CONCORDIUM

# SAY HELLO TO THE WORLD'S FIRST ID/KYC READY BUSINESS BLOCKCHAIN NETWORK

**LARS SEIER CHRISTENSEN,**
Chairman of the Concordium Foundation

SUMMARY:

# THE CONCORDIUM PROJECT

What the Concordium Foundation is proposing is the creation of a global, decentralized, publicly accessible, fully secure transaction logging network that can be used by any business to log and act on almost any sort of transaction. The availability of such a network can potentially deliver large savings to many kinds of businesses—cost savings that relate both to gaining access to new possibilities and to saving money on internal infrastructure.

In many ways this is not all that different from what we have witnessed with the rapid growth of the internet—but where the founders of the internet failed to set in place a mechanism that would create an intrinsic economy around using the network transport provided, the whole idea behind the Concordium Network is to create what will in essence become an automated global market place for transaction logging—a resource any user, company, business or public sector agency can tap into in order to run smart contracts and other services—and where doing so leads to considerable efficiency gains and cost savings while at the same time fueling the intrinsic economy of the Concordium Network and creating network growth by rewarding participants for enabling the networks operation.

Lars Seier Christensen



The Concordium Network is a proof-of-stake-based blockchain network that will be designed from the ground up to deliver a trustworthy and solid foundation for business. It will feature a protocol-layer ID/KYC mechanism that ensures that every user on the network is identified, and that every transaction involves provenance tracking. These features do not prevent the provision of privacy (based on zero-knowledge proofs), but they provide an environment that we believe will be acceptable to regulators, to public institutions, to financial institutions and to "big business," while solving a number of key issues in blockchain-based transaction logging such as avoiding single points of failure and providing finality in transactions. With this initiative, the Concordium Foundation intends to address and improve various technical aspects of existing blockchains, but most importantly, it aims to provide a blockchain network that delivers a regulatable and compliant transaction logging, transaction settlement and transaction finalization environment while enabling a wide range of powerful and legitimate business applications through use of flexible smart contracts.

# TABLE OF CONTENTS


SUMMARY: THE CONCORDIUM PROJECT 2

WHY BLOCKCHAINS MATTER 7

- Bitcoin was the Beginning 9
- Ethereum Represented Extended Functionality 10
- The Future Belongs to a New Generation of Blockchains 12
- How Will Money Be Made in the New Generation of Blockchains? 13
- A $3.1 Trillion Business by 2030 15
- How Concordium Aims to Deliver 16

CONCORDIUM: DESIGNED FOR BUSINESS 18

- Who Is the Concordium Network For? 19
- Regulatory Compliance: An Opportunity for Concordium 20
- What Will Regulators Require? 21
- What Will It Take to Become Mainstream? 22
- How Business Can Benefit from Blockchains 23
- The Concordium Use Case Laboratory 26
- The Future Is Wide Open 27

CONCORDIUM NETWORK REVIEW 28

- Basic Structure and Key Features 29

CONCORDIUM BUSINESS FUNCTIONALITY 30

- Programmable Accounts 30
- Identity Layer 30
- Transaction Privacy 31
- Revocation of Privacy 31
- Protected Amounts and Balances 32
- Hyper-Transactions 32
- Unlinked Same-Owner Transactions 32
- Transaction Proofs 32

CONCORDIUM TECHNICAL FEATURES 33

- Protocol Upgrades 34
- OAK Programming Language 34
- Outstanding Transaction Speed 35
- Pre-Calculation of Needed Gas 35
- Certified Smart Contracts 36
- Verified Repository of Smart Contracts and Libraries 36
- Upgradeable Smart Contracts 36
- Illegal Content Revoke Mechanism 37
- Concordium P2P Network 37
- Formally Verified Codebase 37

CONCORDIUM TOKEN MECHANICS 38

- GTU tokens: Consistent Win/Win Design 38
- Creation of GTU 40
- Token Issuance 40

ROADMAP: CONCORDIUM PROJECT PLAN 41

- Marketing Intelligence 41
- Science-Based Development 42
- Building a Developer Base 42
- Designed-In Ease of Use 42
- Concordium Project Timeline 43

THE CONCORDIUM ORGANIZATION 44

- The Concordium Foundation 45
- Concordium AG 46
- The Concordium Science Team 47
- Making the World Embrace Concordium 47
- Where the Road Ahead Might Lead Us 48

TEAM AND ADVISORY BOARD 49

CONCORDIUM: CORE SCIENCE TEAM 50

- Professor Ueli Maurer, ETH Zurich, Science Advisor and Concordium Board Member 50
- Professor Ivan Damgård, Aarhus University, Cryptography Lead 51
- Professor Jesper Buus Nielsen, Aarhus University, Chief Scientific Advisor, Consensus Protocol 51
- Associate Professor Bas Spitters, Aarhus University, Chief Scientific Advisor, Formal Verification 52
- Associate Professor Claudio Orlandi,Aarhus University, Scientific Advisor, Cryptographic Protocol Design 52
- Chaya Ganesh, PhD, Aarhus University, Scientific Advisor, Zero Knowledge Proofs and Privacy Design 53

CONCORDIUM: CORE EXECUTIVE TEAM 54

- Lars Seier Christensen, Concordium Foundation Chairman 54
- Mateusz Tilewski, Chief Technology Officer 55
- Soren Kenner, Chief Marketing Officer 55
- Bjorn Krog Andersen, Chief Legal Advisor 56
- Daniel Tschudi, PhD, Science Liaison Officer 56
- Conor Ringland, Chief Operating Officer 57
- Jørgen Hauglund, Chief Financial Officer 57

CONCORDIUM: ADVISORY BOARD 58

- Anders Fogh Rasmussen, former Secretary General of NATO 58
- Lone Fønss Schrøder, Vice-chair VOLVO, IKEA and AKER boards and Fintech expert 58
- Hans-Ole Jochumsen, former Vice Chairman of NASDAQ 59
- Lars Christensen, Monetary Economist 59
- Steen Jakobsen, Chief Investment Officer, Saxo Bank 60
- Claus Nielsen, former Head of Markets, Saxo Bank 60

HOW TO CONTACT US 61

In the estimation of the Concordium Foundation and the Concordium team we are at the threshold of a new paradigm in blockchain development—one that will change the overall tenor of the space and leave older blockchains and cryptocurrencies behind in the wake of a new generation of more business-focused projects.

The sheer scale and scope of this opportunity is magnitudes larger than the current cryptocurrency market, which, despite the hype, in reality comprises an industry with a combined market cap smaller than that of Apple or Google.

What drives this potential for change is not, however, what media has dubbed "the disintermediation of the middleman," but rather the opportunity to instigate what could in essence be the greatest technology and infrastructure outsourcing project the world has ever seen. Think of how cloud computing has already begun changing the landscape of how businesses think about storage and servers and the savings this has led to. Then imagine a world, where businesses large and small begin to realize that a cheap, ubiquitous, secure, robust, unbreakable and fully decentralized infrastructure can in fact deliver on most of their needs for record-keeping and transaction logging and can do so at a fraction of the cost of the systems these functions are being run on today!

The Concordium Foundation's goal is to make the Concordium Network the world's first ubiquitous, standardized, easy-to-use and fully compliant blockchain network designed to provide both a solid store of value and the global backbone for keeping track of the world's transactions.

# WHY BLOCKCHAINS MATTER

Goods, services, money and information now move at a velocity that was unheard of even five years ago. The internet has grown to encompass more than half of the planet's population, and every single day millions and millions of business transactions are conducted online at every level of society—between individuals, businesses, public sector agencies, governments and more.

However, while the internet is capable of facilitating this gigantic daily exchange of information, it delivers no inherent mechanism for secure tracking and logging. In essence, the trust required to transact must be established either directly between the transacting parties, or in many cases via a trusted intermediary. And even when trust can be established, there is no guarantee that every transaction will be correctly documented and logged for later retrieval.

In other words, there is a substantial need for secure, trusted logging and storing of transactions of every sort.

Blockchains are secure online ledgers shared between thousands or even millions of computers that allow untrusted parties to reach digital consensus without a middleman. They represent immutable and, practically speaking, unbreakable logs of transactions that operate as a trusted intermediary by establishing verification of any agreed transaction.

The current generation of emerging blockchain technologies holds enormous promise for delivering on these vital requirements of trust, transparency and secure logging. They will in all likelihood become a new and ubiquitous backbone for the secure storage of the world's transactions—and as such this nascent technology might in the future become as widespread and as widely used as the internet, or even become a de facto extension of the internet used to undertake and document transactions between individuals, businesses and public sector agencies. It holds the promise of adding efficiencies, security and cutting costs in fintech, procurement, logistics, distribution, payment, journalizing (healthcare, public records), decision-making (voting), identity management (ID, licenses, permits, etc.) and many other areas.

## BITCOIN WAS THE BEGINNING

The Bitcoin network was created by an anonymous programmer (or perhaps a group of programmers) using the nom de plume Satoshi Nakamoto. The identity remains uncertain to this day. Their idea, however, has had a massive impact: creating a digital, secure and unbreakable currency that would remain beyond control of governments and central banks.

