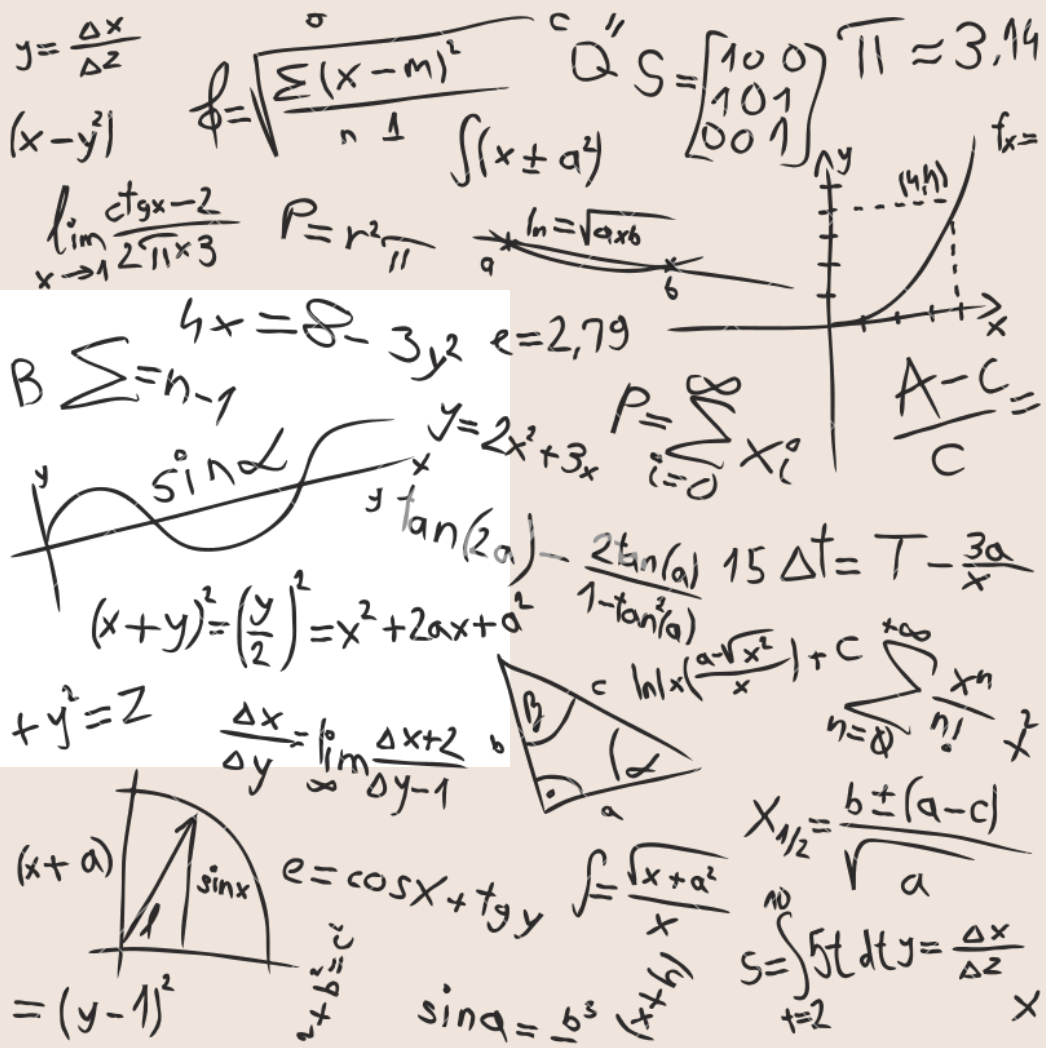
Le Photon



N°34 - 2023

BULLETIN DE L'ASSOCIATION DES ANCIEN·NES ÉTUDIANT·ES ET COLLABORATEUR·TRICES DU DÉPARTEMENT DE PHYSIQUE DE L'UNIVERSITÉ DE FRIBOURG

Comité de l'Association des ancien·ne·s étudiant·e·s et collaborateurs·trices du Département de physique de Fribourg

Comité du Photon

Président	Roland-Pierre Pillonel-Wyrsch
Vice-présidente	Marie-Laure Mottas
Caissier	Stefan Tresch
Rédactrices (français)	Eliane Esseiva et Amandine Pinard
Rédacteur (allemand)	Peter Stadlin
Président du Dép. de Physique	Guillermo Acuña
Membre du comité	Aloïs Raemy
Membre du comité	Roger Röthlisberger
Membre du comité	Lukas Schaller

Administration du Photon

Amandine – mise en page	amandine.pinard@unifr.ch
Doriana Pedrioli – envoi	doriana.pedrioli@unifr.ch

UNIFR - Département de Physique - Chemin du Musée 3 - 1700 Fribourg

Editorial

Dr Roland-Pierre Pillonel-Wyrsch

Pour les ancien·ne·s du Département de physique, l'année 2023 restera endeuillée par les décès de deux personnes qui auront largement marqué la formation et la recherche en Physique à l'Université de Fribourg : le Photon a la douleur de devoir présenter ses condoléances à tous les ami·e·s et proches de Messieurs les Professeurs Schneuwly et Baeriswyl.

M. Prof Hubert Schneuwly était entré à l'Université de Fribourg en 1957 comme étudiant et ne l'a plus vraiment quittée même après sa retraite en 2002 : plus de 60 ans de fidélité, liée à une volonté sans faille de mieux comprendre le monde. « Comprendre » était en effet son maître mot, et son approche de la physique a toujours été accompagnée d'une bonne dose de philosophie. Il s'en est allé l'année du 400ème anniversaire de la naissance de Blaise Pascal, un autre scientifique philosophe animé par la même soif de proposer une manière globale d'appréhender le monde.

Quant à M. Prof Dionys Baeriswyl, il a rejoint l'Université de Fribourg en tant que Professeur ordinaire en 1989 avec la ferme intention d'y apporter une nouvelle dynamique à la recherche en physique théorique. Pari réussi à l'heure du bilan. Il aura servi la science jusqu'au bout, mais tout le monde se rappellera aussi son caractère convivial et sa facilité de contact : c'était toujours un plaisir de le rencontrer et d'échanger quelques mots avec lui. Merci à M. Prof Xavier Bagnoud de lui avoir rendu un hommage mérité dans ce numéro.

Le passé ne doit pas nous faire oublier le présent : rien n'arrêtera le développement de notre Département et le meilleur hommage que l'on pouvait rendre à nos disparus est sans aucun doute de démontrer que la recherche et la formation en physique n'ont en rien perdu de leur vigueur à l'Université de Fribourg.

Mais la physique ne concerne pas que les docteur·e·s en la matière. Trop longtemps les sciences en général, et la physique en particulier, a négligé l'importance de communiquer au-delà du cercle des initié·e·s. Aujourd'hui sous la pression des restrictions budgétaires qui touchent à peu près tous les secteurs, il n'est plus question de limiter la vulgarisation aux seules revues spécialisées. Notre collaboratrice Amandine a visité le CERN et nous transmet ses impressions avec son regard de non-spécialiste. Voilà qui va dans le bon sens.

