learning and learning effectiveness in order to teach mathematics well, and refer to the use of board games to integrate mathematics teaching for pupils in primary school, will there be any changes in teachers' PCK? And what are the changes? Will it help teachers' professional growth in mathematics to enhance the effectiveness of pupils' mathematics learning, and cultivate the core mathematics nurturing of pupils at the same time? These are worth researching.

"Education is nothing but a concern for love and role model". The learning effectiveness of pupils is closely related to the teaching of teachers. Researchers are very interested in forming effective teaching in the field of mathematics in primary schools. Studies have shown that entertaining mathematics learning has a positive effect on pupils' learning effectiveness or learning literacy. Therefore, if mathematics board games are incorporated into primary school mathematics teaching, will teachers' PCK be different from applying the teaching aids? How to develop mathematics literacy-oriented teaching with expert teachers? It is really exciting. Therefore, the research intends to answer the following unanswered questions first:

1. Can students learn the concept of fractions through board games?
2. What is the effectiveness of pupils' learning through board games of fractions?

Literature Review

Game-Based Learning and Board-Games

Game-Based Learning

Game-based learning is usually defined as a model of learning by using computer games as a medium. What is game-based learning in education? “Game-based learning” broadly refers to the use of video games to support teaching and learning. Although it is a relatively established notion, it is hard to define precisely (Perrotta et al. 2013). Therefore, because of the evident motivational qualities of games, educators and trainers alike seek to use them for instruction.

It is argued that games could change education because it makes it possible to learn on a massive scale by doing things that people do in the world outside of school (Shaffer 2006, p. 23):

“They make it possible for students to learn to think in innovative and creative ways just as innovators in the real world learn to think creatively...but they can do this only if we first understand how computers change what it means to be educated in the first place”.

Because pupils in Taiwan have no senses of achievement and feel meaningless on mathematics learning even they have high scores in tests, it is quite necessary to seek meaningful learning and teaching methods for them. Sharma (2012) considered toys and games are synonymous with play, pleasure, and relaxation. Almost everyone likes to play and, in one form or other, this continues throughout one’s life. Play is not just a filling in of an empty period or a relaxation or leisure activity, it is also an important learning experience- an essential ingredient for growth and development for children and adults alike. Therefore, if games and mathematics learning can be combined, it should be quite effective in cultivating students’ knowledge and skills. Although, researchers (Games and Squire 2011) and game designers (Prensky 2011) indicate that games specifically designed for educational purposes are not as much fun to play compared to those designed only for fun. Educational games are certainly not as widely distributed, or as successful financially as those developed for amusement (Tobias et al. 2014), but using games (not just digital games) to learn mathematics is still a topic worth researching.

Board Games and Educational Expecting

In recent years, board games have gradually emerged in leisure activities and have gradually attracted public attention in Taiwan. Board game (or named “tabletop game”, “table game”) generally refers to that there is no need to plugin, as long as it is any game played on a flat surface, it is considered a board game, so it is also called “unplugged game”, including card games (also including trading card games), board games, tile-based games, etc., as well as other general names for games played on the table or any multiplayer face-to-face plane. Broadly speaking, chess, poker, mahjong, etc. are also board games. Board games also

generally refer to games that do not rely on electronic devices and electronic products, and usually do not require large-scale actions.

Among the many games, board games, which require less time than others, have become the choice of activities when gathering together. Compared with other types of games (such as video games and group health games), board games have barriers low to entry, convenience high, and the concept of group interaction, so it is suitable as a medium for interpersonal interaction. Michael Mindes, the founder of “Tasty Minstrel Games” company, mentioned that board games can provide new ideas for learning, interpersonal interaction and life connections. When children want to win and have enthusiasm and motivation to learn, they will get the greatest pleasure. When playing board games, participants need to interact with each other and require a variety of abilities, such as concentration, expression, reaction, judgment, memory, empathy, logic and reasoning skills. Feel and experience the interaction and feelings of different situations through activities. Learning in games may include the use of games designed for learning purposes, as well as games that were not originally built for the education market. Many researchers have found their learning value.

Figure 1. Model of Game-Based Learning



Source: Garri et al. 2002.

Let us consider, based on the Model of game-based learning Figure 1, how and when learning occurs when learners interact e.g. play a game, contrast with board game, there are six characteristics (Wu 2011):

Personal actual participation: stresses the interaction between people.

Safety: Compared with group active games or sports, it will not be hurt.

Flexible: According to the different attributes and needs of players, choose suitable game scenes.

Easy to get started: The entry barriers of the game are low, and you can choose a suitable game according to the player's level.

Convenience: It is less affected by the venue, weather, and equipment, as long as there is a flat surface and the board game starts.

Encourage interaction: Whether it is a competitive game or a cooperative game, it is necessary to communicate and negotiate with each other through language or expressions in order to influence or persuade the other party to propose ideas or strategies.

In the course of many years of teaching, researchers have devoted themselves to combining various games with learning. Through long-term observation, we

have found that learners of any age group are more capable of focusing on game-like interaction methods. And interest, the main reason is that all individuals can adjust the learning rhythm with their own adaptability during the game, and because the game has many cyclic characteristics, all individuals can receive the effect of repeated verification without falling into boring. Pupils can set goals according to their own abilities. For example, those who are quicker in learning response can further challenge the answering speed after reaching a higher rate of correct answering; on the contrary, those who need more time for learning response can also gradually improve step by step. Accumulate the number of correct answers, even if learners have differences in learning abilities, they can cooperate and be compatible, advance together, compete, and help each other, and further match the rigorous rule design, so that learners can form a co-prosperity and coexistence. The relationship between peers, to give play to the power of mutual help and mutual learning among peers, to enhance the sense of honor gained by those who are superior in learning, and to strengthen the willingness to learn again for those who are lagging behind in learning. The effect is indeed better than that of a single teaching and teaching mode.

Designing Playful Learning by Using Educational Board Game

Board game according to Scoviano (2010) in Game Board History and Game Psychology, the board game is a type of game where tools or parts of a game are placed, moved, or moved on a marked or divided surface according to a set of rules. The game may be based on a pure strategy, opportunity, or mixture of both and usually has a goal to be achieved. The media board game games need to be developed because there are currently many games that only contain cognitive aspects such as play stations and online games without regard to affective and psychomotor aspects which can cause students to have high individualism (Erlitasari and Dewi 2016). In addition board games can be used as a channel for information and help in the learning process. That agreed with Gagne (Sadiman et al. 1990) states that the media are various types of components in the student environment that can stimulate learning. For example, using some blocks with different colors or shapes, pupils will learn some concepts through the classifying and matching activities, and they will be more interested in those challenges while playing.

Some of the studies, including Erlitasari and Dewi (2016), have developed integer line board media games in grade IV elementary school. Furthermore, Fathurrohman et al. (2016) has developed a labyrinth game board for calculating operating material for elementary school. Ningrum and Mariono (2016) have developed board game visual media in the material of Junior high school Algebra form, as well as Prasetyo (2018) which has developed the game of mathematical monopoly on the material of the straight line equations for class VIII junior high school. The results of the research concluded that the media created had a positive impact on students' interests and learning outcomes. Above on, several studies have proven the positive impact of using board game media on student learning outcomes, such as in physics and astronomy (Cardinot and Fairfield 2019) or library learning (Alvarez 2017). Through these existing theories and research

results, we know it is worth the development of board game for teaching and learning.