Bitcoin was, and remains, a network where anonymous account holders can send and receive bitcoins (digital cryptocurrency tokens); where bitcoins can be stored securely in digital wallets and can be traded against other cryptocurrencies or legal tender such as dollars or pounds on a number of "cryptocurrency exchanges," such as Coinbase, Binance, Bitfinex and Kraken.

Bitcoin was intended as an unregulable alternative to central banking and therefore designed to cloak transactions beyond the reach of any regulatory or governmental agency. An immutable record of transactions would allow anonymous parties to trust each other and allow cryptocurrency to attain many of the same properties as legal tender.

In some sense that idea has come to fruition because, although the Bitcoin cryptocurrency remains extremely turbulent, some would say it has already become a better store of value than currencies such as the Venezuelan bolivar, Argentine peso, South African rand or Zimbabwean dollar. However, despite demonstrating that ability, its inherent structure—the basic functionality and the use of anonymous transactors—has led to considerable problems with the platform being used for money laundering, to the point where most banks today refuse to receive funds originating from the trading and sale of bitcoins.

## ETHEREUM REPRESENTED EXTENDED FUNCTIONALITY

In 2015, a team of programmers led by 21-year-old Vitalik Buterin launched the Ethereum network, and with it took a large step forward in the evolution of blockchain networks—they introduced the idea of "smart contracts" extending usage of blockchain beyond transactions relating to a single cryptocurrency and into the logging of transactions of any sort.

It was smart contracts in particular that captured the interest of the market. Via a smart contract type known as ERC-20, it became possible for users of the Ethereum network to create their own cryptocurrencies, as well as so-called "utility" tokens that provide network functionality beyond simple currency use, that could then be sold or traded. This sparked a frenetic rush of ICOs, an acronym for "Initial Coin Offering," which are in many ways similar in nature to initial public offerings.—

```
= GiveRightToVote Address
| Delegate Address
| Vote Proposal
| GetWinningProposal (String → toMsg)

receive : Blockchain → Model → ( Caller, Amount, Maybe (Msg wrapper) ) → ( Model, Tx )
receive blockchain model ( caller, txAmount, msg ) =
    case msg of
        Nothing →
            ( model, Tx.none )

        -- Give `address` the right to vote on this ballot.
        -- May only be called by `model.chairperson`, has no effect if voter is already registe
        Just (GiveRightToVote voterAddress) →
            if caller.address == model.chairperson && not (Dict.member voterAddress model.voters
                ( { model | voters = Dict.insert voterAddress (NotVoted 1) model.voters
            else
                ( model, Tx.none )

        -- Delegate your vote weig
        -- Will sub-dele
```

In essence, the Ethereum network became a mechanism for making previously illiquid startup investments liquid and tradeable. The issuer of an ICO publishes a "white paper" describing the intended use of proceeds from the sale of the coins issued via the Ethereum ERC-20 contract. Purchasers buy tokens in the hope that a successful launch of the project will lead to rapid appreciation of the tokens, which could then be resold at a substantial profit to the next buyer.

Between 2015 and mid-2018, more than 10,000 ICOs were conducted, raising a total of almost US$20 billion, with the largest offering being the EOS ICO, which took in approximately US$4.1 billion in investor funding. This ICO frenzy has not been without problems. There is little doubt that a large percentage of them are, at best, ideas that will not come to fruition and, at worst, regular scams aimed at relieving gullible investors of their hard-earned money, fueled, of course, by the 2017 rally in Bitcoin and Ethereum and the promise of getting rich quick.

The initial rounds of ICOs were generally conducted without compliance with securities laws. Not surprisingly, these transactions attracted attention from the SEC and other regulatory agencies, with the result that new coins or blockchain tokens are now generally considered to be securities, and ICOs or token launches are generally conducted in compliance with securities laws applicable to "private placements," or unregistered offerings, of securities. The characterization of most utility tokens as securities, in addition to potentially hampering initial capital-raising activity for blockchain enterprises, also poses challenges to the development of their utility networks, as many network plans depend on widespread distribution of tokens to achieve network effects—an objective that runs counter to the initial sale and resale limitations of private placement rules. It remains to be seen how these challenges will be addressed.

## THE FUTURE BELONGS TO A NEW GENERATION OF BLOCKCHAINS

From 2016, a wealth of new ideas and perspectives have entered the blockchain arena. New projects with a more scientific approach have become the norm, with cryptography developed by academic research teams using math that can be formally verified to prove that their blockchains are for all practical purposes unbreakable. Projects such as Concordium, Cardano, Tezos, Zilliqa, RChain, Dfinity and Algorand show that the real future for blockchain reaches well beyond cryptocurrencies. It has more to do with global, secure logging and storing of transactions of every sort. Its power is its potential ability to immutably document those billions of deals conducted online by millions and millions of users at every level of society. Now, to be successful, new blockchains must deliver on requirements well beyond the simple ability to move tokens between anonymous parties and instead develop technologies that support a very wide range of business requirements.

In the estimation of the Concordium Foundation and the Concordium team we are at the threshold of a new paradigm in blockchain development—one that will change the overall tenor of the space and leave older blockchains and cryptocurrencies behind in the wake of a new generation of more business-focused projects.

The sheer scale and scope of this opportunity is magnitudes larger than the current cryptocurrency market, which, despite the hype, in reality comprises an industry with a combined market cap smaller than that of Apple or Google.

## HOW WILL MONEY BE MADE IN THE NEW GENERATION OF BLOCKCHAINS?

Most newer blockchain projects require the payment of a fee in cryptocurrency tokens, often referred to as gas, for every transaction on their network. Gas is partly to reward network participants—often known as miners or bakers—and also to bolster the treasuries of these networks.

Imagine a network, which, at the outset, has a limited number of users and a limited number of transactions, and for which a fixed number of tokens is issued to investors. Initially the value of these tokens will represent the investors' belief in the network's ability to grow and generate transactions. If the network proves capable of growing into managing billions and billions of transactions, all of which require gas, then it follows that the value of the issued tokens will also increase, based on simple supply and demand mechanics.

In essence, each network then runs an internal economy where tokens become the basis for complete ecosystems of trade between constituencies and stakeholders; where transaction fees drive user participation; where business requirements drive developer engagement and fuel delivery of new smart contract types; and where the network as a whole grows and thrives by creating an infrastructure with a win/win scenario for each and every participant.

Interestingly, looking at token transactions taking place on the Ethereum blockchain, and comparing the gas value (fee payment) to the overall market cap of Ethereum tokens, this network appears to be running at a price/earnings ratio of around 100—expensive compared to the current P/E of Google and Apple (both in the 20s), cheaper than the P/E of GoDaddy at 171, HubSpot at 388 and Square at a staggering 1052. What this indicates is that while Ethereum tokens are very volatile, they are also priced within range of what you see in quite a few other investment scenarios.

We believe the best measure for determining the future value of a new blockchain network, and its tokens, is to look at the overall functionality and quality of the features on offer, as well as its approach to driving market entry, building growth-oriented ecosystems, developer engagement and use case development. In other words—if the network looks set to deliver something needed by the market and is easily adaptable across a host of different sectors, its initial issuance of tokens should increase in value over time.

The paradigm here is completely different from the first generations of blockchains, and it is the belief of the Concordium Foundation that we will witness these early cryptocurrencies and tokens lose value because there is no intrinsic value in their purpose. At the same time, newer networks, whose in-network economies create profit by dint of transaction fees, will become better and more efficient stores of value and will grow in value as they grow in transactions served.

## A $3.1 TRILLION BUSINESS BY 2030[1]

The first generations of blockchains launched the idea of cryptocurrency but did not really make any significant move towards capturing the enormous underlying global market for transaction logging—in some sense it was as if all the hype surrounding the idea of cryptocurrencies and the suggestions that they would and could replace central banking and fiat currency obscured the underlying potential.

On top of that, these early generations of blockchains did not and still do not have the features and functionality required to become a truly global backbone for transaction logging. They lack flexibility and feature richness but most of all the idea of anonymous transactors, while perhaps appealing to a fringe crowd of anarcho-capitalists—, is not, at the end of the day, in line with what businesses or regulators require.

However, once networks that can deliver on key business requirements start to get off the ground there is little doubt that the overall potential is staggering—Gartner Group believes the value of this nascent market will be around $3.1 trillion just 12 years from now in 2030. In many ways this outlook corresponds to the development of the Internet—from a slow start in the early 1990s with little clarity on what it could be used for to the emergence of the massive juggernaut that today, some 30 years later, dominates and pervades pretty much every aspect of how we do business and has wrought enormous amounts of disruption and transformation on industries that had no idea of the tsunami that was about to hit them when the transformation began.

[1] According to Gartner Group. https://www.zdnet.com/article/what-is-the-future-of-blockchain/

## HOW CONCORDIUM AIMS TO DELIVER

Our decision to organize the Concordium project as a non-profit foundation has to a large extent been shaped by our understanding of how best to organize resources to create results: the Concordium Foundation will become the focal point for the Concordium Network and spearhead its development.