Vous avez dit « bitcoin » ? C'est quoi au juste ? Une cryptomonnaie présentée pour la première fois en 2008, nous dit Wikipédia, et à laquelle on met une majuscule lorsqu'il s'agit du système de paiement pair-à-pair. D'accord ! Mais les scientifiques que nous sommes avaient besoin d'en savoir plus et Peter a bien voulu nous faire partage ses connaissances dans ce domaine.

Bonne lecture !

La vie au Département

Prof. Guillermo Acuña

It is with great pleasure that I set out to write a few lines to summarize the main events that took place in our Department of Physics during the academic year 2022-2023.

A new face

The most noticeable things that happened to our Department are (and continue to be) the different works in the building. These can be mostly divided in two tasks. First, there has been an initiative to improve the quality of the wireless signal to connect to the internet in every part of our building. To this end, several routers and repeaters were installed not only in corridors and other common spaces but also in offices, laboratory space and classrooms. This is also supposed to reduce the overall number of physical internet power sockets. These tasks are finished. Second, window curtains are being modernized complying with the protected status of the building since the previous solution of installing a film did not work out. I would like here to take the chance to thank Nathan Fuchs and particularly Anne Fessler for coordinating with the workers to try to minimize the noise and disturbance during lectures and exams.

PER08 building

New Department members

During this period the main additions to our Department occurred in the workshop. Following the departure of Gabriel Bächler, Markus Baeriswyl has started working in the workshop on the first of October 2023. He was previously working for W. Schweizer AG in Düdingen. We wish him a good start in our Department!

Outreach activities

Perhaps still experiencing an enhanced interest after some years of restrictions due to Covid in previous years, outreach activities led by Dr. Baptiste Hildebrand, Anne Fessler and Nadia Pury took a significant part of the agenda. A list of the main activities is included below:

- January 16th and February 15th: “Démonstrations pour gymnasiens” with Maxime Rumo and students from the Gymnase Gambach.
- February 1st: Stage laborantin (demande individuelle) by Dr. Baptiste Hildebrand.
- February 6nd and 14th: “Labos gymnasiens“, with Chassot Frédéric, Muster Augustin and students from Gymnase CSUD and Gambach .
- February 15th and 16th: “Perspectiva” both in German and in French led by Dr. Baptiste Hildebrand and Prof. Philipp Werner respectively.
- March 8th: “Masterweek” by Dr. Baptiste Hildebrand with bachelor students from Uni Fribourg.
- March 13th and 14th: “Science for youth workshop” led by Prof. Ana Akrap, Dr. Hildebrand Baptiste and Chassot Frédéric.
- May 3rd: “Kids Uni” by Dr. Hildebrand Baptiste and Chassot Frédéric.

- May 4th: “Séance infos nouveau plan d'études” by Dr. Hildebrand Baptiste with bachelor students from Uni Fribourg.
- September 23rd: “Explora” science fair with experiments for kids and adults. This was one of the biggest events of our faculty with the participation of several members of our Department including professors, MAs, post-docs, PhDs and students. Different experiments were particularly designed to amuse, entertain, and awake the interest in science in our local community. It is estimated that approximately 500 visitors took active part in these activities. Special thanks to Dr. Veronique Trappe, Dr. Baptiste Hildebrand, Nadia Pury, Dr. Luis Froufe, Dr. Premysl Marsik and everyone from the Department that came on a Saturday to support these activities.

Explora 2023

New students and graduates

14 new physics students started the Fall semester 2023. This number seems to consolidate a slight incremental trend. This is a remarkable fact, considering that numbers in other natural science departments are witnessing a considerable drop and also reflect on the work of Baptiste Hildebrand who four years ago started working on promoting the activities of the Physics department in different schools in Fribourg.

Finally, the following is a list of the Bachelor, Master and PhD graduates:

Bachelor:
Sophie BAMERT
Vincent GARRIDO
Vincent GLAUSER
Kira LUND
Katja Sophia MOOS
Laura RÜEGGER
Jessica RUFFINER
Jules SCHADT
Albano Francesco TABACCHI
Théo THOMAS
Eileen WAEBER

Master:
Nicolas BRUDER (Prof. Acuña)

PhD:
Maxime RUMO (Prof. Monney)
Olivier SIMARD (Prof. Werner)
Markus LYSNE (Prof. Werner)
Philipp MARMET (Prof. Brader)
Björn SALZMANN (Prof. Monney)
Yuhao ZHOU (Prof. Zhang)
Wenyao ZHANG (Prof. Zhang)
Tianlong FAN (Prof. Zhang)
Salomée TSCHOPP (Prof. Brader)

Awards and Prizes

The following prizes were awarded during the last academic year:

- Bourse Thürler-Reeb: Frédéric Chassot.
- Ludwig-Genzel-Prize: Prof. Ana Akrap.
- Winner prize Innovation Challenge: Morgane Loretan.

- Best Bachelor of Science Prize: Joel Morf.

Congratulations to all of them!

Departures

Unfortunately, not only we have good news to write about, but we have departures to lament. Markus Andrey´s wife passed away after months of battling. We were really moved by this event and by the way both Markus and his colleagues at the workshop dealt with it.

In addition, our emeritus Professor Dr. Dionys Baeriswyl also left us. Following several years of commitment to our Department through his notable research and dedication to teaching and shaping young students, Dr. Baeriswyl continued to be amazed and interested in Science as evidence by his regular attendance to our weekly Wednesday seminar. We deeply regret his loss. To celebrate his activities in our Department, a Colloquium in memoriam of Dionys Baeriswyl entitled “Dionys and the Fractal Hubbard Model” will take place on October 25th organized by the Scheffold group and with the presence of Cristiane Morais Smith, a former member of Dr. Baeriswyl group at our Department.
Our thoughts go with the families and friends in these sad moments.

Specialized NRBC Exercise

During the last semester, the Department of Physics witnessed a significant event. The "group of measures," comprised of a dozen members, organized an NRBC (Nuclear, Radiological, Biological, and Chemical) exercise. This team, primarily composed of firefighters with a solid scientific background, intervenes across the Fribourg canton in cases of NRBC incidents.

The three-hour exercise aimed to enhance the necessary skills for managing complex NRBC situations, including working under respiratory protection, measuring toxic substances, and collecting samples. Nathan Fuchs, a member of the physics

Department, played a central role in coordinating the exercise.
These exercises, conducted about ten times a year in various locations across the canton, highlight the Department's ongoing commitment to safety and preparedness for NRBC situations. They also underscore the interdisciplinary collaboration within our University.

The Roman Die and the Locus Ludi Project

The Department of Physics was involved in an exceptional collaboration with Véronique Dansen's team from the University of Fribourg (UNIFR) as part of the ERC project titled "Locus Ludi." This project aims to set a benchmark by reconstructing the history of ludic culture in the Greco-Roman world. Through in-depth philological, historical, archaeological, and anthropological studies, Locus Ludi has embarked on the identification, categorization, and reconstruction of ancient games. This research offers a fresh perspective on the cultural fabric of ancient society, provides

models for training and research in related fields, and supplies updated materials for schools, museums, and libraries. Understanding the educational, societal, and integrative role of play in the past is crucial for understanding the present and expanding the discourse on high-tech toys and new forms of sociability.

