Report on the 2023 CIMPA school “Blockchain in Theory and Real Applications”

Preliminaries.
The submission of the school was done in October 2021 more than two years ago. From the original submissions there have been several important changes. The submission was planned with the former director of AIMS Barry Green and the academic director of the institute Simukai Utete. The director retired from his position, and Simukai Utete resigned as co-organizer of the school. Luckily the new director of AIMS Ulrich Paquet, took also the place of Simukai Utete and became the co-organizer of the CIMPA school.

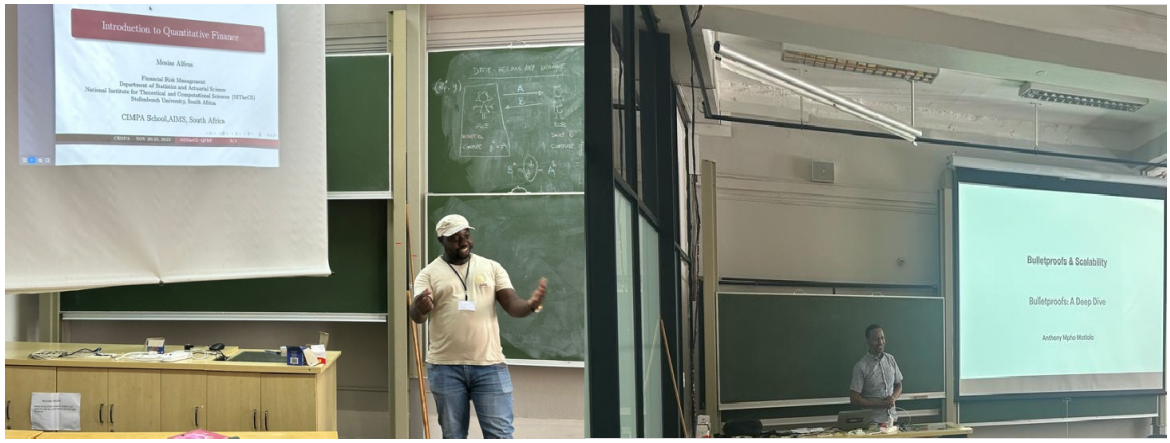
There were also changes in the list of the speakers. Primavera de Filippi could not come for personal reasons.
For Matan Fields, original from Israel, the reasons not to come are related with the conflict with Palestine.
And we had new speakers, that inspired the students. Concretely Jules Mba, Anthony Matlala and Mesias Alfeus, all the three of them original from African countries and working in South Africa were an example for the students.

Description.

The CIMPA school took place at the Institute of Mathematical Sciences (AIMS) at Muizenberg in Cape Town, South Africa. All the participants were hosted at AIMS while the speakers were hosted at closed by accommodations. The activities for the school started on the 20 November 2023. The lectures started every day at 09:00am and run till 17:00 (see the schedule attached to this report).
Participants from all over Africa, Benin, Cameroon, Democratic Republic of Congo, Senegal, Nigeria Madagascar and South Africa, as well as from India, took part to this workshop and were very delighted by such opportunity offered to them by CIMPA. A detailed list of participants is at the end of the document

Ranging from Cryptography, Zero-knowledge Proof to Decentralized Finance (DeFi), the participants were exposed to cutting-edge concepts driving the Blockchain technology and cryptocurrency space. The late afternoon sessions were conducted in the lab were participants had hands-on writing a smart contract in Solidity language, and compiling and

deploying it on the testnet Sepolia through Remix which is an online development environment for smart contract. The participants were also exposed to Hardhat which is a local development environment for Ethereum software and differs from Remix in its syntax and methods for creating and deploying smart contracts, sending transactions, and calling functions. Using Hardhat, the participants were able to build a basic decentralized exchange.
One of the concepts amply discussed during the workshop was the zero-knowledge proofs. Zero- knowledge proofs are cryptographic protocols that allow one party to prove to another that a statement is true, without revealing any information beyond the validity of the statement. To generate such proofs, the participants were exposed to Circom which is a programming language and a compiler for designing and creating arithmetic circuits that can be used to generate zero-knowledge proofs. The slides of the courses can be found at the web page of the school, below, and a list of the speakers can be found at the end of the document.
https://sites.google.com/aims.ac.za/cimpaschool-blockchainintheory/home



Opening Ceremony.