The Concordium Foundation will work with developers and scientists to create the cryptography and code development required to launch the network and will act as the coordinator and manager of our outreach programs. Furthermore, we have designed the entire incentivation scheme surrounding the Concordium Network on the premise that every action must by necessity lead to continued network growth by continuously rewarding behavior that leads to usage and transaction growth.

To facilitate a focused development process the Concordium Foundation has entered into a development agreement with Concordium AG, a software development company set up for the express purpose of developing the Concordium Network as specified by the Concordium Foundation. Likewise, the Concordium Foundation has already made agreements with leading cryptographers and mathematicians to create the initial cryptographic framework for the Concordium Network and subsequently to research and develop science packages aimed at further commercialization of the Concordium Network.

For all of these reasons we believe the value of the Concordium Foundation in delivering a focused, directive and business-oriented thrust cannot be overestimated and in fact the role of instigator and manager of network development has been written into the Concordium Foundation's mission statement. The Concordium Foundation will strive to ensure strong governance and business focus – something that has often been lacking in other projects.

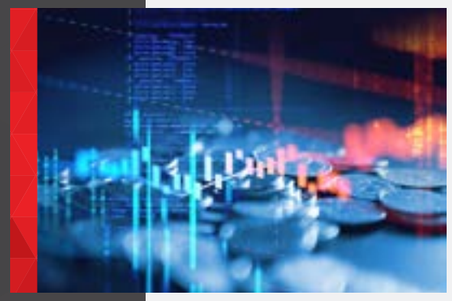
**NETWORKS** A blockchain-based network based on state-of-the-art technology and designed from the ground up to deliver on what businesses require vis-à-vis transaction logging and finalization.

**DEVELOPERS** developer support program, that helps ensure that users, whether they be individuals, businesses or public sector agencies will have easy access to resources that can help create whatever sort of application they require.

**TOOLS** A set of tools to help blockchain-based transaction logging become mainstream by delivering flexibility and functionality that makes this technology easy and cost-effective to use.

**OUTREACH** An outreach program designed to set the ball rolling by actively engaging a number of relevant users—whether they be businesses or public sector agencies—to cooperate on creating use cases and building experience in the use of this nascent technology.

**STANDARDS** The creation of shared standards in a number of areas such as code verification, protocol upgradeability, code libraries and more. A key driver in the rapid growth of the Internet has been the establishment of cooperation to define common standards such as IP, TCP, TLS, DNS, etc. There is no reason the same approach could not work for distributed networks.



# CONCORDIUM: DESIGNED FOR BUSINESS

The Concordium Foundation aims to bring together state-of-the-art cryptographic science, cutting-edge software and solid business acumen to create the robust and scalable blockchain network that we believe big business demands and deserves. Through our exploration of the market, we have identified the following areas in which we believe blockchain technology must be adapted to suit the needs of businesses.

## ANONYMITY IS OUT

Businesses are not interested in anonymity. They must know who they are dealing with and be able to comply with any current and future regulatory requirements.

## TRANSACTION PRIVACY

While professional users do not like anonymity they do require transaction privacy. The idea of anyone viewing your transactions, as is the case with most blockchain networks, holds little appeal.

## REGULATORY COMPLIANCE

Businesses must comply fully with regulatory requirements, ranging from ID/KYC to simple things such as checking VAT numbers or customer age.

## INCREASED SECURITY REQUIRED

Businesses will not run mission-critical applications on new technology unless they are absolutely certain it is, for all practical purposes, unbreakable.

## FLEXIBILITY AND EASE OF USE

It is difficult for businesses to get current blockchain networks to perform as they want them to. Smart contract creation is cumbersome, network performance often lags, glitches are too common, and functional flexibility is poor.

# WHO IS THE CONCORDIUM NETWORK FOR?

Financial institutions and fintech businesses are expected to become the predominant users of blockchains[2], with manufacturing and procurement, distribution and services, and the public sector also in the frame.

In the past, the key barriers to the broad adoption of blockchain technology by banks and big business were regulation and compliance-oriented issues. We consequently believe that networks that successfully tackle these issues while also delivering solid functionality and flexibility stand a very good chance of success.[3]

The Concordium Foundation's goal is to make the Concordium Network the world's first ubiquitous, standardized, easy-to-use and fully compliant blockchain network designed to provide both a solid store of value and the global backbone for keeping track of the world's transactions. The Concordium Network's key features—the identity layer, ability to support KYC/AML regulation, account flexibility and smart contract flexibility are based on what businesses and public sector users have asked for, and we are currently setting up work groups to focus on industry-specific blockchain needs and to understand in greater depth, and share with our developer base, where the technology can make a difference. We want to get the dialogue and experimentation flowing. We want to make it easy to try out things and, ultimately, work with industry to create ongoing use cases that showcase Concordium's cost-effective transaction logging, and help us grow the presence of the network.

[2] https://www.cbinsights.com/research/blockchain-disrupting-banking/?utm_source=CB+Insights+Newsletter&utm_campaign=2207499c76-TuesNL_09_04_2018&utm_medium=email&utm_term=0_9dc0513989-2207499c76-91396985

[3] https://www.cbinsights.com/research/blockchain-disrupting-banking/?utm_source=CB+Insights+Newsletter&utm_campaign=2207499c76-TuesNL_09_04_2018&utm_medium=email&utm_term=0_9dc0513989-2207499c76-91396985

## REGULATORY COMPLIANCE: AN OPPORTUNITY FOR CONCORDIUM

Regulation of both cryptocurrencies and the blockchain space is coming. In April 2018, the European Commission stated: "Twenty-three European countries have signed a declaration on the establishment of a European Blockchain Partnership. The Partnership will be a vehicle for cooperation amongst Member States to exchange experience and expertise in technical and regulatory fields and prepare for the launch of EU-wide blockchain applications across the Digital Single Market for the benefit of the public and private sectors. This should ensure that Europe continues to play a leading role in the development and roll-out of blockchain technologies."[4]

While government legislation and regulation may strike concern for investors in older blockchain networks, there is a clear opportunity for newer networks to take advantage of the impending change. According to Forbes: "2018 is poised to be a year of regulatory clarity for cryptocurrencies - but in what capacity? Legislatively or via regulatory action? Under state or federal law? Or will it be some combination of all the above? And, even if government action can catch up, how long can that parity last before the crypto-space speeds ahead? Governments inherently, and usually appropriately, move slowly and with deliberation, and investors may hesitate as they wait for government action. In that case, the market may need to step in to police itself. Cryptocurrency managers should anticipate and get ahead of these coming changes by identifying their own risk areas, developing mitigation controls or even a formal market-wide due diligence process."[5]

The sentiment is shared by The Next Web company, which provides a list of 15 countries where regulation is being discussed. Among them are the US, Canada, Japan, Korea, China, Singapore, Australia and the EU: "If 2017 was the year of the ICO, it seems as if 2018 is destined to become the year of regulatory reckoning. Things have already begun to heat up as countries around the world grapple with cryptocurrencies and try to determine how they are going to treat them. Some are welcoming, others are cautious. And some countries are downright antagonistic."[6]

[4] https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership
[5] https://www.forbes.com/sites/rosemaryfanelli/2018/05/29/four-things-to-watch-for-in-cryptocurrency-regulation/#42a4407f7012
[6] https://thenextweb.com/hardfork/2018/04/27/cryptocurrency-regulation-2018-world-stands-right-now/

### KNOW YOUR CUSTOMER (KYC)

Capital gains made on token trading will be something that many governments will require reports on in order to inform tax bills. To do so requires knowledge of the transacting parties and that means KYC regulations on blockchains and exchanges—the ability during onboarding to identify users as individuals or corporations with registered signatories. A successful blockchain must have compliance preassured across numerous jurisdictional boundaries.

### CONSUMER EXPOSURE

Under the current SEC approach, tokens are only being sold to accredited investors. To our knowledge, no blockchain tokens have been offered in a fully SEC-registered public offering. The SEC and other market regulators have been aggressively pursuing scams and other violations.

### REVOCABLE PRIVACY

On one hand, blockchain users require fully private transactions. On the other, regulatory agencies with court orders in hand must retain the power to revoke that privacy if needed. A successful blockchain must provide both—full transaction privacy and a trustworthy system for privacy revocation, mindful of jurisdiction.

### ANTI-MONEY LAUNDERING (AML)

To prevent blockchains and cryptocurrencies from becoming havens for money launderers, organized crime and drug or weapons trafficking, each transacting party must be accountable for incoming and outgoing transactions. We predict that regulation will demand full provenance and traceability of all circulating tokens and the undoubtable identification of who is behind them.

## WHAT WILL REGULATORS REQUIRE?

Until specific regulations of the blockchain/cryptocurrency market are announced, the details remain uncertain. However, ID/KYC and taxation will likely be first on the list.