Our Department was approached by Véronique Dansen's research team at UNIFR, and Thomas Daniaux, a doctoral student in art history at UNIFR, who conducted a unique study of a Roman die discovered during archaeological excavations in Belgium as part of this project. This die proved to be an exceptionally ancient and unique artifact, as it was rigged: a cavity had been hollowed out inside it, and an amalgam of mercury and gold had been concealed within. This allowed the player to manipulate the die to achieve the desired outcome.

To gain a better understanding of this rigged die, the Department of Geology, under the guidance of Christoph Neururer, conducted X-ray tomography to examine its internal structure. Additionally, our Physics Department was tasked with replicating the die using 3D printing technology. Enlarged versions, measuring 20 cm on each side, were produced from the original, which was originally 8 mm in size. These enlarged replicas will allow the audience at the "Bible and Orient" museum to visualize the inside of the die on a larger scale. Furthermore, full-sized replicas are currently being created to study the behavior of this unique rigged die. Remarkably, this die had been damaged and broken during the excavation, which ultimately led to the discovery of its mercury content and its rigged nature.

This fascinating collaboration between our Physics Department and the Locus Ludi project demonstrates the diversity of skills and interests within our academic community, as well as our commitment to exciting interdisciplinary research.

Le CERN par une non-physicienne

ou les questions du droit de propriété des sols

Amandine Pinard travaille depuis le 1er janvier 2022 comme collaboratrice RH au Département de physique.

Le Conseil européen pour la recherche nucléaire (CERN) a décidément une place importante pour le Département de physique de l'Unifr. Après la visite des étudiant·e·s organisée par le Prof. Beck en décembre 2022, c'est au tour de la team admin de s'être rendue au CERN à Meyrin dans le but de découvrir un endroit emblématique de la recherche en physique.

Ma sœur y travaillant comme ingénieure, nous avons pu organiser une visite remplie de surprises, le 7 mars 2023.

L'équipe : Anne, en charge des étudiant·e·s et du groupe du Prof. Werner, Magali, apprentie employée de commerce de 2ème année, Doriana, en charge des frais de voyage et du groupe du Prof. Zhang, Nadia, responsable des finances et moi qui m'occupe des ressources humaines pour le Département ainsi que ma sœur, Lucile.

L'idée de base était d'aller visiter ATLAS (acronyme de *A Toroidal LHC ApparatuS*) ainsi que le Data Center. Des visites guidées

étaient organisées pour nous permettre de découvrir ce centre gigantesque, qui toutefois, ne ressemblait pas du tout à ce que j'imaginais. Naïvement, je me représentais le CERN comme un édifice à hauteur de la complexité de la recherche qui y est effectuée – un colosse futuriste où des gens en blouse blanche circulent en *segway* d'un bout à l'autre des bâtiments constitués de colonnes en verre dont les façades afficheraient, grâce à des LED, des calculs en continu. Mais que nenni, le CERN est la représentation de ce que j'ai d'une ville d'ex-union soviétique, avec différents bunkers ayant tous l'air abandonnés, subissant rouille et écailles dans la peinture. En même temps, le CERN fête ses 69 ans en septembre 2023, ce qui en fait une institution relativement ancienne comparée à de nombreuses autres organisations scientifiques – on lui pardonne l'état de certains de ses bâtiments.

Après avoir mangé dans une des nombreuses cafétérias qu'offre le centre, nous devions nous rendre à ATLAS pour y faire une visite guidée. Toutefois, arrivées sur place après avoir effectué près de 8000 pas (le CERN est extrêmement étendu), la personne en charge de la visite nous a fait faux bond et n'a jamais répondu aux nombreux appels désespérés de ma sœur. Nous avons tout de même pu voir la construction sous sa forme en LEGO qui reste une œuvre intéressante (cf. image) – une exposition photographique nous a permis de comprendre également le rôle que joue ATLAS au sein du LHC. En résumé, son rôle est de détecter et d'analyser les particules produites lors des collisions de protons qui ont lieu dans le LHC. Il faut noter qu'en période de fonctionnement standard du LHC, le nombre de collisions de protons peut atteindre plusieurs dizaines de millions par seconde !

ATLAS en LEGO

Dans un deuxième temps, nous avions rendez-vous pour une visite du Data Center qui notamment stocke les données réalisées lors de collisions de protons des expériences comme ATLAS ou CMS (Compact Muon Solenoid - en français «Spectromètre à Muons Compact"). Après plusieurs kilomètres de marche soldés par un drop en bus dont le chauffeur connaît bien ma sœur, nous sommes arrivées au Data Center à l'heure. À nouveau personne, mais après un coup de téléphone, un peu de négociations, nous avons eu la chance de rencontrer le Dr Stefan Lueders, responsable de la sécurité informatique au CERN. Son intervention d'une heure environ nous a littéralement basculées dans un monde plus que fascinant. Dr Lueders a clairement su s'adapter à un public majoritairement non-initié à la recherche faite au CERN.

Pour reprendre le site du CERN, le Centre de calcul du CERN se trouve au cœur de l'infrastructure scientifique, administrative et informatique du CERN. Tous les services, y compris la messagerie électronique, la gestion des données scientifiques et la vidéoconférence, utilisent du matériel installé dans le Centre de calcul. 450 000 cœurs de processeurs et 10 000 serveurs fonctionnent 24 heures sur 24, sept jours

sur sept. Plus de 90 % des ressources informatiques du Centre de calcul du CERN sont déployées via un nuage privé basé sur OpenStack, un projet open source établissant un environnement en nuage extrêmement modulable.

La présentation du Dr Lueders était passionnante : au-delà du Data Center, c'est toute la structure de ce centre et la recherche réalisée qui nous a été expliquée. En quelques phrases, nous avons pu comprendre ce qu'est un accélérateur de particules, comment fonctionne le complexe d'accélérateurs et finalement les raisons pragmatiques de toute cette recherche qui peut paraître démesurée aux yeux de personnes peu scientifiques comme nous. Nous avons même terminé la rencontre sur une réflexion plus philosophique sur l'équilibre si fragile qui permet la vie sur Terre et la responsabilité qu'ont les humains – et encore plus les chercheur·euse·s – de maintenir cette précieuse harmonie.
Notre visite s'est achevée à l'entrée du CERN où nous avons pu voir une maquette présentant le projet de Futur Collisionneur Circulaire (FCC) dont le tunnel aura un tracé de 100km de circonférence entre la France et la Suisse, projet qui pourrait voir le jour en 2040 et qui coûterait près de 20 milliards de francs suisses. Une carte définissait le tracé que pourrait avoir cet énorme tunnel dont, à nouveau, nous ne saisissons pas complètement l'intérêt scientifique. Toutefois, une question plus pragmatique a traversé nos esprits en voyant sur la carte des habitations sous lesquelles passerait le tunnel : à quelle profondeur le terrain nous appartient ? Est-il possible de contester la présence d'un tunnel sous nos habitations ? Et là, ce n'est plus de la physique mais du droit international dont nous avons besoin pour répondre à cette question. Pour vous libérer du suspense intense que provoque cette question, lorsqu'il s'agit d'un projet étatique ou validé par l'Etat que ce soit en France ou en Suisse, la profondeur du terrain qui appartient aux propriétaires reste très limitée.
Notre visite s'est terminée en fin de journée. J'en garde un souvenir riche en découvertes et surprises. Je retiens que la physique ne se résume pas à des calculs abstraits qui semblent parfois sortis de la réalité. La physique joue un rôle essentiel dans la réalisation de projets concrets en fournissant les fondements théoriques et les outils nécessaires pour comprendre et manipuler le monde qui nous entoure.