Therefore, it is expected to improve the teachers' PCK who participate in the mathematic board game designing and teaching, and when they join and playing, they will know how the board games facilitate learning interest of pupils. In addition, the board games can also be used as learning tools that are developed based on aspects of validity, practicality, and effectiveness especially for learning mathematics in Algebra material, as well as a means of training questions for the student and can be used by other teachers who can improve Learning Innovation (Andini and Yuniarta 2018). So, it is discussed to integer board game into pre-service teachers training (Avdiu 2019, Baranyai et al. 2019, Zsoldos-Marchis 2019, 2020).

For mathematics learning, a meaningful learning task is necessary. Meaningful learning tasks have the following mathematical characteristics, according to Wittmann (2010):

- (i) Elements (entities) are provided, which can be mathematically defined and which are in mathematical relations to each other.
- (ii) The elements can be dealt with using mathematical rules.
- (iii) The mathematical activity has an aim. It therefore always includes the examination of patterns and orders and problem-solving through the use of these structures.
- (iv) The mathematical learning activities need to be a foundation for future learning processes.

In summary, combining teaching aids with mathematical game rules to create an educational board game for pupils to learn in the game is a topic worth researching.

Mathematical Fraction Concept Instruction

Fraction Conceptual Development of Pupils

Piaget (1960) pointed out that the cognitive development of children is gradual. He used his theory of children's cognitive development and designed activities to study children's development of the concept of fractions, and found that the relationship between the part of perception and the whole and the subdivision of operation; there is great difference between them. Piaget et al. (1960) did a series of studies on the development process of the fraction concept of children aged 3 to 8. At the same time, they also found that children must have the following seven sub-concepts:

- (i) There must be a whole that can be divided in order to have fraction thinking.
- (ii) Fraction contains the limited number of each part, and each part must correspond to the recipient when assigning things.
- (iii) In the sub-segmentation activity, all must be exhausted and there is no remainder.

- (iv) There is a fixed relationship between the number of parts that the whole is cut into a number of cuts.
- (v) The concept of fractions means that each part after division is equal.
- (vi) When children manipulated part of the subdivided concept, they learned that the subdivided part is a part of the whole. At the same time, this subdivided part itself is also a subdivided whole.
- (vii) Because the fraction comes from the whole, the whole is always the same.

Based on the above, the concept of fraction is established from the experience of dividing into equal parts. Therefore, understanding through manipulating will be an appropriate learning process and be more suitable for the development of pupils.

Curriculum Structure of Mathematics Fraction Concept in Taiwan

Fractions often have different usages and interpretations due to different situations. Many scholars have different views on the meaning of fraction. They analyze the cognitive significance of fractions in different problem situations and all advocate that fractions have multiple meanings; some instances are shown in Table 1.

Table 1. *Different Views of Scholars of Fractions*

Scholars	Proposal Year	Meaning of fraction
Kieren	1976	Propose seven interpretations of rational numbers: fractions, decimals, ratio, ordered pairs, quotient, measures, operator.
	1980	Simplify it into five interpretations: part-whole, ratio, quotient, measures, operator
	1988	Simplify to: ratio, quotient, measures, multiplicative operators.
Behr et al.	1983	Seven different meanings of fraction: fraction measures, ratio, rate, quotient, linear coordinate, decimals, operator.
Dickson et al.	1984	different meanings of fraction: 1. Sub-area of whole region. 2. A comparison between a subset of discrete objects and the whole set. 3. A point in number line which line at intermediate point between two whole numbers. 4. The result of a division operation. 5. A way of comparing the sizes of two sets of the objects or two measurements.
Nesher	1985	There are five interpretations of fraction: part-whole, quotient, ratio, operator, probability.
Ohlsson	1988	Divide into four constructions and eleven meanings: 1. The quotient function: contains equal division (partitioning), including (extracting), shrinking (shrinking), educing. 2. Rational number: including fractions and measurement (measures). 3. A binary vector: ratio, intensive quantities, proportion, average (rate). 4. Synthesis function.

The meanings of fraction are various depend on what situation we want to describe, such like sub-sets/all sets, the result of division with two integers, ratios, averages,...etc. In the syllabus of primary school stage in Taiwan, which ages of pupils will learn the different meanings of fraction shown in Table 2.

Table 2. *Different Meanings of Fraction and Learning Age in Taiwan*

Concept of fraction	Content Example	Grade (pupil's age)
Divide Equally	How to divide 9 candies among 3 students fairly?	Grade 2 (about 7 years old)
Part/All	How to describe the result: A pizza is cut into 8 pieces, and Tom eats 1 of them. How many pizzas does Tom eat?	Grade 2 (about 7 years old)
Addition and subtraction with fraction	While the same denominators: $1/8 + 3/8 = ?$ While the different denominators: $1/4 + 1/8 = ?$	Grade 3-5 (about 8-11 years old)
proper fraction, improper fraction, fraction with integer	Proper fraction is less than 1; Improper fraction is bigger than 1 without integer; All improper fraction could be convert as proper fraction with integer.	Grade 4 (about 9 years old)
Equivalent fraction	$3/5 = (?) / 10$, what number should be written in ?	Grade 4 (about 9 years old)
The fraction is a number/a point on the number line	Draw a point on the line to show $2/6$?	Grade 4 (about 9 years old)
The result of integer division	The result of the division is expressed as a fraction while the division of two numbers cannot be divided into an integer, for example, $3 \div 9 = 3/9$	Grade 5 (about 10 years old)
Average (including rate)	Use fractions to express the result of comparing two measurement units with one of them as the benchmark. For example, rate is the result of comparing length and time.	Grade 6 (about 11 years old)
The ratio in the ratio/scale/ratio/comparison amount \div reference amount	When the result of comparing two sets or two measures, the representation of the scale and the ratio are expressed in p/q , the meaning of the fraction is the result of the comparison of the two quantities.	Grade 6 (about 11 years old)

In order to be transformed into teaching guidelines for teachers, the syllabus of mathematics is written into learning performance and learning content. Content about fraction is excerpted as in Table 3.

Table 3. Curriculum of Fraction in Primary School Grade 1-2 in Taiwan

Grade (age)	Learning content code & describe	Learning performance code & describe
Grade 1 (6)	None	n-I-6 Recognizes the unit fraction.
Grade 2 (7)	<p>N-2-9 Problem solving: segmentation fairly. Focus on operational activities. Divide pre-experience. Understand the meaning and method of equal splitting. To guide the pupils to discover the relation between the problem and the multiplication in the problem-solving process.</p> <p>N-2-10 Recognition of essential fraction: Through manipulating activities (origami as an example), guide the pupils trying to describe with fraction, like seeing the half of all and say that be “one-second”, or try to use the word “one-forth”, “one-eighth” to describe what they see in the graph if there is not fill.</p>	

This study is based on the fraction concept of grades 1-2 in Taiwan primary school stage as the learning objective. Therefore, only part of the required syllabus is listed. The learning goal of this stage is to communicate the meaning of fractions, that is, to understand the meaning of fractions and the naming of fractions, that is, to be able to write “ $\frac{1}{4}$ ” and say “ $\frac{1}{4}$ ” of the learning goals. In particular, the reading of fractions in English is to read the numerator first and then the denominator, but in Taiwan, the reading method is to read the denominator first and then the numerator. Students are expected to confirm all the cuts first, and then judge the number of parts. This part sometimes allows students to write wrong fractions or wrong reading. This part will be explained later when there is a chance.