For a network to deliver on all of these requirements is difficult, and for many existing blockchains will be impossible. Regardless of what Bitcoin, Ethereum, Stellar, Monero, Dash or Zcash do in the future, they will find it exceedingly difficult to untangle the identities or provenance of past transactions, their willingness to bend to regulatory pressure notwithstanding. The technology structures of many of these prominent blockchains simply cannot be modified to allow it, Bitcoin and Ethereum included. Any blockchain capable of supporting regulatory requirements gains an opportunity for traction over older, non-compliant networks.

## WHAT WILL IT TAKE TO BECOME MAINSTREAM?

Delivering on future regulatory requirements is only a small part of what is needed to succeed as a truly mainstream global backbone for keeping track of the world's transactions.

### PRIVACY MUST REPLACE ANONYMITY

The first versions of blockchains (Bitcoin and Ethereum) were built on the idea of anonymous users transacting publicly, with every transaction out in the open. A business-ready blockchain must allow known users to transact in private without that veil of privacy interfering with the provability, immutability and decentralization of the blockchain concept.

### FLEXIBILITY, FUNCTIONALITY AND OPENNESS

For a blockchain to succeed as a mainstay of industry it must be extremely flexible, enabling a myriad functionalities that allow businesses to integrate and interoperate with it as they choose. It must be open and interoperable with other technologies and legacy systems.

### SPEED AND SCALABILITY

Anything shy of near-instantaneous transaction speed and scalability will not be accepted. The blockchain must be able to bear the weight of ubiquitous, pervasive and multifaceted use without crumbling or slowing down.

### STANDARDS-BASED AND STANDARDS-CREATING

Like most nascent technologies, the ability to create de facto standards helps the whole market move forward, as does an invitation to developers and other network organizations and providers to participate in forging these agreements.



## HOW BUSINESS CAN BENEFIT FROM BLOCKCHAINS

With a network that delivers functionality and flexibility, businesses can use blockchains to cut costs, enhance security and improve efficiencies. It is only the technical issues, vulnerabilities and lack of functionality in current networks that have prevented them so far.

With the reins off, the potential applications are staggering. The Concordium Network will be designed from the ground up to address these shortcomings and supply business users with standardized, automated trust guarantees that we believe will help businesses deliver significant transaction cost savings. Almost any sort of business has a need to register and finalize transactions, whether via a simple ledger, a more complicated escrow system or in the shape of a fast-moving automated transaction logging system.

What the Concordium Foundation in essence is proposing is the creation of a global, decentralized, publicly accessible, fully secure transaction logging network that can be used by any business to log and act on almost any sort of transaction. The availability of such a network can potentially deliver large savings to many kinds of businesses—cost savings that relate both to gaining access to new possibilities and to saving money on internal infrastructure.

In many ways this is not all that different from what we have witnessed with the rapid growth of the internet—but where the founders of the internet failed to set in place a mechanism that would create an intrinsic economy around using the network transport provided, the whole idea behind the Concordium Network is to create what will in essence become an automated global market place for transaction logging—a resource any user, company, business or public sector agency can tap into in order to run smart contracts and other services—and where doing so leads to considerable efficiency gains and cost savings while at the same time fueling the intrinsic economy of the Concordium Network and creating network growth by rewarding participants for enabling the networks operation.

The next pages showcase some obvious examples of the type of solutions we believe businesses will be able to create with the Concordium Network—and it is worth noting that the majority of these examples gain their validity precisely because of the intended functionality of the Concordium Network. Simply put, knowing your counterpart is an absolute requirement in any number of applications that deal with monetary transactions, supply chains, distribution, etc. Hence, blockchain designs based on user anonymity and lacking the ID/ID/KYC layer suggested by the Concordium Foundation will have a hard time delivering on these obvious requirements.

### TRUST BUILT ON PROOF

Blockchains are based on cryptography. At their heart is the idea that the process and output cannot be breached or broken and that created logs or records are immutable. There are, however, two ways of looking at this. One is believing that a system is safe until someone comes along and proves that it is not. The other is proving that it is as secure as it is possible to be by using functional language programming and formal verification that your technology delivers exactly what your cryptography's math states.

### UPGRADEABILITY

One difficulty with earlier blockchains is that their individual components - P2P layers, consensus protocols, computation layers, etc.- are set in stone and difficult or impossible to upgrade without hard forking the network. A modern, mainstream blockchain network needs to be future-proof. While individual components can be upgraded it must retain integrity without affording anyone the opportunity to tamper with the system or attain control of the network.

### LARGE AND ROBUST ECOSYSTEM

For a blockchain network to become truly ubiquitous in scope and scale it requires a large ecosystem of independent developers, ranging from individual freelancers to larger consultancies and software houses. The programming language used to build smart contracts and applications to run on the network must be simple, easy to learn, and preferably already in widespread use. It should deliver very solid mileage in terms of libraries, ready-to-use packages and templates and just plain, old, easy-to-build structure.

## FINANCIAL SERVICES

The potential use cases for the financial services industry is wide ranging.
Obviously, these are merely examples, but the point being that anyone that is familiar with the inner workings of banking infrastructure will quickly realize that there are a large number of processes that can be optimized and automated by using distributed ledger technology—and if implemented intelligently would lead not just to enhanced performance but also to substantial cost-savings compared to existing solutions.

**COMMUNICATIONS:** Corresponding bank communications, tracking and finalization. Making it easier to transfer funds between banks and across borders. Reducing transactions costs. Resolving transfer disputes.

**ESCROW:** Smart contracts that stipulate escrow release when both seller and buyer agree that the conditions of the sale have been met.

**PAYMENT MANAGEMENT:** Using blockchains to document payment transactions. Transactions can be summed up/aggregated in order to deliver an environment with very high transaction processing speed.

**TRI-PARTY REPO:** Collateralized loan where cash is exchanged for securities and then reversed the following day. Blockchains could be used to document agreement, ownership, bank information, etc. An easily automatable process.

**ASSET CUSTODY:** Blockchains can be used to establish the provenance of an asset and prevent its transfer without a "green light" from a provenance-tracking smart contract. This could potentially reduce theft as well as transaction costs by automating functions relating to verifying ownership.

**ASSET-BACKED SECURITIES:** Blockchains can potentially manage portfolio of assets used to collaterilize loans and could automate the replacement of collateral as loans are paid.

**MORTGAGE FINANCING PROVENANCE:** Where mortgages are extended in real estate transactions (or sometimes for boats, cars and planes) blockchains can be used to establish the provenance of a mortgaged asset and can be written as a block on the issuing bank's blockchain solution.

**SETTLEMENT:** Blockchains can be used to automate immediate settlement, reducing operational risk and potentially eliminating settlement failure or incomplete deliveries.

## SUPPLY CHAINS AND PROCUREMENT MANAGEMENT

A key component in supply chain management as well as in procurement management and invoice settlement including invoice collaterization is the ability to quickly and securely log transactions whether they be deliveries, processes, freight, goods, parts, services or any other component of the myriad of gadgets, processes and structures that make up the foundation of any big business doing manufacturing, distribution or process management. Some obvious examples:

**CHAIN OF CUSTODY:** Blockchain networks can be used to provide provenance, chain of custody and certification of supply chains. An enormous amount of business is being transacted in this area annually and any means of automating, enhancing or making processes more efficient will have great value for users.

**PRODUCT VERIFICATION:** Blockchains can be used to log and track the provenance of any type of goods or services—and doing so can help fight counterfeit products and the resale of stolen items. The number of potential use cases here are staggeringly wide: from pharmaceutical companies needing to help protect their customers against counterfeit products, to manufacturers of phones, stereos, computers, glasses, cars, motorcycles, yachts, planes, diving equipment, etc.

**SHIPPING MANAGEMENT:** Every day, millions of containers are making their way from continent to continent carrying goods of many, many different kinds. Blockchains can help provide tracking and product provenance data, making shipping and distribution easier for shippers, freighters, customs and customers by supplying close-to-real-time immutable data on what is being shipped and where it is at any given moment.

**PROCUREMENT MANAGEMENT:** Pretty much every business on the planet is trying to figure out how to pay suppliers on time while keeping cash on hand as long as possible—and in many situations procurement management also involves payment services and often also collateralized financing of invoices. Blockchains can help organize chains of custody and agreements helping everyone in the supply chain understand who is responsible for what and when—and can help automate the movement of procurement management processes, whether this is about dealing with payment, delivery confirmation, invoice financing or any other related service.



## RETAIL BUSINESS

Small and large retailers can benefit from blockchain networks in a number of ways. When interacting with suppliers, blockchains can be used to establish the provenance and status of goods and can be used to manage suppliers and vendors. Blockchains can also be used in a variety of customer-facing scenarios such as:

**LOYALTY PROGRAMS:** Obviously blockchains are also well suited for optimizing loyalty programs, keeping track of consumer transactions, allowing consumers to claim rewards and benefits and allowing merchants to harvest transactional data that can be used to refocus and retarget sales and marketing processes.

**CONSUMER PROVENANCE ACCESS:** Blockchains can make it easy for retailers to help their customers look up information on products they have purchased. In principle this registry can be anything from the provenance of a product to a manual, warranty, overview of content, use of chemicals, etc. The key point being that a shared global network for looking up information such as this would be much cheaper than each retailer having to build its own.