Blockchain

Peter Stadlin

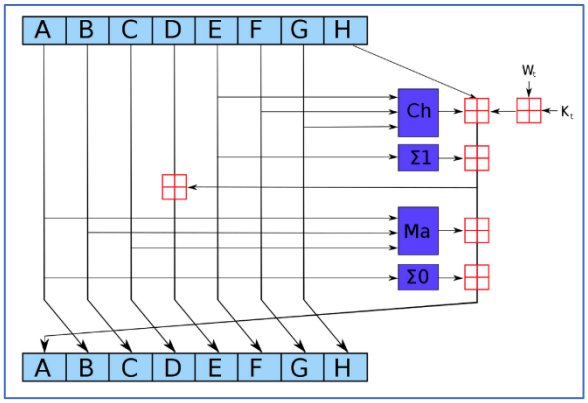
Was ist eine Blockchain

Bei Blockchain handelt sich dabei um eine Summe bzw. Liste, die aus Datensätzen besteht. Diese Datensätze bilden zusammen einzelne Blöcke, die wiederum mittels der Kryptographie zu Blockketten verbunden werden. Dies ist eine gute Basis zur Umsetzung eine sog. Distributed-Ledger-Technologie. Unter Distributed-Ledger-Technologien werden Datenbanksysteme verstanden, die eine synchronisierte Verifizierung und Speicherung von Daten in Peer-to-Peer Netzwerken ermöglichen. Distributed-Ledger-Technologien besitzen weder einen übergeordneten Verwalter noch einen zentralen Datenspeicher. Stattdessen kommunizieren die vernetzten Rechner des Peer-to-Peer Netzwerks miteinander, indem sie neu eingehende Transaktionen im Netzwerk auf Basis verschiedener Konsensmechanismen überprüfen, bestätigen, unveränderbar kryptographisch miteinander verketten und anschliessend verteilt abspeichern. In sog. Peer-to-Peer Netzwerken stellen Netzwerkteilnehmer

Hardware-Ressourcen zur Verfügung, um Inhalte bzw. Leistungen des Netzwerks bereitzustellen so dass direkte Austausche zwischen den Netzknoten stattfinden können. Diese Prinzipien tragen dazu bei, dass auf eine zentrale Instanz zur Koordination der Kommunikation zwischen den einzelnen Netzknoten verzichtet werden kann. Darüber hinaus sind Blockchain-Architekturen verteilte Systeme. Sie bestehen aus gleichberechtigten Rechnern (Netzknoten, „Nodes“), die miteinander kommunizieren und sich automatisch synchronisieren. Da die Daten der Blockchain grundsätzlich an jedem Netzknoten redundant gespeichert werden und die einzelnen Netzknoten alle die gleichen Funktionen ausüben können, hat ein Ausfall einzelner Netzknoten nicht den vollständigen oder teilweisen Ausfall des Netzwerks zur Folge. Um Teilnehmer in einem Blockchain-Netzwerk zu identifizieren, Transaktionen auszulösen, neue Blöcke zu bilden und diese Blöcke unveränderbar miteinander zu verketten, nutzen Blockchains kryptographische Funktionen. Die beiden wichtigsten Funktionen, die dazu eingesetzt werden, sind Public-Key-Kryptographien und kryptographische Hash-Funktionen.

Hash-Funktion

Eine Hashfunktion H(M) verarbeitet eine beliebig lange Nachricht M. Die Funktion erzeugt einen Hashwert h fester Länge (z. B. 256 Bit). Das Besondere an dieser Funktion ist die Schwierigkeit, ein M, d. h. eine Nachricht, aus dem Hashwert h zu berechnen. Anders ausgedrückt bedeutet das: Es ist schwer, zu gegebenem h ein M mit H(M) = h zu berechnen. Des Weiteren sollte es eines großen Rechenaufwands bedürfen, zu einer gegebenen Nachricht M eine andere Nachricht M' zu berechnen mit H(M) = H(M'). Genau diese Eigenschaften machen Hashfunktionen für die Kryptographie so interessant und wird Kollisionsresistenz genannt. Grundlagen von Hashfunktionen sind ausgeklügelte sog. Kompressions-Funktionen, welche die Daten auf einen bestimmten Hashwert reduzieren, dabei aber alle Daten eines Blocks berücksichtigen. Die Hashfunktion beruht auf einem iterativen Verfahren unter der Anwendung einer Merkle-Damgård-Konstruktion mit Davies-Meyer-Kompressionsfunktion. Die SHA-256 Hashfunktion verwendet 32-Bit-Wörter und teilt die Nachricht M in Blöcke zu 512 Bit auf. Sie verschlüsselt in 64 Runden unter Verwendung von vier logischen Funktionen und je Runde einer anderen Konstanten.



Rundenfunktion von SHA-256:
A bis H sind die Wörter des Datenblocks, der
verschlüsselt wird, W_i sind aus dem Nachrichtenblock berechnete Rundenschlüssel und K_i Konstanten.

$$\mathrm{Ch}(E,F,G) = (E \wedge F) \oplus (\neg E \wedge G)$$
$$\mathrm{Ma}(A,B,C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$
$$\Sigma_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$
$$\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$

Public Key Verfahren

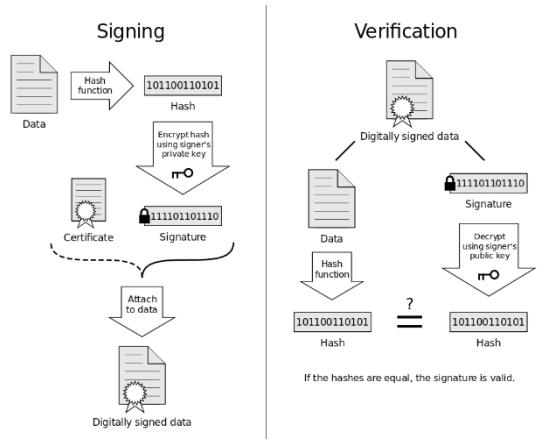
Public Key Verfahren sind asymmetrische Verschlüsselungsverfahren. Aus der Kenntnis eines Schlüssels lassen sich keine Kenntnisse oder Informationen über den anderen Schlüssel ziehen und umgekehrt. Der private Schlüssel muss geheim gehalten werden und es ist praktisch unmöglich, ihn aus dem öffentlichen Schlüssel zu berechnen. Der öffentliche Schlüssel muss jedem zugänglich sein, der eine verschlüsselte Nachricht an den

Besitzer des privaten Schlüssels senden will. Dabei muss sichergestellt sein, dass der öffentliche Schlüssel auch wirklich dem Empfänger zugeordnet ist.

Digitale Signatur

Eine digitale Signatur, ist ein asymmetrisches Kryptosystem, bei dem ein Sender mit Hilfe eines geheimen Signaturschlüssels (dem Private Key) einen Hashwert einer digitalen Nachricht (d. h. zu beliebigen Daten) verschlüsselt und so einen Wert erhält, digitale Signatur genannt wird. Dieser Wert ermöglicht es jedem, mit Hilfe des öffentlichen Verifikationsschlüssels (dem Public Key) die nicht abstreitbare Urheberschaft und Integrität der Nachricht zu prüfen. Um eine mit

einem Signaturschlüssel erstellte Signatur einer Person zuordnen zu können, muss der zugehörige Verifikationsschlüssel dieser Person zweifelsfrei zugeordnet sein. Die Transaktionen Tx_n werden von den jeweiligen Sendern signiert.