Lack of Game-Based Fraction Learning and Board Game Designing

After collecting board games in Taiwan, they are related to the “Number”, “Amount”, and “Shape” mentioned in the mathematics curriculum. These board games are related to mathematical concepts. We call this type of board games as “Mathematics Board Games”. There are many kinds of mathematics board games. Basically, the activities that determine the winner by counting fractions, although required calculation experience to be carried out, but we excluded choices that only have this nature. The mathematics board games we referred to activities that can learn mathematical concepts during the game playing, or solving problem with mathematical concepts. Take the themes of number, amount, and shape to illustrate:

- (1)Number- “COWABANGA”: The situation is to go surfing with his own cow. The players need to control the height of the wave with the number

poker card in their hands to avoid dangerous factors in the sea and avoid injury. This board game tests the player's ability to calculate the addition of integers. When the board game is set in the retreat phase, it tests the player's ability to calculate the subtraction of integers.

- (2) Amount- "Noah's Ark": The game consists of actual, reduced animal models with different weights, and cards with animal photos. The player draws a card from the animal cards, and selects the correct animal from the animal pile according to the pattern and name on the card. Since animals are different in size and weight, pupils must maintain the balance of the Ark, so they must be carefully placed on Noah's Ark each time, and then the next pupil will draw cards to continue the game. The test is the feeling of weight.
- (3) Shape- "Geistesblitz": This board game contains five small models of different colors and tools, as well as some pictures of playing cards. In each round, a player draws a card from the card pile and puts it on the table, because the shape and color shown in the card may not be the same as the actual tool. Only one option in each card will be the same as the actual tool, the player must grab the only same tool as fast as he/she can, the winner can get a point, and then continue to the next round. This board game tests the players' quick judgment on shape and color.

There are no board games about fractions. For example, "Splittissiuo" is a board game. The game is created with round cards, which is marked with a pizza sliced in eight equal parts. There are 0, $1/8$, $2/8$, $3/8$, $4/8$, $5/8$, $6/8$, $7/8$, $8/8$ cards, if the player can combine the two cards on the table into a whole pizza, then the player can get the card back and get the scores of the game; or you can find three cards and combine them into a merged relationship.

But for the fraction board games collected so far, pupils cannot play the game if they did not have essential concept of fraction before. For example, in the rules of "Splittissiuo", how do students know which two round cards can be combined into a whole one? What about the complete drape? These mathematical concepts require experience and guidance, as well as prior experience in reading the information on the chart. Therefore, this type of game is suitable for mathematics exercises. If it is used in mathematics teaching, there will still be some shortcomings.

Although it is not possible to collect all the board games to analyze and research, it is probably understandable why no board games related to the preliminary concept of fractions in this research can be found. Because the recognition of the fraction comes from the establishment of the relationship between the total amount and the part being cut, it is difficult to emphasize the whole amount and part of the amount from the game image if there is no cutting mark.

Therefore, this research attempts to enable pupils to observe the proportion of the partial amount to the overall amount from the previous experience of dividing and equalizing in the process of the game, try to describe these phenomena that are less than 1, and learn to express it in fractions.

Materials and Methods

Design the Board Game with Fraction Concept Guiding

For learning with manipulating and playing, we must create board game that is a situation to enhance pupils to describe with fraction. As the learning goal of knowing fraction, pupils need to “listen”, “speak out”, “read” and “write” as the learning performance. So we try to set the game rule to make sure pupils could win the game if they described with fraction correctly.

How to accomplish the goal of essential fraction learning? We divide the goal into several abilities to show:

- (1) We still can count and state, while the amount less than integer 1.
- (2) Even all the appearance of amount are less than integer 1, we can arrange them according the amount and describe the result with symbols or numbers.
- (3) Through the manipulating arrangement, pupils could experience the meaning of fraction with amount.

So we try to design the board game that pupils could arrange intuitively and must to describe correctly to win the game as to achieve the learning goal.

Board Game Playing and Teaching

Instead of offering the definition, we expected pupils learn the essential fraction through observing and generalizing, not by reciting proficiently. We need to reduce the expectation for pupils to learn these just by listening to statement in the classroom, but to understand the meaning of these fractions, whether the denominator or the numerator represent. We must guiding carefully to avoid tell the definition of fraction directly and encourage pupils to describe what they see and to think how to state.

There are eight teachers who teach in primary school join into the research since board game designing, we will observe from them whether there is any change in their views on fraction teaching before and after. In addition to observing the learning effectiveness of pupils after board game learning, we also observed how teachers integrate board game activities into teaching. The teachers come from two different schools in Taichung, Taiwan. There are two teachers in School A (one is a 6th grade teacher, one is a 1st grade teacher), six are B school teachers (two are 1st grade teachers, one is a 2nd grade teacher, one teacher in grade 3, one teacher in grade 4, one teacher in charge of science teaching in grades 5 and 6).

Assessment for Board-Game Learning

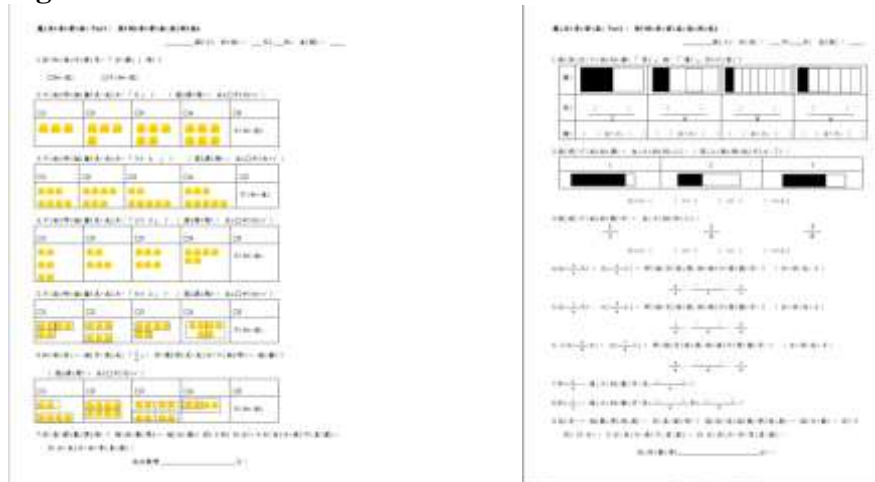
In order to be used in classrooms, we hope that the design of this math board game can enhance students' interest in learning and have learning effects.

Therefore, we hope to understand the effectiveness of students' learning through some tests and interviews, and whether students' interest in learning has improved.