## HEALTH CARE

When we interact with health care providers the collection and secure storage of transactional data is not just important but in some cases can be life-or-death. Knowing about prior diagnoses and treatments, medications, allergies, or adverse reactions helps health care professionals provide better treatment. As patients seek help from different providers and different specialists, having access to shared yet fully secure and immutable records is extremely valuable to both health care providers, specialists, insurance companies and, not least, patients. Blockchain solutions can help provide secure logging of transactions relating to a wide range of health care services—and can potentially have great impact in terms of documentation, record-keeping and patient journals for both health care and the pharmaceutical industry.

## INSURANCE

At its most basic level, what is insurance but a ledger of risk, provenance, assets and agreements? Which is exactly what blockchains are good at handling. Insurance companies can use blockchains to help verify provenance of customer claims of many different types and they can use blockchains to document their underwriting, store agreements and contracts, etc.

## VOTING

Vote casting is an obvious task to run on a blockchain. You can create voting systems that will not allow the same vote to be cast twice, that will not allow tampering with votes, and that can identify who has voted while ensuring that how they voted remains private. A solution like this can be made to run on a smartphone or a tablet or it can become an integral part of a voting booth. And while casting votes is an important part of democracy the use cases do not stop with the election of public officials—thousands and thousands of organizations around the world, such as trade unions, professional organizations, universities, etc. use vote casting quite frequently. Blockchain-based voting solution can help increase voting quality, can help reduce voting fraud and can help make vote casting and tallying quicker, faster and less expensive.

As should be clear from these examples from different industries, blockchain networks can potentially open up very large markets and help individual users as well as businesses and public sector agencies solve a large number of tasks related to transaction logging, transaction verification, transaction settlement and transaction finalization.

Yet, while the promise is certainly there, progress has been slow. Why? Probably because earlier generations of blockchain networks have not been capable of creating the combination of features and functions required to deliver on these needs. At the end of the day, regardless of what sort of solution you are building, if you want it to function in the real world, knowing your counterpart is a prerequisite for most kinds of interaction, as is the ability to comply with any regulatory requirements.

By combining seasoned financial service executives with a group of the world's best cryptographers, and an in-depth understanding of online marketing software solutions and community development, the Concordium Foundation aims to deliver a blockchain network predicated entirely on meeting exacting business requirements. Our design aims to deliver a robust framework that is capable of supporting regulatory requirements, and provides a wide range of smart functionality backed by thorough documentation.

## THE CONCORDIUM USE CASE LABORATORY

As part of the initial planning and preparation for the Concordium Network we have had meetings with a number of businesses and discussed creating shared use cases. Here are some of the expressions of interest we have had in building use cases with us:

### MAJOR PROCUREMENT MANAGEMENT PROVIDER

A software company delivering global supply chain finance management has expressed interest in using Concordium technology to log customer transactions in near real-time.

### INVESTMENT AND ONLINE TRADING BANK

Concordium may help this global player in online trading with finalization and documentation of transactions.

### INTERBANK PAYMENT PROVIDER

This global bank-to-bank payment management service is interested in the Concordium Network for tracking and finalization.

### LARGE NGO WITH FOCUS ON DEMOCRACY

Concordium's technology could help increase transparency of democratic processes globally with a blockchain-based voting solution.

### AND QUITE A FEW OTHERS ...

Apart from the above examples we are in discussion with more than 20 other companies in fintech, procurement, shipping, distribution, settlement solutions, and public sector offices, all of which have shown a keen interest in the Concordium concept and have expressed willingness to continue the dialogue.

Although we have not obtained (and have not sought) any firm commitments for any shared use case deployments, we believe the discussions outlined above illustrate Concordium's potential and, in fact, also illustrates some aspects of the almost boundless opportunity that we believe exists for blockchain technology if it is brought into the realm of accountability, identifiability and compliance.

## THE FUTURE IS WIDE OPEN

While business and the public sector could reap very significant benefits from the advent of blockchain networks dedicated to transaction logging, settlements and finalization on a global scale, this is only the beginning. A number of other technologies would potentially also be able to run on these networks—not least applications dealing with multiparty computation and distributed computing.

Multiparty computation would allow transacting parties to engage in business or to cooperate without disclosing proprietary knowledge—for example, combining results from different databases (e.g. in pharmaceutical or materials science) without disclosing what is actually in these databases, or being able to do bidding rounds for future contracts where multiple parties can bid and a winner can be found without disclosing the actual bids.

Distributed computing is exactly what it sounds like—the idea that you can use the processing power of a distributed network to run calculations—in principle delivering computing power that is way beyond what is currently possible.

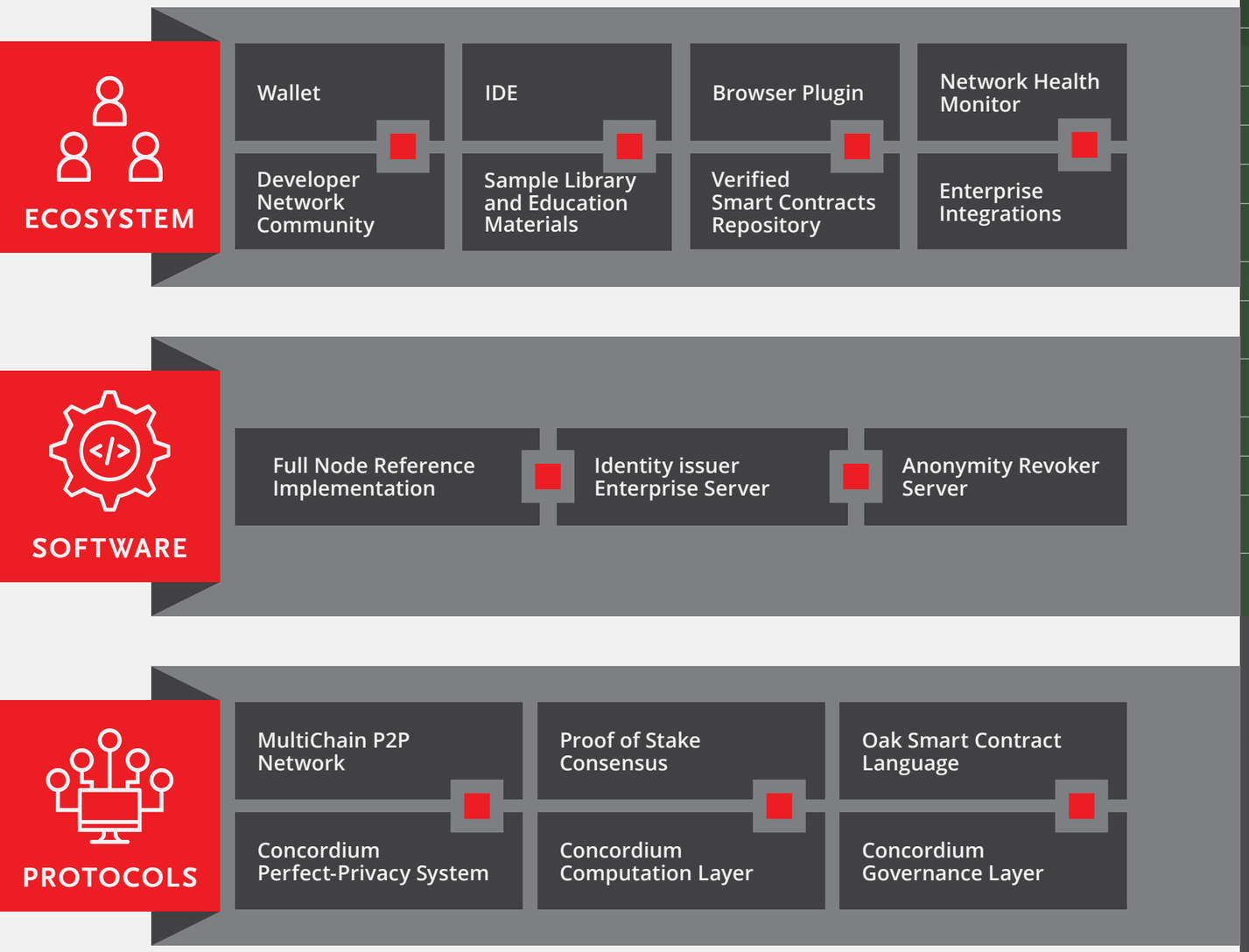
While both multiparty computation and distributed computing are in their early stages of development, who knows what sort of impact can be delivered by these technologies in five, ten or twenty years? And both of these technologies would most probably be able to run on the distributed network infrastructure the Concordium Foundation proposes setting up for global transaction logging.

# CONCORDIUM NETWORK REVIEW

The Concordium Network will be different from other blockchains. Our network will introduce a number of new concepts to the technology, allowing for mainstream business use and rapid growth. We are in the midst of creating a revolutionary consensus protocol, a ground—breaking system of manageable transaction privacy, and a new approach to finalization, resulting in a flexible, robust and secure network with outstanding transaction speed and the ability to capture a very large number of transactions.