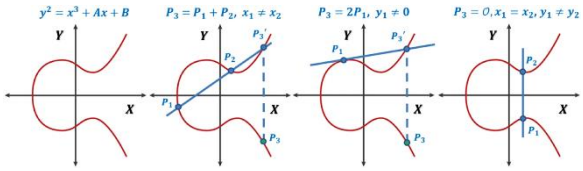


Elliptische Kurven (Public Key Verfahren)

In der Mathematik sind elliptische Kurven spezielle algebraische Kurven, auf denen geometrisch eine Addition definiert ist. Diese Addition wird in der Kryptographie zur Konstruktion sicherer Verschlüsselungsmethoden verwendet. Die Untersuchung elliptischer Kurven über den rationalen Zahlen oder endlichen Körpern ist Gegenstand der Zahlentheorie und ein Spezialfall der auch in höheren Dimensionen betrachteten abelschen Varietäten. Diese abelsche Gruppenstruktur überträgt sich auch auf elliptischen Kurven über den rationalen Zahlen und auf eine besondere Art von Addition für Punkte auf elliptischen Kurven. Der Mathematiker Andrew Wiles bewies im Jahr 1994 den Modularitätssatz, der besagt, dass alle elliptische Kurven über den rationalen Zahlen durch Modulformen parametrisiert werden. Mit Hilfe dieses Satzes konnte der Große Fermatsche Satz bewiesen werden, eine bekannte zahlentheoretische Aussage, die sich einfach formulieren, aber nur schwer beweisen lässt. Praktische Anwendung finden elliptische Kurven in modernen Verschlüsselungsverfahren (Elliptische-Kurven-Kryptosystem), die die oben erwähnte besondere Addition von Punkten auf elliptischen Kurven für die Definition von Einwegfunktionen verwenden. Ist eine elliptische Kurve über einem Körper mit Charakteristik durch die Weierstrass-Gleichung gegeben, so existiert ein Koordinatenwechsel, der diese Weierstrass-Gleichung in die Gleichung transformiert. Diese nennt man eine kurze Weierstrass-Gleichung. Die durch diese kurze Weierstrass- Gleichung definierte elliptische Kurve ist zur ursprünglichen Kurve isomorph. Häufig geht man daher ohne Einschränkung davon aus, dass eine elliptische Kurve von vorneherein durch eine Weierstrass-Gleichung gegeben ist. Elliptische Kurven haben die Besonderheit, dass sie bezüglich der in diesem Abschnitt beschriebenen punktweisen Addition kommutative Gruppen sind. Die Spiegelung eines rationalen Punktes an der x-Achse liefert wieder einen rationalen Punkt der Kurve, das Inverse $-P_3$ von P_3'. Die Gerade durch die rationalen Punkte P_1, P_2 schneidet die Kurve in einem dritten Punkt, Spiegelung dieses Punktes an der

x-Achse liefert den rationalen Punkt P_3.

Im Fall einer Tangente an den Punkt P1 (also des Grenzfalles P_2 -> P_1 auf der Kurve) erhält man mit dieser Konstruktion (Schnittpunkt der Tangente mit der Kurve, dann Spiegelung) den Punkt $P_3=2P_1$. Der Punkt P_3 wird mit $2P_1$ bezeichnet, entsprechend definiert man kP_1 = P1 + …. P1 als k-fache Addition des Punktes P_1. Man kann zeigen, dass diese „Addition“ sowohl kommutativ als auch assoziativ ist, sodass sie tatsächlich
die Gesetze einer abelschen Gruppe erfüllt. Die Aufgabe, aus gegebenen Punkten P_1, P_2 diesen Wert k zu ermitteln, wird als Diskreter-Logarithmus- Problem der elliptischen Kurven (kurz ECDLP) bezeichnet.



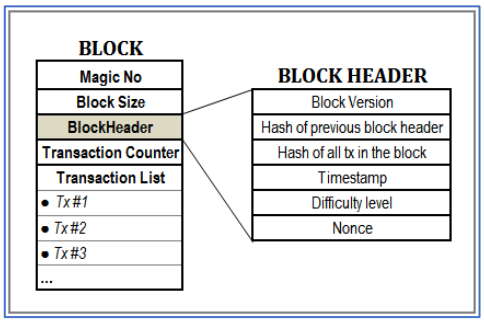
Ethereum und Bitcoin nutzen zur Umsetzung von ECC eine spezielle elliptische Kurve, genannt SECP256K1, mit der Gleichung
y2 = x3 + 7. In dieser Kurve ist der Basispunkt P_1 bereits festgelegt und ist immer gleich.

Elemente der Blockchain

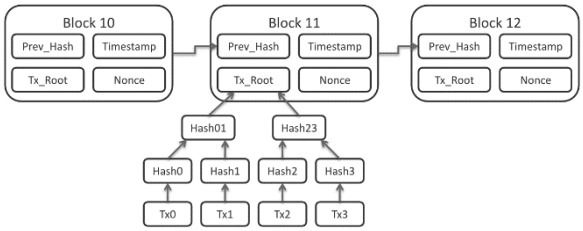
Eine wichtige Eigenschaft der Blockchain besteht darin, dass diese Datensatz-Liste kontinuierlich erweitert wird. Technisch betrachtet ist es so, dass jeder Block aus der Kette einen sicheren Hash des jeweils vorherigen Blocks beinhaltet. Die Sicherheit spielt ohnehin eine grosse Rolle, sodass es für jeden Block die drei folgenden Sicherheitsmerkmale gibt:

- Hash (Sicherheit des vorherigen Blocks)
- Transaktion beginnen und bestätigen
- Zeitstempel

Damit kann eine Blockchain als ein verteiltes Register, in dem digitale Datensätze, Ereignisse oder Transaktionen in chronologischer Reihenfolge für alle Teilnehmer nachvollziehbar in Datenblöcken gespeichert („Block“) und unveränderbar miteinander
verkettet („Chain“) sind, definiert werden. Ein Block weist folgende Struktur auf:



Eine Blockchain weist folgende Struktur auf:



Tx_Root: Die »Wurzel« eines Merkle Tree, d.h. der Stamm aller gehashten Paare in einem Baum. Block-Header müssen eine gültige Merkle Root für alle Transaktionen in einem Block enthalten

Tx_n: Transaktion: Einfach ausgedrückt die Übertragung von Inhaltswerttoken von einer Adresse an eine andere. Genauer formuliert, ist eine Transaktion eine signierte Datenstruktur, die den Transfer von Werten ausdrückt. Transaktionen werden über das Blockchain-Netzwerk übertragen, von Minern gesammelt und in Blöcken eingetragen, um permanent in der Blockchain festgehalten zu werden.