Learning Effectiveness

We have made two tests, one as a pre-test to examine the students' previous experience before learning; the other as a post-test to evaluate the effectiveness after teaching and learning (Figure 2). The samples come from the primary school grade 1 to 6 (about 6 to 11 years old). The purpose is to test the pupils' ability to use symbols to represent images. Therefore, most of the questions in the test are represented with pictures and fewer words. To reduce the confusion of students answering questions, the answers are mostly design as multiple-choice or filled-in questions, without narrative questions.

Figure 2. Pre-Test and Post-Test



The pre-test is mainly to test the children's ability to use symbols to describe image representations, such as Figures 3-5.

Figure 3. '2. Which one represents "6"? Make a ✓ on your answer'

2. 下面哪個圖是表示「6」？（選擇題，在□中打✓）

□1	□2	□3	□4	□5
				不知道

Figure 4. '5. Which one represents "6 ÷ 2"? Make a ✓ on your answer'

5. 下面哪個圖是表示「6 ÷ 2」？（選擇題，在□中打✓）

□1	□2	□3	□4	□5
				不知道

Figure 5. ‘6. Which one represents “ $\frac{2}{4}$ ”? Make a ✓ on your answer’

6. 如果有一个字写成“ $\frac{2}{4}$ ”，你觉得它是表示下面哪一个图？
(选择题目，在□中打✓)

□1	□2	□3	□4	□5
				不知道

The pre-test is mainly to test the pupils’ ability to record image representations with numerical symbols, such as in Figure 2, ‘2. Which one represents “6”?’ Make a ✓ on your answer.’ And in Figure 3, ‘5. Which one represents “ $6 \div 2$ ”?’ Make a ✓ on your answer’ is used to evaluate whether students can use numbers and calculations to represent the meaning of the images. ‘6. Which one represents “ $\frac{2}{4}$ ”?’ is to assess whether students have the ability to represent images with fractions, as shown in Figure 4.

All the pre-test items can be distinguished into five dimensions, to know how pupils treat the arithmetic representation, shown in Table 4.

Table 4. Dimensions of Pre-Test

Characterization of					
Counting	Addition	Multiple	Division	Fraction	Interest
Item2	Item3	Item4	Item5	Item1, Item6	Item7

In the test after board game learning, we want to know whether pupils can use fraction to represent graphics, such as ‘1. Write a number so that the result has the same meaning as the figure, and write the spell of the fraction.’ The numerator of the answer is both 1. Will the children’s observation of the image misunderstand the number of divisions instead of the number of parts after division? ‘2. Sort the codename with the amount of each figure’ is to test whether the children’s intuitive comparison of the amount is correct. ‘3. Sort the fraction below: $\frac{1}{2}$, $\frac{1}{4}$, $\frac{3}{8}$ without figure’ is to observe whether students have a correct understanding of the amount expressed by the fraction. These are examples of test questions, and each question design has indicators to be observed (Figures 6-8).




Figure 6. Post-Test ‘1. Write a Number so that the Result has the Same Meaning as the Figure, and Write the Spell of the Fraction’

1. 請寫出：下面圖的圖「寫」與「讀」作什麼？

圖：				
寫：	$\frac{(\quad)}{2}$	$\frac{(\quad)}{4}$	$\frac{(\quad)}{8}$	$\frac{(\quad)}{6}$
讀：	() 分之 ()	() 分之 ()	() 分之 ()	() 分之 ()

Figure 7. Post-Test '2. Sort the Codename with the Amount of Each Figure'

2.請將下面的圖，由大排到小。(寫上號碼就可以~了)

1	2	3
		

大=> () => () => () => 小

Figure 8. Post-Test '3. Sort the Fraction Below: 1/2, 1/4, 3/8 without Figures'

3.請將下面的數字，由大排到小。

$\frac{1}{2}$

$\frac{1}{4}$

$\frac{3}{8}$

大=> () => () => () => 小

About the concept of fraction in the post-test, to know how pupils treat the arithmetic representation, shown in Table 5.

Table 5. Dimensions of Post-Test

Fraction Writing	Denominator	Numerator	Amount Comparing	Fractions			
				Comparing	Representation	Reduce	Expand
Item1	Item1	Item4	Item2	Item3	Item5	Item7	Item8

Learning Interest

There is only one question on the pre-test and post-test to investigate students' interest in mathematics and board games. In the pre-test, students are asked to give mathematics an "interest level" of 10 points to represent their favorites, and 0 points to dislike them very much; in the post-tests, It is to let students have an "interest score" for math board games. A score of 10 means that they like it very much, and a score of 0 means that they hate it. We then conducted interviews with several school children based on the pre- and post-tested learning effectiveness and interest scores. The distribution of the number of interviews is shown in Table 6.

Table 6. Distribution of Students Interviews

	High achievement	Low achievement
High interest	2	2
Low interest	2	2

*Achievement refer to the test grade of pupils, high will be the lead of 25%, and low will be last 25% of samples.

*Interest refers to the questionnaire result.

The sample of students in our study comes from two different schools in Taichung, Taiwan. The sample of the number of students in each school and each grade is shown in Table 7. Among them, the fourth grade children cannot cooperate with the implementation of the time, so this study did not receive any information. I hope there is a chance to add more in the future.

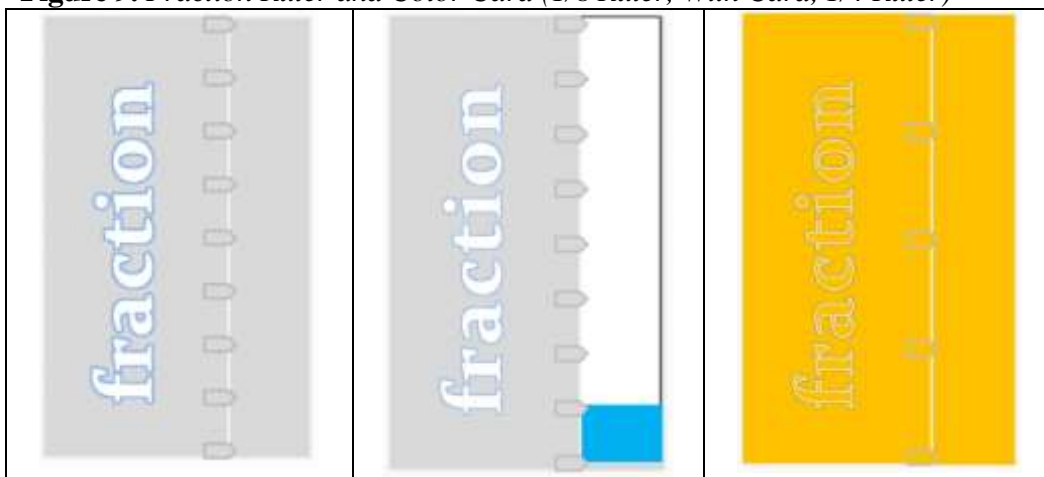
Table 7. *Pupil Sample Distribution*

School\Grade	1	2	3	4	5	6
A	17	-	-	-	-	21
B	18	15	17	-	15	11
Total	35	15	17	-	15	32

Results and Discussion

“Pull the Fraction Wall Down” - The Board Game of Fraction Design

(1) The teaching aids used in the board game include 20 cards in two colors, and the colors and amounts displayed on each card are unique and non-repetitive; there are also fraction rulers designed with equal divisions, and 36 black fraction cards include 0/8, 1/8, 2/8, 3/8, 4/8, 5/8, 6/8, 7/8, 8/8, per number 4 cards (Figure 9).