This high-level review of the project focuses on the Concordium Network's functionality. More granular detail will be available in our upcoming technical white papers.

Some of the planned and proposed features of the Concordium Network are not described in this document because we are not yet ready to disclose them.






## BASIC STRUCTURE AND KEY FEATURES

The Concordium Network is designed to operate for mainstream business. As such, it offers an entirely different set of features than classical networks such as Bitcoin or Ethereum.

| THE CONCORDIUM NETWORK | CLASSIC BLOCKCHAINS (BITCOIN, ETHEREUM, ETC.) |
|---|---|
| Known users with verified identities | Anonymous users |
| Transactions can be private | Transactions are always publicly visible |
| Accounts have programmable features | Accounts consist of a number |
| Smart contracts can be based on multiparty provisioning of data | Smart contracts are strictly peer-to-peer |
| Provenance of tokens is tracked | Provenance of tokens is unknown |
| Upgrading mechanism for smart contracts | Live contracts cannot be upgraded |
| Supports ID/KYC regulation | Does not support ID/KYC regulation |
| Easy formal verification of contracts | Non-standard and cumbersome formal verification |
| Enables pre-execution gas calculations | Does not allow pre-execution calculations |
| Functional programming language: easy to program—hard to make mistakes | Hacky programming languages: hard to program—easy to make mistakes |
| Transactions are finalized periodically | Transactions are never finalized —rollback is always possible |
| Accounts have secret and public balances | Accounts only have public balances |
| Sharding available on protocol level | Sharding is not possible |
| Dynamic reward system—rewards adjusted on network health, speed and congestion | Static, predefined reward system |
| Block size and time adjusts dynamically, based on network health, speed and congestion | Block parameters are predefined and hardcoded |

Dependable management of accounts and identities, privacy of transactions and regulatory compliance—these are significant departures from the usual blockchain approach.

Unlike most blockchain projects, the Concordium Foundation does not believe this technology will disintermediate financial service institutions or do away with middlemen to provide a trusted environment. Instead, we see blockchain as a practical tool for logging transactions in a secure manner, and as a tool that offers new opportunities for business users in financial services, procurement, logistics, fintech and more.

# CONCORDIUM BUSINESS FUNCTIONALITY

## PROGRAMMABLE ACCOUNTS

On most blockchains an account consists merely of a number that identifies it. On the Concordium Network, accounts will function as programmable smart contracts. This allows users to set rules as to how transactions and funds are managed.

These rules can take the form of a receival policy, which may, for example, automatically reject funds that originate outside a given jurisdiction, or from unknown senders. This ability to reject transaction requests is a unique feature of the Concordium Network. Other planned features include automatic forwarding, making it easy to instantaneously manage VAT, taxes, referral fees, etc.

Contract calls can be set such that activity on one transaction can be used to alert others, which is useful for reporting and account aggregation.

The Concordium Network aims to deliver programmable functionality where users can choose from a wide range of predefined logic scripts or can develop their own custom applications. This level of flexibility is unprecedented and entirely new to blockchain networks. It will allow business users to create their own structures and to do transaction logging much more efficiently and in line with what they expect from their usual operating procedures.

## IDENTITY LAYER

With Concordium, new users will be onboarded via a Trusted Identity Issuer[7] that screens and verifies the user's identity before assigning a user ID, also known as an Identity Object.

This object is not directly deployed on the blockchain since it might hold personal data that in some parts of the world needs to be GDPR-compliant. What is deployed on the blockchain instead is an encrypted pointer that can only be unlocked by compatible anonymity revokers,[8] together with zero-knowledge proof of any fact contained in the Identity Object. Such proof can be checked for validity without anyone actually seeing the source or content of that proof, as its zero-knowledge name suggests.

Users can receive Identity Objects from any number of Trusted Identity Issuers, with each object generating only the specific subsets of information requested, such as proof of age, physical location, etc. As such, this mechanism can be used to integrate licenses, permits, credit scores, diplomas, certificates or any other profile statistic into a user's identity and store it all in a single file.

In addition, anyone can become an "untrusted" identity issuer. This allows companies using Concordium to establish facts about their own users, partners and providers—such as internal ID numbers and authorizations—that do not necessarily need to be verified by a Trusted Identity Issuer. Consequently, organizations can structure themselves into complete sub-networks on the system.

Identified users will be able to create an unlimited number of accounts linked to their identity and, in principle, each account can operate on different rules. Users will be visible to each other in the sense that you can look up a name, see whatever attributes that party allows and check who issued the identity. Once involved in a transaction, receivers will always be able to see the sender's required proofs, such as legal age, VAT number, etc.

[7] The first Trusted Identity Issuer will be the Concordium Foundation operating via a number of identity-checking services. Over time more Trusted Identity Issuers will be added. Corporations that want to use the Concordium Network can also become trusted identity issuers in regard to their own employees, business partners, etc.

[8] See "Revocation of Privacy" later in this document.



## TRANSACTION PRIVACY

In contrast to most blockchains, where anonymous users transact publicly, on the Concordium network known users will transact in private. This may sound simple and straightforward but it is most certainly not. We will use zero-knowledge proofs to cloak users privacy.

This is a cryptographic algorithm created in 1985 by Shafi Goldwasser, Silvio Micali and Charles Rackoff. Using this cryptographic technique every user can see the proof that the transaction was logged and registered correctly in an immutable network block.

## REVOCATION OF PRIVACY

The Concordium Network is designed for regulatory compliance. This means that an agency with the legal right to do so must be able to review specified transactions. The challenge is to construct a setup which allows for a legal disclosure of private transactions while maintaining user confidence that a breach would not be possible by any other means. The solution to this conundrum is the establishment of another Concordium innovation, the Directed Revocation Service. When a Trusted Identity Issuer delivers an Identity Object, this carries a key that designates compatible Trusted Revokers. A list of Trusted Revokers is maintained by the Concordium Foundation and is written into the network's governance layer. The Concordium Foundation has an additional, but different, key.

A user's privacy can only be revoked if two or more Trusted Revokers from an appropriate jurisdiction agree to do so on the basis of a court order or other legal requirement delivered to them. A single revoker cannot breach privacy on its own.

Even if privacy is revoked by court order this only means that the proper authorities can audit transactions. Other users, including the Trusted Revokers and Concordium, will not be able to view the transactions in question. Other users will not even know that a set of transactions has been ordered to be opened for review. If an audit uncovers no problems, there is no issue of the transactor becoming exposed to reputational damage. The audit will remain private.

Through the use of local Trusted Revokers, jurisdiction becomes easier to manage. For example, it will not be possible for someone outside a user's jurisdiction to demand revocation of privacy. The revocation request must originate with an agency inside the user's jurisdiction with the legal right to make such a request.

## PROTECTED AMOUNTS AND BALANCES

Every account on the Concordium Network will have two balances: a public balance and a protected balance. The public balance can be seen by anyone while the protected balance is always private. Users determine the value they want to keep in either account. Therefore, although identifiable as a user, you are not obligated to let others see your funds.

Accordingly, users can make either public transfers or protected transfers as needed. The only caveat is that the privacy of protected balances may be revoked by a set of Trusted Revokers as outlined on the previous page.

## HYPER-TRANSACTIONS

A common issue with blockchains is that contracts which fail to meet pre-agreed standards are executed anyway. This is because almost all other blockchains have sequential processing of contracts. We aim to introduce parallel execution to enable multiparty contracts. This means that users will be able to make the execution of contracts contingent on external data requested from a third party where that party may also function as an escrow. Transactions may be made dependent on a specific precondition existing in another smart contract and automatically verified. If a check-up on an external database reveals that a buyer does not have a valid permit or VAT number, for example, then that contract will not execute. As such, hyper-transactions enable easy-to-agree terms on more flexibly built contracts.

## UNLINKED SAME-OWNER TRANSACTIONS

The Concordium Network will allow unlinked transactions between a user's accounts to avoid loss of privacy through outside monitoring of common traffic, which would expose the accounts as linked. Since unlinked transactions can only be made between accounts owned by the same person, they do not conflict with KYC regulation.

## TRANSACTION PROOFS

Similar to an identity proof, users will be able to attach zero-knowledge proofs of specific actions having been performed. In other words, we will make it possible for one party to prove to the other that they have carried out a specific action as per the agreement. This might be signing a contract or making a transfer or checking an another kind of external requirement.

# CONCORDIUM TECHNICAL FEATURES

In describing the features of the Concordium Network we use the following terms:

### NETWORK SERVER

Software that can be installed on a PC and which, when running, functions as a network node.

### NETWORK USER

Anyone using the Concordium Network to process and log transactions.

### NETWORK BAKER

A network server that runs in baking node enabling the server to write blocks to the network.

The Concordium Consensus Protocol is a proof-of-stake–based consensus protocol with finalization and dynamic adjustment of parameters. There are four major innovations that set this protocol apart from other consensus protocols.