Konsensverfahren

Die Technik der Konsensbildung ist ein Grundpfeiler der Blockchain. Die dabei verwendeten Verfahren beruhen auf Konzepten, die im Kontext verteilter Netzwerke und verteilter Systeme bereits seit Längerem untersucht wurden. Das aktuell bekannteste von einer Blockchain-Implementierung verwendete Verfahren ist

der Proof-of-Work der Bitcoin-Blockchain. Das eigentliche Proof-of-Work-Konzept wurde schon 1993 zur Eindämmung von Junk-E-Mails vorgeschlagen. Es basiert auf einem asymmetrischen Ansatz, bei dem ein Dienstnutzer, das heisst der E-Mail-Absender, Arbeit leisten muss, die von einem Dienstanbieter, das heisst dem E-Mail-Netzprovider, ohne grossen Aufwand überprüft werden kann. Im Blockchain-Kontext sind die Nutzer die *Miner*, die den Proof-of-Work aufwändig berechnen und die Anbieter alle *Knoten*, die ohne grossen Aufwand prüfen, ob der erfolgreiche Miner den Proof-of-Work ordnungsgemäss berechnet hat. Ein Peer-To-Peer (P2P) ist ein verteiltes System, welche mehrere Computer nutzen, um eine gemeinsame Aufgabe zu erledigen. Es muss jedoch sichergestellt sein, dass eine Überweisung ähnlich einer Datenbanktransaktion exakt einmal ausgeführt wird. Dabei darf es keine Rolle spielen, ob die Systeme zu jedem Zeitpunkt korrekt funktionieren: Ein Softwarefehler oder Hardwaredefekt darf keine Transaktion verändern. Dieses Problem ist in der Informatik unter dem Stichwort »Byzantinische Generäle« bekannt: Man stelle sich eine Stadt vor, die von mehreren Armeen unter der Führung jeweils eines Generals umzingelt ist. Die Armeen sind nur mit einem gemeinsamen Angriff in der Lage, die Stadt einzunehmen. Um den Angriff zu koordinieren, schicken die Generäle Boten mit Nachrichten zu den anderen Armeen. Was passiert, wenn ein Bote unterwegs abgefangen wird? Was, wenn ein Bote die Nachricht böswillig verändert? Oder zufällig? Ein »byzantine fault tolerant«-System ist eines, das trotz derartiger Fehler stabil bleibt und z. B. die Transaktionseigenschaften garantiert. Die Blockchain ist ein Beispiel eines solchen Systems. Das Konsensverfahren beruht auf einem Wettbewerb der Miner in einem Verteilten System, welche in Konkurrenz stehen und entsprechenden ein gesundes Misstrauen gegenüber dem Mitbewerber haben und durch die Entlöhnung mittels digitaler Währung motiviert werden, in das System zu investieren und Gewinn zu realisieren. Wichtig für die Stabilität einer Kryptowährung ist, dass ein vertrauenswürdiger Nutzer ausgewählt wird, eine Transaktion in die Blockchain einzutragen. Die Transaktionen werden durch Computer (Nodes) validiert. Ein Angreifer könnte an dieser Stelle eine Transaktion fälschen, sich unrechtmässig Geld zuschreiben oder die Stabilität einer gesamten Kryptowährung in Gefahr bringen. Um sicherzustellen, dass ein Teilnehmer der Blockchain vertrauenswürdig ist, kann er sich auf zwei Arten beweisen:

1. durch Einsatz von Rechenleistung (Proof of Work)
2. durch Einsatz von Vermögen (Proof of Stake)

Es ist unlogisch, eine Blockchain zu zerstören, in die man viel Geld oder (teure) Rechenleistung investiert hat. Wer ein persönliches Risiko eingeht, wird also nicht betrügen. Der Ansporn, am Proof of Stake teilzunehmen, ist der Reward. Produziert ein Teilnehmer einen korrekten Block, erhält er dafür Coins oder Tokens der jeweiligen Kryptowährung

Proof of Work

In der Bitcoin-Blockchain basiert der Proof-of-Work-Algorithmus auf dem von Adam Back als Hashcash präsentierten Verfahren
Das Ziel des Algorithmus ist es, eine Zahl zu finden (Nonce = number used only once),
die in Kombination mit dem neuen Block, der an die schon existierende Blockchain angehängt werden soll, einen Hashwert ergibt, der aus einer vorgegeben bestimmten Anzahl führenden Nullen besteht (Blockschwierigkeit). D.h. die Arbeit der Miner entspricht der Lösung eines asymmetrischen mathematischen Rätsels, explizit die Lösung einer partiellen Hashinversion. Es muss eine Nonce so

gefunden werden, dass der resultierende Hashwert kleiner ist als der SHA256-Ziel-Hashwert, welcher mit mehreren Null-Bits beginnt. Finden mehrere Miner gleichzeitig einen solchen Wert und hängen diesen an die Blockchain, so führt dies bei der Verteilung dieses neuen Blocks an alle Knoten des P2P-Netzwerks, zu einer Verzweigung der Blockchain. Finden z. B. drei Knoten nahezu zeitgleich einen passenden Nonce, dann würde sich durch das Anhängen der neuen Blöcke die existierende Blockchain in drei Zweige aufteilen. Um diese Aufteilung wieder zu konsolidieren, gilt die Mehrheitsentscheidung: der Zweigwird ausgewählt, der die längste Kette repräsentiert, das heisst die meisten Transaktionen bzw. die meiste Arbeit repräsentiert. Die beiden anderen Blöcke verfallen und die darin enthaltenen Transaktionen, die nicht in dem angehängten Block enthalten sind, werden wieder in den Pool der noch zu validierenden Transaktionen aufgenommen. Dieses Proof-of-Work-Verfahren ist CPU-basiert, das heisst die Rechengeschwindigkeit der Knoten hat massgeblichen Einfluss darauf, wer das Rätsel löst und einen passenden Nonce-Wert findet. Da die Miner für das Finden des Nonce mit neuen Bitcoins belohnt werden, entsteht ein Wettbewerb, der dazu führt, dass diese in immer mehr Rechenleistung investieren.

Proof of Stake

Der erste Schritt des Proof of Stake ist die Hinterlegung des Stakes. Die Nutzer geben einen Teil ihres Vermögens auf die Blockchain. Dieser Stake wird während des gesamten Konsensverfahrens eingefroren. Deine hinterlegten Coins gehören weiterhin dir, aber du kannst erst nach einer abgeschlossenen Validierung wieder darauf zugreifen. Betrügt ein Nutzer, erhält er seinen Stake nicht wieder. Unter allen Nutzern, die den Stake hinterlegt haben, wählt der Algorithmus aus, wer den nächsten Block erzeugen darf. Das passiert mit einem gewichteten Zufallsverfahren. Das bedeutet, grundsätzlich ist zufällig, wer ausgewählt wird, aber es gibt Faktoren, die die Wahrscheinlichkeit erhöhen. Ein solcher Faktor ist unter anderem die Höhe des Stakes. Wer mehr Vermögen hinterlegt, wird wahrscheinlicher ausgewählt. Die Konsensfindung findet bei diesem Verfahren ebenfalls über die Validierung der Lösung mittels einer partiellen Hashinversion statt. Die Schwierigkeit den richtigen Hashwert zu finden ist gekoppelt an die Summe der Währung im Umlauf dividiert durch die zu erwartende Zeit zwischen der Validierung von zwei Blöcken. Wesentliche Vorteile dieses Verfahrens sind: Sehr energieeffizient und damit ressourcenschonend, Das Netzwerk kann einfach vergrössert werden. Wesentliche Nachteile dieses Verfahrens: Es kann zu einer starken Aufspaltung der Blockchain kommen, weil die Betreibungskosten so niedrig sind, dass sich die Validatoren bei einem Fork nicht für einen Strang der Chain entscheiden müssen, manche Menschen befürchten mehr Zentralisierung durch vermögende Teilnehmer, Gefahr der 51%-Attacke (51% Stake des ganzen Sytsems). Das Delegated Proof of Stake (DPoS) ist eine Weiterentwicklung des PoS-Mechanismus. Durch ein Wahlsystem soll die Blockchain vor Zentralisierung und böswilliger Nutzung geschützt werden. Beim DPoS gibt es Wähler und Delegierte. Jeder, der Tokens einer Währung besitzt, ist ein Wähler. Er erhält genauso viele Stimmen, wie er Tokens in seinem Wallet hat. Mit diesen Stimmen können die Wähler die Delegierten (auch Zeugen genannt) wählen. Delegierte sind Menschen aus der Community, die sich freiwillig mehr einbringen wollen. Die Gewählten bekommen bestimmte Aufgaben zugeteilt, zum Beispiel die Validierung neuer Blöcke. Dafür werden sie, je nach Kryptowährung,