Figure 9. *Fraction Ruler and Color Card (1/8 Ruler, With Card, 1/4 Ruler)*

(2) Before the start of the game, each participant can choose five of the 20 cards, whether blue or green, and according to the amount displayed on the card, put the cards from the left to the right according small to large. When encountering the same amount, treat the blue cards as small and green as the big one. At this time, it is not possible to use fractions to describe the amount of these cards.

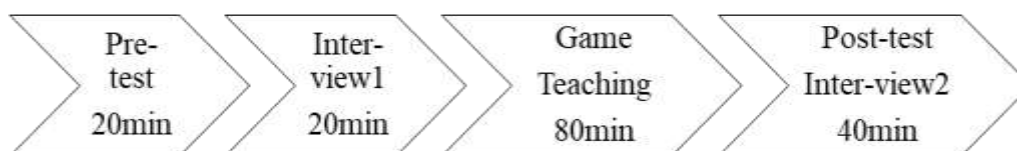
Next, put the card into the tool-fraction rulers, and a correspondence will appear. Participants can see that a card is divided into 8 grids, and the colored area occupies part of the grid. The description of this card can be described as a fraction. For example, when the card in Figure 8 is placed on the ruler, it can be seen that the spell of this card is one-eight ($1/8$).

(3) Design and learning: The goal of learning is to cultivate pupils' ability to "listen", "speak" and "read" in fractions. Therefore, these learning goals are integrated into the design of the rules of the game. In "Pull the Fraction Wall Down", each pupil has 5 fraction rulers of eight-division scale, 1 fraction ruler of four-division scale, and 1 fraction ruler of two-division scale. There are three types

of fraction cards: green, blue, and black, each Color cards have $0/8$, $1/8$, $2/8$, $3/8$, $4/8$, $5/8$, $6/8$, $7/8$, $8/8$, so there are 10 cards in each of the three colors. For fractions cards, pupils can choose five of the blue, green or mixed cards and put them in their own fractions rulers. The cards are facing and placed from left to right according to their amount. Therefore, only they know the correct spell (fraction) of this card. (Reading), these fractions are like a wall to protect yourself, the winner of the board game is the one who did not fall at the end. If you want to pull down the fraction walls of other players, you have to speak the fractions walls of other players. If your fraction wall is spelled, the fractions wall will be pulled down. We expect pupils to learn fractions in these activities.

Teaching Implement (Figure 10)

Figure 10. Flow Chart of Teaching Implement



(1) In the past, when teachers in Taiwan taught mathematics, they emphasized the definition of mathematical symbols. For example, “ a/b is meant that the ‘ a ’ parts of 1 divided into ‘ b ’ parts”. Students often ignore the “parts be divided into” when practicing reading. The habit of observing and reading out the part of the quantity first, so we expect that in the board game activities, we expect pupils to observe the equal ruler to cut the card into 8 equal parts, and then observe how many equal parts the color occupies. Speak out the denominator first, then the numerator, and finally you can say the correct fraction. But sometimes teachers still use direct teaching methods to make the game go smoothly, for example:

Student G1: Teacher, I don't know what the spell of this card is?

Teacher T3: Look, this card occupies three of the eight, so its spell is three-eighths.

We expect teachers to guide the recognition of fractions in a guiding way. Therefore, we hope that when the children cannot tell the correct fractions during the board game, the teachers will first guide the pupils to understand the scales they use and confirm the denominator. Then, look at the numerator, that is, the number of squares that the color occupies, and combine the denominator and numerator to form the correct fraction as a spell, extending from the correct spell rules to the correct fraction reading.

(2) The rule design of the board game is to sort the cards by size before performing activities. Therefore, students can guess the correct card spells by this rule, for example, between three-eighths and five-eighths cards, except Outside of the special rules card, it should be four-eighths. Let the children experience the relationship between the actual size sorting and the fractions sorting. When comparing with the denominator fraction, the larger the numerator, the larger the

fraction. But when the teacher wants to assist the children, he directly brings the relationship between the fraction into the game guide, for example:

Teacher T4: Dear, what's the middle between 3 and 5? So how much is between three-eighths and five-eighths? You are really good, and you will know what spell to use to attack this card next time.

Although the teacher's guidance is quite fast, it ignores the guesswork of the pupils. The number of integer points is indeed the ordinal number of 3, 4, 5..., but it is not helpful in establishing the sense of the quantity of the fraction. For example, if when he is using a four-equivalent ruler, when a four-eighths card is put into the four-element ruler, the fractions that will appear should be two-quarters. At this time, the pupils follow the teacher's Guiding, answering four-quarters, which is not surprising. Therefore, we expect the teacher to guide the students to guess the amount of change before interpreting the fractions. For example: "Boys and Girls, this eighth grid is full of three grids, this eighth grid is full of five grids, which card will be between the situation? There are four squares in the eight squares? Two squares in the four squares? So what is the fraction spell of this card?" Let the pupils experience the inference of the quantity and the reading of numbers at the same time.

(3) In the process of preparing lessons, the teacher believes that it does not take too much time to learn the unit fractions that numerator is 1, because the denominator can be confirmed by cutting the items into several equal parts, and the numerator can be confirmed by taking out several equal parts. The points experience goes to the points of the denominator and numerator, and it does not take much time to learn. Since the education of primary schools in Taiwan is a staged education, the six grades of primary schools are divided into three stages. Each stage will be reclassified and teachers will be reassigned to teach mathematics. The advantage is that students can adapt to different situations. For group opportunities, you can also try different learning methods and learning environments, but the mathematics curriculum is continuous, and the conclusions of learning will not vary from person to person. Therefore, if the learning fractions is an integer for the learning fractions, then the pupils will learn the concept reached is not a partial quantity of the whole quantity, but an explanation of the proportional relationship between the large whole and the small whole, and the pupils do not know what that means. We emphasize the correct reading of practice fractions, which is a conventional way, so we have integrated into the spells of the magic world. After all, if the spells are misspelt, their magic will not be able to achieve their wishes.

Learning

In the Learning Achievement Part of the Fraction

In the pre-test, we designed some questions to examine some of the students' pre-learning experience, such as knowing the fractions, counting numbers, knowing the signs of addition, knowing the signs of multiplication, knowing the signs of division, knowing the signs of fractions, etc., corresponding to each grade

performance, expressed in terms of correct answer rate (number of correct answer samples/number of subjects), and the results are shown in Table 8.