### PROOF-OF-STAKE

In older proof-of-work protocols like Bitcoin, network servers participate in calculation process to win the right to create new blocks and be rewarded for their "mining." The process consumes lots of power and sets a very high bar for becoming a miner. In the newer proof-of-stake protocols the server software's chance of "baking a block" is determined by how many tokens the server has on account. A trivial implementation of proof-of-stake would be to simply look at a servers wallet and adjust its winning chances accordingly. The Concordium proof-of-stake protocol, however, will use a number of additional parameters to incentivize "good server behavior"—among these are the amount of time the tokens have been in the wallet, how long the baker has been on the network and also an adjustment for "too large" to avoid ending up with a very small set of very token-rich bakers. This will ensure that there is a form of democracy on the network—all honest nodes that behave correctly have a chance of writing blocks and being rewarded.

### FINALIZATION

A big problem in current blockchains is rollback. In big projects, like Bitcoin, a rollback for more then a couple of blocks while improbable is theoretically possible. Only a few of the newer blockchains have finalization mechanisms, and Concordium Network may be only project that aims to deliver mathematically provable finalization. Finalization is part of the Concordium Network's consensus protocol where a number of network servers run a Byzantine fault-tolerant decision-making agreement to agree on finalization timestamps based on specific best chain rules. When a block has been finalized, it is not possible to roll back to a point in time before that finalization timestamp. This will effectively make the Concordium blockchain truly immutable and verifiable final. Obviously, being able to deliver rock solid finalization will be of major interest to the financial services industry.

### DELEGATION

Not every network user will run a baking node. But that does not mean that they cannot participate in the block baking rewards. Concordium aims to introduce a delegation mechanism so any network user can delegate their stake to any baker. That stake will then be included in the calculations of the baker's chances for winning the reward for writing the next block, and the rewards will be split between the baker and the delegating user. By default, all users delegate baking power to the Concordium Foundation. With time, it is envisioned that charities such as the Red Cross or USAID could run their own baking nodes that enable inactive users to delegate baking rewards earned on their stake to a chosen charity.

### OVERVIEW LAYER AND DYNAMIC PARAMETERS

The Concordium Network's consensus protocol defines some initial constants, such as block size, block time, finalization range, baking rewards, etc. However, the Concordium Network also includes an overview layer as part of the consensus protocol. This overview layer will monitor topical network data such as distribution of peers, transaction volume, local network latency, etc. and will combine this information with system-wide data such as overall number of Concordium GTUs transferred, complexity of invoked smart contracts during the last blocks, and so on. Every key blockchain parameter can then automatically be dynamically adjusted based on overview-layer data to keep the network running at optimal levels. When there is a lot of activity on the network, block time will get smaller, while peak activity will mean block time gets longer. If there are many baker nodes online, rewards get smaller and if there are fewer baker nodes online, rewards get higher, etc. We have named this approach the "dynamic consensus parameter." By adjusting all parameters dynamically, the network is more responsive and scalable and less prone to any kinds of bottlenecks.

## PROTOCOL UPGRADES

Decisions on the Concordium Network regarding who bakes blocks, defines finalization, etc. are based on rules that will be defined in the protocol and identified by a protocol version number. Since it is impossible to foresee all possible future situations we intend to make protocol upgrades and adjustment mechanisms part of the consensus protocol itself.

## OAK PROGRAMMING LANGUAGE

The Concordium Network will have its own smart contract programming language called Oak. It is based on a functional programming language called Elm and enables formal verification of smart contracts as well as pre-execution gas-requirement calculations.

In computer science, functional programming is a programming paradigm, a style of building the structure and elements of computer programs, that treats computation as the evaluation of mathematical functions and avoids changing-state and mutable data. It is a declarative programming paradigm, which means programming is done with expressions or declarations instead of statements.

In functional code, the output value of a function depends only on the arguments that are passed to the function, so calling a function 'f' twice with the same value for an argument 'x' produces the same result 'f(x)' each time; this is in contrast to procedures depending on a local or global state, which may produce different results at different times when called with the same arguments but a different program state. Eliminating side effects, i.e., changes in state that do not depend on the function inputs, can make it much easier to understand and predict the behavior of a program, which is one of the key motivations for the development of functional programming.

Oak is a purely functional language, developed with an emphasis on usability, performance, and robustness, and it delivers "no runtime exceptions in practice," via static type checking compilation. Oak is easy to learn, easy to program, difficult to make mistakes in yet still delivers a lot of mileage, allowing developers to get a lot done with just a few lines of code.

Elm, which is the precursor of Oak, already has a large user base, all of whom can start working on Concordium smart contracts right off the bat with only minor prerequisites. Additionally, Elm and Haskell package libraries has more than 10.000 packages, most of which are directly usable in Oak to create smart contracts on the Concordium Network.

## OUTSTANDING TRANSACTION SPEED

Concordium smart contracts will deliver parallel execution, which means bigger blocks can be written in a shorter time. However, our consensus protocol adjusts working parameters based on the health and state of the network as a whole. In less busy periods, block times are longer. In more busy periods, block times are shorter. As such, the transaction speed constraint in Concordium will not be the virtual machine/compiler, as in most other blockchain networks, but solely overall network latency.

Bigger blocks allow for aggregate transactions, for example, micropayments running on side-chains, which can then be aggregated and written onto a single block every so often.

Even when running with a heavy transaction load we expect to see significantly faster transaction speeds than with most other networks. This is made possible by a smart contract design that relies on pure functions, and which does not modify global states inside any execution path, but only as a result of execution.

## PRE-CALCULATION OF NEEDED GAS

Most blockchains operate on the basis of a token gas payment for contract execution, typically to reward the miners or bakers that write the blocks. Until now, however, there has been no way of pre-calculating the correct amount of gas to get a contract executed. This often results in contracts either not being executed because not enough gas was offered, or tokens being wasted because more gas was offered than required.

The Concordium Network aims to change that paradigm with the introduction of pre-calculation and contract certification. We will use a version of the Actor Model of concurrent computation with a message passing to a contract inbox. This means that you will know beforehand exactly how much gas to include to be sure that your transaction is successful. The Concordium Network will be the first blockchain network to allow pre-execution gas calculation and that means lower execution costs for the user.

## CERTIFIED SMART CONTRACTS

We aim to make it possible to formally verify and certify any Concordium smart contract. Contract certification means publishing a formal verification proof of the contract and its ability to execute and perform as required. Our protocol will ensure cheaper gas prices for certified smart contracts than for uncertified ones, giving developers incentives to do this certification.

As such, certified contracts can be proven to deliver what they are set up to do and will cost less to execute.

The Concordium Foundation aims to offer certification as a service and we intend our contract library and app store to have pre-certified contracts deployable by users.

## VERIFIED REPOSITORY OF SMART CONTRACTS AND LIBRARIES

Concordium aims to save users time and effort with access to libraries of already programmed smart contracts and libraries of functions. Developers can submit their smart contracts for library verification and, if their contracts are used on the blockchain, they will be rewarded. The users of the library material will pay less in gas costs for their contracts and the creators of the contract gets a kickback of some of that gas saving, thus incentivizing both parties.

## UPGRADEABLE SMART CONTRACTS

A smart contract is by default an immutable piece of code that cannot be destroyed once written into the blockchain. This is part of what ensures the unbreakability of the concept, but Concordium smart contracts will have an added feature: they can be upgraded at any time to deliver new features for new requirements.

We aim to make it possible for the user or designer of a contract to include version numbering and to make sure that it will always be the latest version of the contract that is executed.

## ILLEGAL CONTENT REVOKE MECHANISM

It is not hard to envision a situation where a contract is used to store illegal data, GDPR-revoked data or other unwanted content, and it may be that the owner of that contract is no longer on the network. In most other blockchains, there is no way to deal with this situation. However, we aim to include functionality to the Concordium Network's finalization layer that provides a solution to this challenge.

## CONCORDIUM P2P NETWORK

Concordium's P2P network is a fully secure peer-to-peer broadcast and message communication channel, encrypted with the latest Transport Layer Security (TLS) standard where the nodes participating in the network use existing, proven internet technology including DNS for node registration and discovery.

The network will be able to layer several blockchains on top of each other—a feature used in conjunction with the Concordium sharding and finalization protocol—and will be developed to be easily extensible and adaptable to carry whatever future communications are required as the concept develops, for example, the sharing of larger files. As such, the Concordium Network aims to become a fast network transport in a fully secure setting.

## FORMALLY VERIFIED CODEBASE

We aim to formally verify key elements of the Concordium Network codebase. Formal verification is a method normally used when creating software for airplanes and medical devices. These methods ensure that the codebase actually follows formal specification, so the risk of unexpected code exploits is minimized compared to traditional development techniques. Thus cryptographic strength does not have to be taken on trust, but can be proven.