The opening ceremony was held on Friday 24 November. We count with the special guests Jesús Silva Fernández, the Spanish General Consul, Prof. David Holgate, Chair of the AIMS Council, and Mr Prof. Barry Green former director of AIMS who guided the ceremony. We were privileged to have the famous young Dutch opera singer, Amira Willighagen who was performing live. We thank her very much for her uninterested performance.
Amira also held a Q&A session on Saturday morning after given an overview of her success trajectory. This session was facilitated by Jorge Urroz.

Special session.

Soon after the Q&A session with Amira, participants were introduced to the conference “the mathematics of music” çby Prof. Zurab Janelidze from the University of Stellenbosch. The conference included a marvelous, improvised song, constructed by a tree graph with lyrics done by the participants and sang by Amira Willihagen.

The Saturday program closes with an Olympiad session facilitated by Zurab and Cerene (from the University of Kwazulu-Natal). During the Olympiad, participants were requested to provide 10 keywords (Algorithm, Entropy, Blockchain, Algebraic structure, Hash function, Factorization, Partial derivatives, Complexity, Graph, Likelihood function) linked to the concepts discussed so far in the first week of the workshop. Participants formed 5 groups (P2P, Alpha, Freedom, Vram and the Sharks) and each group selected three keywords out of the ten.

	P2P	Alpha	Freedom	Vram	Sharks
Keyword 1	Blockchain	Algorithm	Blockchain	Algebraic structure	Entropy
Keyword 2	Algorithm	Entropy	Hash function	Factorization	Blockchain
Keyword 3	Hash function	Hash function	Factorization	Graph	Partial derivatives

The exercise consisted for each group to formulate a research topic from the selected keywords and give a short presentation before the judges consisting of Jordi, Vlad and Jules. The following table present the topic formulated by each group.

	Topic
P2P	How can the integration of an advanced hash function and algorithm enhance security efficiency and scalability of the blockchain system?
Alpha	How to use blockchain enabled algorithm to enhance electricity process?
Freedom	How can blockchain improve the equal distribution of energy in Africa?
Vram	How to solve factorization problem?
Sharks	Measuring entropy: Is it possible to redesign the transaction encoding model of an existing blockchain so that the amount of data sent to the network is minimized using a function that uses partial derivatives?

During the presentation, each group was assessed based on the originality and interest of its topic as well as the sound motivation provided. Freedom came out to be the leading group while P2P held the last position. Engaging participants in this way was really an interesting exercise.

Career path.

On Friday 01 December, after the morning lecture, the career path in the blockchain space was presented by Anthony. While narrating how he navigated his way in the blockchain space, he articulated the importance of mathematics in understanding the underlying principles of the blockchain technology. An opportunity was given to each participant to express their dream career and how they are working towards it.

Budget.

The school was supported by CIMPA with 11K, AIMS with 15K, Polygon with 7K and IMU with 4k. Appart from the CIMPA support the rest was transferred to an account from AIMS and all the expenses were handled by the account manager at AIMS. A detailed report on the expenses will be prepared by them.

Newsletter.

To make accessible to a wide public AIMS has created a link on its newsletter including a short description of the school at https://aims.ac.za/2023/12/01/cimpa-school-2023/, as well as the web page with the whole contents of the school

https://sites.google.com/aims.ac.za/cimpaschool-blockchainintheory/home

Acknowledgment.

We sincerely thank all the following institutions.
We would like to thank CIMPA for its constant resolution to advance knowledge through various school. We would like to thank IMU for its financial support, in this occasion, as well as its many programs to spread science in underdeveloping countries.
We would like to thank AIMS South Africa for hosting us during the entire period of school. Last, but not least we would to thank Polygon. This school is a project in cooperation with them. We had their notable scientific contribution and its financial support to bring the speakers to South Africa.

Schedule of the school.

SCHEDULE.

Cimpa School South Africa.

AIMS
Date: From November 20 to December, 1, 2023.