Table 8. Results of Pre-Test

Item Sch-Gra	N	Heard Fractions	Characterization of				
			Counting	Addition	Multiple	Division	Fraction
A-1	17	76.5%	94.1%	82.4%	5.9%	35.3%	11.8
B-1	21	77.8%	88.9%	100%	11.1%	27.8%	33.3%
B-2	18	86.7%	100%	93.3%	40.0%	26.7%	33.3%
B-3	15	94.1%	100%	94.1%	41.2%	76.5%	47.1%
B-5	17	100%	100%	73.3%	60.0%	93.3%	66.7%
A-6	15	90.5%	95.2%	71.4%	38.1%	76.2%	52.4%
B-6	11	100%	100%	100%	45.5%	72.7%	63.6%

In Table 8, we can see that the first grade (A-1, B-1) and second grade (B-2) pupils are not very familiar with the representation of multiplication and division, which is in line with the level of students at this stage; Have you ever heard of fractions? There is a clear difference from knowing the representations of fractions. This also shows that students know the fractions but do not know the meaning of the fractions. In the third to sixth grades (B-3, B-5, A-6, B-6) students should have learned fractions according to their school age, but in the representation of fractions, there is no obvious high achievement. This phenomenon may come from the experience of pupils learning fractions and tests the characterization is different.

In the post-test, we design some questions to detect how children write fractions, recognize reading denominators, recognize reading numerators, compare quantities, represent fractions, reduce equivalence, and expand equivalence after board games. The performance is expressed in terms of the correct rate (number of correct answer samples/number of subjects sampled), and the results are shown in Table 9.

Table 9. Results of Post-Test

Item Sch-Gra	N	Fraction Writing	Denominator	Numerator	Amount Comparing	Fractions			
						Comparing	Representation	Reduce	Expand
A-1	17	27.9%	47.1%	14.7%	82.4%	3.9%	76.5%	0%	14.7%
B-1	21	16.7%	84.7%	19.4%	66.7%	0%	85.2%	0%	30.6%
B-2	18	31.7%	66.7%	21.7%	100%	0%	93.3%	0%	6.7%
B-3	15	72.1%	86.8%	72.1%	88.2%	11.7%	98.0%	29.3%	50.0%
B-5	17	98.3%	100%	98.3%	100%	84.4%	100%	86.7%	86.7%
A-6	15	100%	95.2%	95.2%	95.2%	76.2%	100%	100%	100%
B-6	11	90.9%	100%	91.0%	90.1%	48.5%	97.0%	81.8%	81.8%

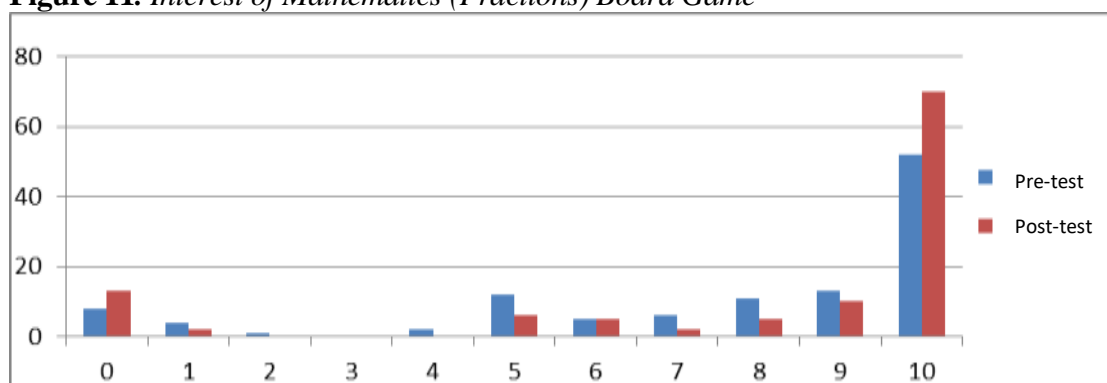
In Table 9, it is worth noting that the first grade (A-1, B-1) and second grade (B-2) pupils can use fractions to express the amount of what they see. There is no obvious problem with the intuitive comparison of the pupil's presence, but if the comparison is based on fractions alone, the results have not been seen. In addition, when fractions interpreting and reading, the accuracy of the denominator is higher than that of the numerator. It can be guessed that the pupils have already observed

how many equal parts of the whole quantity are, but further guidance is needed in the interpretation of the numerator. What is in line with expectations is that pupils have not yet had a clear learning effect on fractions writing. This involves the recording of fractions and needs to be strengthened after being integrated into the mathematics curriculum. In the evaluation of value equivalent fractions, the expanded fractions have begun to be interpreted by pupils, but the reduction of fractions is more difficult for them.

In the Learning Interest of the Fractions

We interviewed the pupils about their interest in mathematics in the pre-test and post-test respectively. 10 points means that they are very interested, and zero point means that they are very annoying. For the statistical results, we use histograms to represent the results of the before and after tests, as shown in Figure 11.

Figure 11. *Interest of Mathematics (Fractions) Board Game*



We can find that the number of students who are very interested in mathematics learning through board games has increased significantly, while the number of pupils in the middle distribution has decreased. Although this is only a simple statistical analysis method, it can be seen that the way of learning mathematics through games can trigger the learning motivation of pupils. Even though they still know, the content of game playing is about the concept of mathematics. We interviewed several pupils from high achievement and high interest, high achievement and low interest, low achievement and high interest, low achievement and low interest. We found that regardless of whether the pupils have achieved high or low level of achievement, they are still playing games and highly interested.

For high-achieving pupils, most of them can share ways to win, such as:

StG101: I guess. Because it is from small to large, if I already know one of the cards, I can guess that the two sides of this card will be plus or minus one, just like next to five-eighths, one It may be six-eighths, and the other side may be four-eighths. I usually guess right. This is the method I found myself, and I am very happy.

StG601: The order of the cards is regular, the colors are also regular, and there is only one card. I can see my own cards, so I know their cards must not have these five

cards. If you add some reminder cards, I can guess what their card is. After playing it twice, I can win every time. I think I have found a way to win the game.

For pupils with low learning achievement, they provide more intuition and less thinking, but they still have the motivation to win:

StG201: I don't know what card they have, so I lock a card that I don't have. When it's my turn, I will guess everyone and I will always guess right. If others have guessed, I will remember, don't try to guess the same card or the same fraction again, it will be more accurate.

StG301: If I have any card in my hand, I think I will win better. Because other people's cards must be arranged in order, I can specifically find the same color to attack until all the fractions of that color are found. Although you can't win every time, at least it's not the first to get out.

Among the high-achieving and low-interest pupils, the special thing is that these pupils liked mathematics at first, but in the post-test they said they didn't like this board game, and they were all pupils who had already studied fractions and didn't like this. The reason for board games comes from not being good at games, even though they already know the rules well:

StG602: I don't like playing this math board game. This is too simple. They always guessed my card, and they only attacked my card, so that my card was pushed down quickly, and because it was pushed down, the other cards were easier to guess out. In addition, unfortunately, I have not been able to draw any cards, so it is easier to be guessed in the order, and I can only be in a daze after being out. I don't like that there is nothing to do in math class.

StG501: Others said that my achievement in math is very good. This is a math game, so they are very afraid that I will win, so they all want to knock down my card first. Sometimes I was out of luck, and I got consecutive cards, and my cards were knocked down before the round was finished. In fact, this board game has nothing to do with math fraction, because I don't think it needs calculations, so I can't perform well.