in Form von Tokens bezahlt. Führt ein Delegierter seine Arbeit schlecht aus, wird er wahrscheinlich nicht wieder gewählt. Kann ein Delegierter seine Aufgabe nicht erfüllen, zum Beispiel weil sein Computer nicht die nötige Rechenleistung erbringt, wird seine Position an die Person mit den nächst meisten Stimmen weitergegeben.

Weitere Konsensverfahren

Es gibt noch weitere Konsensverfahren wie Proof of Activity, Proof of Capacity, Proof of Elapsed Time, Ouroboros, Open Representative Voting

Internet-Währungen

Bitcoin und deren abgeleitete und technologisch erweiterte Währungen wie Bitcoin XT, Bitcoin Classic, Bitcoin Unlimited, Bitcoin Cash, Litecoin, Dash, Zcash, Segewit, Ethereum.

Bitcoin

Bitcoin ist die erste und die am Markt weltweit stärkste Kryptowährung auf Grundlage eines dezentral organisierten Buchungssystems. Zahlungen werden kryptographisch
legitimiert (digitale Signatur) und über ein Rechnernetz gleichberechtigter Computer (Peer-to-Peer) abgewickelt. Anders als im klassischen Bankensystem üblich, entspricht eine Transaktion mit Bitcoin dem Settlement zwischen den Beteiligten. Eigentumsnachweise an Bitcoin werden in persönlichen digitalen Brieftaschen (umgangssprachlich »Wallet», engl.) gespeichert. Der Kurs einer Bitcoin zu den gesetzlichen Zahlungsmitteln folgt dem Grundsatz der Preisbildung an der Börse.

Ethereum

Ethereum ist ein quelloffenes verteiltes System, welches das Anlegen, Verwalten und Ausführen von dezentralen Programmen bzw. Kontrakten (Smart Contracts) in einer eigenen Blockchain anbietet. Es stellt damit einen Gegenentwurf zur klassischen Client-Server-Architektur dar. Ethereum verwendet die interne Kryptowährung Ether (abgekürzt mit ETH) als Zahlungsmittel für Transaktionsverarbeitungen, welche durch teilnehmende Computer abgewickelt werden.

Ether ist nach Bitcoin die Kryptowährung mit der zweitgrössten Marktkapitalisierung. «Smart Contracts» sind Programme, die automatisch ausgeführt werden, sobald eine in dem Contract festgelegte Summe in Ether überwiesen wurde. Damit ist keine (manuelle) Überprüfung eines Zahlungseingangs mehr erforderlich, denn die Überweisung startet direkt die im Programm festgelegte Gegenleistung. Die «Smart Contracts» werden meist in der für Ethereum eigens entwickelten Programmiersprache Solidity geschrieben. Sie werden dann in Bytecode übersetzt und auf der Ethereum Virtual Machine (EVM) ausgeführt.

Corda

Corda ist eine Blockchain-Plattform, die friktionslose Transfers ermöglicht. Das Projekt richtet sich vor allem an Business-Kunden, die in komplexen Geschäften Transaktionen durchführen. Die Ursache für diese Probleme liegt laut Corda in der Tatsache, dass der Informationsaustausch über Intermediäre stattfindet. Deshalb möchte das Projekt für eine einheitliche Infrastruktur sorgen, die es Unternehmen ermöglicht, in Form eines Peer-to-Peer Verkehrs direkt miteinander zu kommunizieren, ohne auf viele Umwege über Intermediäre zurückgreifen zu müssen. Es soll sichergestellt werden, dass beide Unternehmen in einer Transaktion dieselbe Datensicht haben.

Blockchain Anwendungsfälle

Identitätsmanagement, Soziale Netzwerke, Betrugsprävention, Anteilsübertragungen, Kundenbindung, Gesundheitswesen mit relevanten Daten wie Anamnese,

Behandlung und Diagnose, Rezepte – Doppeluntersuchungen, Behandlungen und Mehrfacheinreichungen von Rezepten könnten vermeiden werden.

In memoriam : Professeur émérite Hubert Schneuwly

Dr. Roland-Pierre Pillonel Wyrsch

C'est un matin du mois de mars que nous apprenions le décès à l'âge 85 ans de M. Hubert Schneuwly, Professeur émérite bien connu des ancien·ne·s du Département de physique et même largement au-delà. En effet, après avoir dirigé les séances d'exercices pour les futurs physiciens et le répétitoire des futurs médecins, au départ du Professeur Otto Huber, il avait assuré de nombreuses années les cours de Physique expérimentale de première année pour toutes les personnes se destinant à une profession scientifique. Ses cours étaient d'ailleurs très appréciés.

Ce que l'on sait moins, c'est qu'avant de s'engager dans les études de physique, il avait longtemps hésité avec la philosophie. « Par la physique et la philosophie j'espérais pénétrer l'organisation de la nature et du monde pour découvrir leur sens. J'avais l'intime conviction que ce sens était rationnel et qu'il suffirait de dégager des certitudes. Si j'ai choisi la physique, c'est parce que je pensais atteindre par elle plus rapidement des certitudes, plus restreintes parce qu'uniquement matérielles, mais plus absolues ». C'est ce qu'il écrivait en 1995 dans l'opuscule des professeurs de philosophie *Φ la philosophie et son enseignement*.

Aîné d'une famille de 5 enfants, ayant perdu leur père quelques années auparavant, au moment du choix il avait néanmoins beaucoup de mal à envisager d'entamer ses études à l'EPF de Zürich et jusqu'en 1957 Fribourg n'offrait en sciences que la possibilité d'une licence à quatre disciplines, parmi lesquelles il pouvait certes y avoir la physique. Mais en 1957, les instances universitaires validaient le règlement provisoire qui permettait d'obtenir un diplôme spécifiquement en physique, parcours que M. Schneuwly a immédiatement entamé. C'est ainsi qu'avec six de ses collègues, parmi lesquels le futur cardinal Henri Schwery, il appartiendra à la première volée des diplômés en physique de l'Université de Fribourg.