	9:00-10:30	Coffee	11:00-13:00	Lunch	13:30-15:00	tea	15:20-16:50	17:00-18:00
20, Monday.	Marta		Jorge		Marta		Mesias	Exer-Jorge
21, Tuesday.	Marta.		Mesias		Marta		Jorge	Lab-Marta
22, Wednesday.	Jose		Jorge		Jose		Mesias	Lab
23, Thursday.	Jose		Jorge		Jose		Jose	Lab-Jose
24, Friday.	Jose		Jorge		Jose	——–	Opening Ceremony	———
25, Saturday	Program	below					Free	afternoon
26, Sunday					Free			
27, Monday	Jordi		Marc		Jordi		Lab	Lab
28, Tuesday	Jordi		Marc		Jordi		Lab	Lab
29, Wednesday	Jules		Marc		Anthony		Lab	Lab
30, Thursday	Jules		Marc		Anthony		Lab	Lab
1, Friday	Jules		Anthony		Students P∗.		Students P∗.	

Program for Saturday 25.

09h00 – 09h30 Amira to interact with the students 09h30 – 10h30 Zurab talk + Q&A 10h30 –10h45 TEA and snacks 10h45 – 13h00 Olympiad 13h00 – 14h00 LUNCH 14h00 – 15h00 Olympiad

Presentations. On the afternoon of Friday 1, the students will make a short presentation on what they learnt at the school

Lab Sessions. The lab will be for the practical parts of the courses. There will be one speaker during each session.

List of Participants.

CIMPA Supported Participants

Surname	Name	Gender	Email	Foreign/Local
K. Lutala	N. Junior	M	nkaningini@aimsammi.org	F
Ilunga	Godwill	M	ilungagodwill@gmail.com	F
MOUSSE	A. Mikael	M	mikael.mousse@gmail.com	F
deep Kaur	Suman	F	sumandeepkaur.puchd@gmail.com	F
Rasolofoniaina	K. Christel	F	christel.rasolofoniaina@univ-antananarivo.mg	F (Good)
Abubakar	Abdulrazak	M	razi4sure28@gmail.com	L
Mangezi	L. Munesushe	M	lmangezi7@gmail.com	L
Ngwenya	N. Sibahle	F	nokulindasibahlengwenya@gmail.com	L
Pato	Sikhanyiselwe	F	sikhanyiselwepatp@gmail.com	L

IMU Supported Participants

Surname	Name	Gender	Email	Foreign/Remark
Andriasolofo	H. Daniel	M	aheritianad@gmail.com	F (Good)
SARRE	Tony	F	tony.sarre@aims-senegal.org	F
Jonathan	K. Ntumbwa	M	jonathankabemba4100@gmail.com	F
chezeu	vanessa	F	cheuzeuvanessa@gmail.com	F

Non Supported Foreign Participants

Surname	Name	Gender	Email	Remark
Adebisi	Abimbola	F	latifat.abimbola@tech-u.edu.ng	(Should be supported by CIMPA)

Non Supported Local Participants

Surname	Name	Gender	Email	Local/Remark
Herimanana	Volana	F	Volana@aims.ac.za	L
Voalaza	Aubert	M	Aubert@aims.ac.za	L (Good)
Juma	Knight	F	Knight@aims.ac.za	L
Melchior	N'Bouke	M	Melchior@aims.ac.za	L
Rakotondratoetra	Meva	F	Meva@aims.ac.za	L (V Good)
Delien	Delien	M	Delien@aims.ac.za	L
Zeinab	Mohamed	F	Zeinabm@aims.ac.za	L (Good)
Razanaparany	Mickaya	M	mickaya@aims.ac.za	L

Speakers

Surname	Name	Gender	Email	Lecture
Urroz	Jorge	M	jorge.urroz@upm.es	Cryptography
Mba	Jules	M	jmba@uj.ac.za	Automated Market
Belles	Marta	F	marta@dusk.network	Zero Knowledge
Muñoz	Jose	M	jose.luis.munoz@upc.edu	Distributed Ledgers
Baylina	Jordi	M	jordi@baylina.cat	Smart Contracts
Matlala	Anthony	M	tonymmatlala@gmail.com	Bullet Proofs
Guzmán	Marc	M	marcguzmanalbiol@gmail.com	Tools of ZKPS
Mesias	Alfeus	M	mesias@sun.ac.za	Quantitative Finance