Among the low-achievement and low-interest students, the performance is quite similar to the high-achievement and low-interest students:

StG201: They all guess my card first, they only attack my card, it's not fun.

StG102: I will forget the card I guessed before, or I accidentally tell my own card, and then I lose. If there is a chance to play, I will pay more attention.

In the surveys and interviews of school children's interests, it can be found that pupils are willing to continue to learn in board game activities. Although their learning achievements have not been significantly improved, if they can maintain their learning motivation, let them continue to practice, continue to accept the teacher's guidance, perhaps more time, the learning effect can be more easily observed.

Figure 12. Board Game Playing and Teaching

Conclusions

1. It is feasible to integrate board games into mathematic learning and teaching.

Learning through board games can promote the pupils' learning motivation, the same results as other related researches can be discovered from the post-test and interview content of respondents. Besides, the pupils' learning achievement through the board game we designed is very obviously. The aim of this board game is let the pupils could describe the incomplete amount in fractions, the results of pre-test show that pupils of grade-1 and grade-2 do not know division yet, but they could answer the questions in fractions. Therefore, it is effective for pupils to learn describing in fraction through guiding the board game playing.

In the pre-test implemented before board game playing, different from pupils in other grades, the results show that grade-1 and grade-2 can't represent fraction correctly even they say that they have heard fraction. The pupils of grade-3 to grade-6 should have learned the concept of fraction and know what the fraction means, the difference is indeed found in the pre-test. Then, after learning how to play board game not fractions teaching, all pupils have improved their accuracy in answer fraction questions, especially grade-1 and grade-2 pupils, who have made significant progress. Judging from the data this time, although the collection and analysis methods of the research are relatively rough, It is worth studying how to integrate the correct mathematical concepts into the board games, let pupils to learn mathematics and practice to form concepts through playing board games.

The design of the board game in this study is limited by hardware factors. It's a pity that design only fit the fractions with denominators of 8, 4, and 2, but cannot extend and infer fractions with other denominators. But as an initial activity for pupils to recognize fractions, such a board game design is interesting and meaningful.

2. The board game rules are set so that pupils can learn more mathematical concepts in the process of operating teaching aids.

The learning goal set in this study is to learn how to describe the amount with fractions during the game stage, therefore, in the rules of the game, the pupils must have the ability to guess the amount of the card say the fraction represented in order to get victory of the game. But in order to be able to guess all the fraction cards more efficiently, pupils must be able to formulate strategies and not guess without regular pattern. For example, they can observe the strategies adopted by the pupils and the concepts they may learn:

1. Since the design of the cards in three different colors or amount, all cards will appear once. Pupils can use the cards that have already appeared to determine which cards do not need to be guessed for reducing the mistakes, and pupils can experience the probability of the game.
2. While two fraction cards embedded one unknown, for example, the unknown card between $\frac{3}{8}$ and $\frac{5}{8}$, which fraction do you guess? Just think the position, the answer will be bigger than $\frac{3}{8}$ but smaller than $\frac{5}{8}$. Pupils can answer $\frac{4}{8}$ instead $\frac{5}{9}$, that could be seen the learning through board games, which can avoid the mistakes made of they don't have a sense of number and quantity.
3. Pupils can experience the existence of value equivalent fractions through the manipulating teaching aids. For example, a card with a coverage area of half. If the unknown card is between $\frac{3}{5}$ and $\frac{5}{8}$, the pupils can judge the unknown card represents $\frac{4}{8}$, which means that pupils can see the sorting method of "same denominator" and "different numerator"; in addition, in the advanced game, this card is put into a fraction ruler with denominator of 2. Above, some pupils will also use $\frac{1}{2}$ to answer the guessed result. This allows pupils to experience the existence of fractions with different denominators.

Therefore, under the rules of board game with card sorted by size and different fraction rulers, the pupils can learn the notion of fractions beyond their expectation in order to obtain the strategies generated by the victor.

3. The fun-oriented learning comes from the fun-oriented teaching design

Game-based learning needs to be designed in order not to deviate from the purpose of education, the key points of teachers' teaching will be how to facilitate pupils thinking instead of reciting. However, if teachers talk about too many definitions in the process of games guiding, pupils' learning will just conclude some words and behaviors training by imitating without thinking logically that mathematics study pays attention to, then this kind of mathematics teaching and learning cannot be said to be interesting, because we would not think that memorizing the provisions of the pattern is an entertaining learning. Therefore, in order to make teaching joyful, we need to design close to the learning objectives,

discuss how to incorporate the performance of learning into the rules of the game, and show the effectiveness of learning during the game. These are things that need time to design, and it takes time to prove it.

In this study, most of the time was used for board game activities, teachers' teaching was only focus on guiding with game rules, and there was no opportunity for extended discussions on fractions. Therefore, if the effectiveness of fractions learning needed to be strengthened, such as writing method, or as well as different denominators but value equivalent fractions judgments, all have to be guided by teachers using time and not included in this board game learning activity. In the process of board games, it can be seen that pupils can maintain a certain learning motivation, and how teachers can continue their motivation to deepen and broaden learning, and continue to add some gamification elements, all the information perhaps as reference for teachers incorporate them into their own teaching design.

4. The study methods of pupils' learning effectiveness and learning interest could to be refined

As mentioned in the literature discussion, the concept of fractions will be different at each school stage. Fractions do not only mean that part of the quantity occupies the whole, but the concept of fractions will affect how pupils using fractions to solve problems. At present, this research only examines the pupils' recognition of fractions, include their understanding of denominators and numerators, and their initial experience of different denominators and value equivalent fractions. The test questions used have not been analyzed for validity, and the concept of fractions has not been comprehensively studied. Applied analysis, although it is limited by the low literacy rate of the grade-1 and grade-2 pupils and the lack of life situations, the use of these test questions to illustrate the effectiveness of the pupils' board game learning is also quite weak in argumentation. Therefore, researchers look forward to integrating board games into formal teaching in the future. The learning effectiveness can be measured along with regular assessments of primary schools. The comparison between pupils who are integrated into the study of board games and the samples that are not integrated into the study of board games can be analyzed and compared. Yes, there should be more information about differences in learning effectiveness.

In addition, with regard to teachers who use board games to integrate mathematics teaching, what researchers expect is to enhance students' learning effectiveness and interest in learning, and it is also a proof of effective mathematics teaching. Therefore, whether it has an impact on the connotation of teachers' pedagogical content knowledge should also be studied, and that will be one of the key points for the researchers to understand deeply. After all, education has no other but love and role models. It can lead mathematics into an interesting subject, and teachers will guide pupils' interest in mathematics learning. In the future, we can conduct interviews with mathematics teachers who apply game-based teaching, analyze their differences, and use them as a basis for enhancing mathematics teachers' abilities.