On connaît la suite : Diplômé de physique théorique en 1963, Docteur en physique expérimentale en 1969, Professeur assistant en 1973, Professeur extraordinaire ad personam en 1983, Professeur ordinaire en 1989, il sera également, plusieurs années durant, Président du jury d'examen de maturité au Collège du Sud. Durant toutes ces années, il a apporté une contribution importante à la compréhension des atomes exotiques. « Compréhension », tel était en effet le mot qui revenait le plus souvent dans son discours. Pour lui il s'agissait de la condition nécessaire et suffisante pour qualifier une attitude ou une découverte de scientifique, ce qui ne manquait pas de le mettre parfois en porte-à-faux avec des enseignant·e·s pour qui cette condition était nécessaire, certes, mais pas suffisante.

A sa retraite en 2002, loin d'être resté inactif, malgré un terrible AVC dont il est ressorti avec beaucoup de nouvelles questions existentielles, on le voyait régulièrement dans les cafés scientifiques au cours desquels il relançait le débat sur

l'importance de « comprendre la nature et pas seulement la décrire » et cherchait à obtenir des réponses sur ce que représente la vie durant un AVC, renouant avec le lien physique – philosophie de sa jeunesse.

Hommage à la mémoire de Dionys Baeriswyl

Prof. Xavier Bagnoud

Dionys s'en est allé discrètement le 9 août 2023 après s'être battu avec courage contre cette maladie insidieuse qui le consumait jour après jour. Pourtant, jusqu'au moment de son hospitalisation, environ deux mois avant son décès, il poursuivait avec passion ses recherches en physique théorique. Ne disait-il pas sur son lit d'hôpital, les yeux légèrement embués, qu'il devait finaliser la rédaction d'un article sur la formation de quartets dans les systèmes de fermions avec son collègue Philipp Werner. Cette course contre la montre, Dionys l'a gagnée. Le travail détaillé fut soumis quelques semaines avant sa mort et a été entre-temps publié.

Dionys Baeriswyl a suivi un parcours de vie plutôt atypique et riche en expériences. Après avoir achevé ses études en physique théorique à l'Université de Bâle en 1969, il a obtenu son doctorat à l'Université de Genève en 1973. Très vite, il a été engagé par le laboratoire RCA de Zurich. Cependant, la recherche dans une entreprise privée ne semblait pas être faite pour lui. Après environ neuf ans d'activité dans ce milieu, il décida de poursuivre librement sa carrière de chercheur en se déplaçant d'un centre de recherche à l'autre à travers le monde : Max-Planck Stuttgart, Orsted Institute Nordita, Brown Bovery, IBM Rüschlikon, USC Los Angeles, CNLS Los Alamos, ICTP Trieste, ETHZ, ISI Torino. Il marqua ce long périple d'une pierre blanche en obtenant, en 1985, la venia legendi de l'ETHZ pour sa thèse « Theoretical Aspects of Conducting Polymers ».

En 1989, Dionys Baeriswyl a été nommé professeur ordinaire et directeur de l'Institut de physique théorique de l'Université de Fribourg. Les nombreuses relations qu'il avait nouées durant sa période de free-lance, la renommée qu'il avait acquise et l'expérience qu'il avait accumulée ont constitué un apport important pour notre Alma Mater. Dès son entrée en fonction, Dionys s'est engagé sans compter pour donner un nouvel élan à la physique. Il s'est efforcé de réformer les programmes d'études, d'organiser le meilleur encadrement pour ses étudiants et ses doctorants.

La recherche, Dionys la menait avec passion et lucidité. A ses débuts, il s'était intéressé principalement à la physique des polymères conducteurs. D'ailleurs, la publication de ses travaux sur les corrélations électroniques dans le polyacétylène lui avait apporté une reconnaissance internationale. Puis, il s'était focalisé avec succès sur les applications diverses du modèle de Hubbard. En 1986, la découverte inattendue de matériaux supraconducteurs à haute température créa une énorme surprise. Vivement intrigué par cette découverte expérimentale, Dionys s'était résolument engagé à l'étudier, à la comprendre. Dès son arrivée à Fribourg, il incita ses collaborateurs à explorer les divers aspects de ces matériaux formés de multicouches et à développer des modèles appropriés. Par la suite, les projets de recherche s'étendirent de plus en plus aux propriétés conductrices et isolantes de la matière condensée portant le nom générique de « systèmes d'électrons fortement corrélés ». Pour faire avancer cette recherche, Dionys impliqua ses doctorants. Il organisa à

Lausanne, des rencontres régulières ouvertes à tous les chercheurs intéressés par cette physique. Ce fut un grand succès.

Avec ses projets de recherche, Dionys souhaitait avant tout maintenir ses doctorants à la pointe des progrès en physique théorique et à leur donner ainsi une formation de qualité. Leurs travaux étaient suivis avec attention. Ils étaient confrontés aux critiques et conseils des nombreux visiteurs de passage. Le succès a été au rendez-vous. C'est ainsi, qu'au moment de prendre sa retraite, Dionys ne pouvait cacher sa fierté d'avoir amené quatre de ses doctorants vers une brillante carrière académique en Europe et aux Etats-Unis.

Soulignons encore que de 2002 à 2004, Dionys a été doyen de la Faculté des Sciences de l'Université de Fribourg. Il s'est impliqué dans cette fonction avec sa détermination habituelle. Ce fut aussi pour lui l'occasion de participer aux premières démarches en vue de la création de FriMat et de l'« Adolphe Merkle Institute » en collaborant très étroitement avec le généreux mécène.

A la fin de l'année 2012, le Professeur Baeriswyl a pris sa retraite. Il ne s'est toutefois accordé aucun répit. Libéré des charges administratives, son activité de chercheur en physique théorique redoubla. Il poursuivit ses travaux et ses collaborations. Il s'engagea surtout dans le développement de l'« International Institute of Physics » à Natal au Brésil en secondant son collègue Alvaro Ferraz, directeur de l'institut. Chaque printemps, il se rendait dans ce centre de recherche où il avait obtenu le titre de Distinguished Professor en 2013.

Dionys avait une capacité de travail hors du commun qui laissait son entourage perplexe. Il était capable de renoncer à tant de choses pour servir la science. Combien de randonnées en montagne a-t-il annulées pour lancer de nouveaux projets de recherche. Combien de fois a-t-il délaissé son piano pour prendre le temps de discuter avec un étudiant ou de remettre sur les rails un doctorant à court d'idées. Néanmoins, ses grandes passions qui étaient la physique, le piano et les randonnées en montagne, Dionys essayait de les vivre entièrement et d'en faire profiter les autres. Il aimait amener ses collaborateurs dans des excursions qu'il organisait et, au retour, les inviter dans un bon restaurant. Il en était de même lorsque Kazumi Maki de USC Los Angeles, expert mondial en supraconductivité, venait à Fribourg. Ce grand physicien, nous gratifiait de conférences remarquables, nous apportait ses conseils avisés. Mais en fin de journée, avant de partager un repas, il tenait à prendre son violon et à demander à Dionys de l'accompagner au piano pour interpréter quelques concerti.

Jusqu'à la fin, Dionys est resté un éminent professeur de physique théorique, aimé de ses étudiants et de ses assistants, apprécié de ses collègues. Tous ceux qui l'ont côtoyé garderont de lui le souvenir d'une personne attachante, bienveillante et surtout dotée d'une générosité sans limites.