References

- Alvarez V (2017) Engaging students in the library through tabletop gaming. *Knowledge Quest* 45(4): 40–48.
- Andini M, Yunianta TNH (2018) The development of board game “the adventure of algebra” in the senior high school mathematics learning. *AI-Jabar: Jurnal Pendidikan Matematika* 9(2): 95–109.
- Avdiu E (2019) Game-based learning practices in Austrian elementary schools. *Educational Process: International Journal* 8(3): 196–206.
- Baranyai T, Egri E, Molnar AE, Zsoldos-Marchis I (2019) Mental calculation strategies used by pre-service primary school teachers. In *Proceedings of the 11th International Conference on Education and New Learning Technologies*, 8717–8724.
- Behr MJ, Lesh R, Post TR, Silver EA (1983) Rational number concepts. In R Lesh, M Landau (eds.), *Acquisition of Mathematics Concepts and Processes*, 91–126. New York: Academic Press.
- Cardinot A, Fairfield JA (2019) Game-based learning to engage students with physics and astronomy using a board game. *International Journal of Game-Based Learning* 9(1): 42–57.
- Chang C-Y (Ed.) (2018) *The trends in international mathematics and science studies 2015 national report*. Taipei: Science Education Center, National Taiwan Normal University.
- Dickson L, Brown M, Gibson O (1984) *Children learning mathematics: a teachers' guide to recent research*. London: HOLT.
- Erlitasari ND, Dewi U (2016) *Pengembangan Media Board Game Garis Bilangan Materi Bilangan bulat Mata Pembelajaran Matematika Kelas IV SDN Ngampelsari Candi Sidoarjo. J. Mhs.* (Development of media board game about number line material integer mathematics class IV Elementary School in Ngampelsari Candi Sidoarjo. J. Mhs). UNESA, 1–12.
- Fathurrohman M, Nindiasari H, Rahayu I (2016) *Pengembangan Board Game Matematika Di SD Negeri Wadasari Kabupaten Serang.* (Develop mathematics board games in SD Negeri Wadasari, Serang Regency). Eprints UNY, 465–472.
- Games A, Squire KD (2011) Searching for the fun in learning: a historical perspective on the evolution of educational video games. In S Tobias, JD Fletcher (eds.), *Computer Games and Instruction*, 17–46. Charlotte, NC: Information.
- Garris R, Ahlers R, Driskell JE (2002) Games, motivation and learning, simulation & gaming; an interdisciplinary. *Journal of Theory, Practice and Research* 33(4): 441–467.
- Hou H-Z (2016) *Game-based learning*. Taipei: World of Parents.
- Kieren TE (1976) On the mathematical, cognitive, and instructional foundations of rational numbers. In R Lesh (ed.), *Number and Measurement: Papers from a Research Workshop*, 101–144. Columbus, OH: ERIC/SMEAC.
- Kieren TE (1980) The rational number construct – Its elements and mechanisms. In TE Kieren (ed.), *Recent Research on Number Learning*, 125–150. Columbus: ERIC/SMEAC.
- Kieren TE (1988) Personal knowledge of rational numbers: its intuitive and formal development. In J Hiebert, M Behr (eds.), *Number Concepts and Operations in the Middle Grades*, 162–181. Reston, VA: National Council of Teachers of Mathematics.
- Ministry of Education (2018) *Curriculum guidelines of 12-year basic education-mathematics*. R.O.C.
- Nesher P (1985) The development of semantic categories for addition and subtraction. *Educational Studies in Mathematics* 13(4): 373–394.

- Ningrum SS, Mariono A (2016) *Pengembang Media Visual Papan Permainan Pada Materi Bentuk Aljabar Mata Pelajaran Matematika Kelas VII SMP Siti Aminah Surabaya*. (Develop board games with visual media for learning algebra in mathematics for seven grade students in SMP Siti Aminah Surabaya). J. Mhs. UNESA 7.
- Ohlsson, S. (1988). Mathematical meaning and applicational meaning in the semantics of fractions and related concepts. In J Hibert, M Behr (eds.), *Number Concepts and Operations in the Middle Grades*, 53–92. Reston, VA: National Council of Teacher of Mathematics.
- Perrotta C, Featherstone G, Aston H, Houthton E (2013) *Game-based learning latest evidence and future directions*. NFER Research Programme: Innovation in Education. Slough: NFER.
- Piaget J, Inhelder B, Szeminska A (1960) *The child's conception of geometry*. New York: Basic Books.
- Plass JL, Perlin K, Nordlinger J (2010) The games for learning institute: research on design patterns for effective educational games. Paper Presented at the *Game Developers Conference*. San Francisco, CA.
- Plass JL, Homer BD, Kinzer CK (2015) Foundations of game-based learning. *Educational Psychologist* 50(4): 258–283.
- Prasetyo MF (2018) Persamaan Garis Lurus bagi Siswa Kelas VIII SMP Negeri. (Straight-line equation for junior high school students of eighth grade). *MAJU: Jurnal Ilmiah Pendidikan Matematika* 5(1): 14–26.
- Prensky M (2011) Comments on research comparing games to other instructional methods. In S Tobias, JD Fletcher (eds.), *Computer Games and Instruction*, 251–278. Charlotte, NC: Information.
- Sadiman AS, Raharjo R, Haryono A (1990) *Media Pendidikan: pengertian, pengembangan, dan pemanfaatannya*. (Educational media: understanding, development and use). 1st Edition. Jakarta: CV. Rajawali.
- Scorviano M (2010) Sejarah Board Game dan Psikologi Permainan. (The history of board games and gaming psychology). Retrieved from: <http://www.tnol.co.id/games-jackmilyarder/board-game-history.html>. [Accessed 4 April 2019]
- Shaffer DW (2006) *How computer games help children learn?* New York: Palgrave Macmillan.
- Sharma M (2012) *Prerequisite skills and mathematics learning: role of games in learning mathematics*. Mathematics for All Center for Teaching/Learning of Mathematics, hlm. 4.
- Shulman LS (1986) Paradigms and research programs for the study of teaching. In MC Wittrock (ed.), *Handbook of Research on Teaching*. 3rd Edition. New York: Macmillan.
- TIMSS (2011, 2015, 2019) Taiwan International Large-Scale Study Center (TILSSC) Web: <https://tilssc.naer.edu.tw/timss>. Taiwan: TIMSS.
- Tobias S, Fletcher JD, Alexander PW (2014) Game-based learning. In JM Spector et al. (eds.), *Handbook of Research on Educational Communications and Technology*, 485–503. New York.
- Wittmann EC (2010) Grundsatzliche Überlegungen zur frühkindlichen Bildung in der Mathematik. (Basic considerations of mathematics education for children). In M Stamm, D Edelmann (eds.), *Frühkindliche Bildung, Betreuung und Erziehung. Was kann die Schweiz lernen?*, 177–195. Zurich: Ruegger.
- Wu CH (2011) *A study of the type of board game participation effect on the communication skills- Taking customer in board game stores in Taipei area for*

example. Unpublished Master Dissertation. Taipei, Taiwan: National Taiwan Normal University.

Zsoldos-Marchis I (2019) Designing board-games for developing pre-service primary school teachers' mental calculation skills. In *EduLearn 19 Proceedings*, 7757–7765.

Zsoldos-Marchis I (2020) Pre-service primary school teachers' opinion about board-games in developing mental computation skills. *PedActa* 10(2): 1–12.