# CONCORDIUM TOKEN MECHANICS

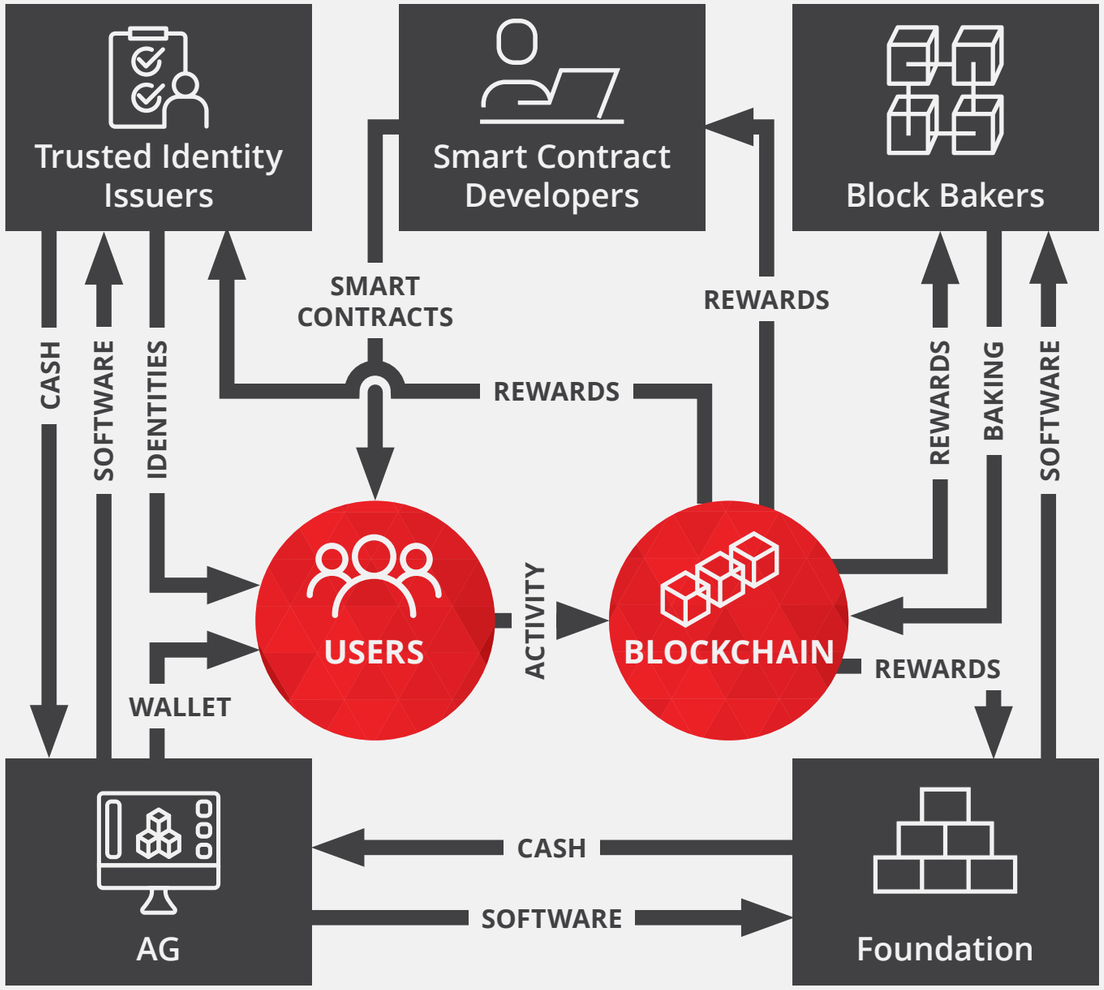
Early generations of blockchains recognized the need to reward network participants for writing blocks, but that was as far as they went. The initial focus remained on facilitating cryptocurrency transactions and not on the creation of entire blockchain network ecosystems.

The Concordium Network is designed for a much broader approach. Our aim is to grow the network to become a global backbone for transaction logging and we have designed our token structure, as well as other activities, with that in mind.

Each and every participant on the network will be consistently rewarded for activity. Whether a user, a developer or a baker, everything is geared towards supporting pervasive growth and, therefore, Concordium's ubiquitous presence and availability.

## GTU TOKENS: CONSISTENT WIN/WIN DESIGN

The Concordium Network is fueled by the GTU token (Global Transaction Unit). Our basic tokenomics design is simple. Logging transactions requires a gas fee payable in GTU while every supporting network role—running network nodes, providing identities, creating smart contracts, delivering consensus (baking) and so on—can and will be rewarded with GTU tokens.




This is a snapshot of Concordium's intrinsic GTU economy and reward structure

### NETWORK SERVERS ARE REWARDED FOR PARTICIPATION

If you run a Concordium Network Server, you will be rewarded for participating in baking, finalization or identity issuance.

### BLOCK BAKERS EARN REWARDS

The Concordium Network will use a sophisticated proof-of-stake algorithm for consensus on block-writing. Baking nodes will be rewarded with GTU tokens for baking blocks.

### BAKING PARTICIPATION CAN BE DELEGATED

If you are a user running a Concordium Network Server but are not interested in setting up a baking node, you can delegate your baking participation rights, allowing you to share GTU token baking rewards with bakers.

### SMART CONTRACT DEVELOPERS CAN EARN GTU TOKENS

The Concordium smart contract framework will enable developers to share network transaction fees. This incentivizes developers to create contracts for a wide range of uses based on a pay-per-use structure. This is a first for blockchains although the same practice is quite standard in other areas of software development, such as most app-store apps.

### CONCORDIUM FOUNDATION GTU TOKENS

When the Concordium Foundation launches the Concordium Network the "genesis block" (the first block of the blockchain) will be used to create a number of GTU-tokens that the Concordium Foundation will own. As transaction fees accrue this number will increase. The Foundation will use these tokens to support network growth by paying developers GTUs to create new contracts and functionality.

### GTU TOKENS TRADED ON CRYPTOCURRENCY EXCHANGES

Subject to applicable securities laws, the Concordium Foundation intends to arrange for GTU tokens to be bought and sold on key cryptocurrency exchanges such as Binance, Coinbase and Kraken. On these exchanges GTU could be traded outside the Concordium network based on simple supply/demand pricing. Which specific exchanges will carry GTU tokens has yet to be determined, and of course there is no guarantee that exchanges will agree to carry GTU, or that GTU holders will recognize any return from exchange trading.

## CREATION OF GTU

A number of GTUs will be pre-baked, meaning that the initial or genesis block of the Concordium Network will allocate GTs to the accounts of early purchasers, the foundation or other organizations that received a promise of GTUs from the foundation prior to the launch of the network. After the network starts, new GTUs will be minted in form of rewards for different actions.

### BLOCK CREATION REWARD

The baker of each block will receive a reward for creating the block. The amount is dynamic and a network protocol will adjust this amount based on block creation speed—so if not enough bakers are writing blocks, the reward will grow. The reward is dynamically updated on each finalization block, and should always cover the actual computation costs for a baker to bake a block.

### FINALIZATION REWARD

If a network server is part of the Concordium finalization protocol mechanism, the server will receive a reward for finalizing blocks. Each successful finalization stamp will generate a set reward.

### IDENTITY ISSUER TRANSACTION REWARD

Each account on the Concordium blockchain will be required to have valid credentials generated from an identity object that was issued by a Trusted Identity Issuer. If an account does not have such credentials, it is not a valid account (meaning that transactions from/to that account will be impossible). A percentage of transaction fees will be given to the Identity Issuers that provided the credentials for transacting accounts.

## TOKEN ISSUANCE

The initial version of the Concordium Network protocol does not define a cap on token supply. The token supply is expected to grow between 2% and 6% each year, and it is envisioned that adoption of the technology will grow at a higher rate than the ongoing issuance of tokens.

We are researching principles for creating a sort of algorithmic "central bank" function that enables token issuance to become higher to keep the coin stable when demand is growing too fast, or lower if demand slows.

# ROADMAP: CONCORDIUM PROJECT PLAN

The Concordium Foundation's launch strategy has been carefully designed to create positive momentum and rapid growth. Our core plan is based on four components—software functionality, developer affinity, quality of cryptography and business orientation—which fuse to give life to an ecosystem with the power and pervasiveness to generate the market penetration we aim for.

## MARKETING INTELLIGENCE

Why guess what the market wants when it is more than ready to tell you? The Concordium Network's key features—the identity layer, ability to support ID/KYC regulation, account flexibility and smart contract flexibility are based on what businesses and public sector users have asked for, and we are currently setting up work groups to focus on industry-specific blockchain needs and to understand in greater depth, and share with our developer base, where the technology can make a difference. We want to get the dialogue and experimentation flowing. We want to make it easy to try out things and, ultimately, work with industry to create ongoing use cases that showcase Concordium's cost-effective transaction logging, and help us grow the presence of the network.

## SCIENCE-BASED DEVELOPMENT

Building a global backbone for transaction logging that is fast, secure, robust and scalable requires rock solid foundations. The Concordium Network—whether considering our ID-layer, privacy management, consensus protocol or finalization layer—is built on cutting-edge cryptography delivered by a world-class science team. Our science and development teams have been putting together the following technical white papers that will published alongside our beta launch.

**8 TECHNICAL WHITE PAPERS**

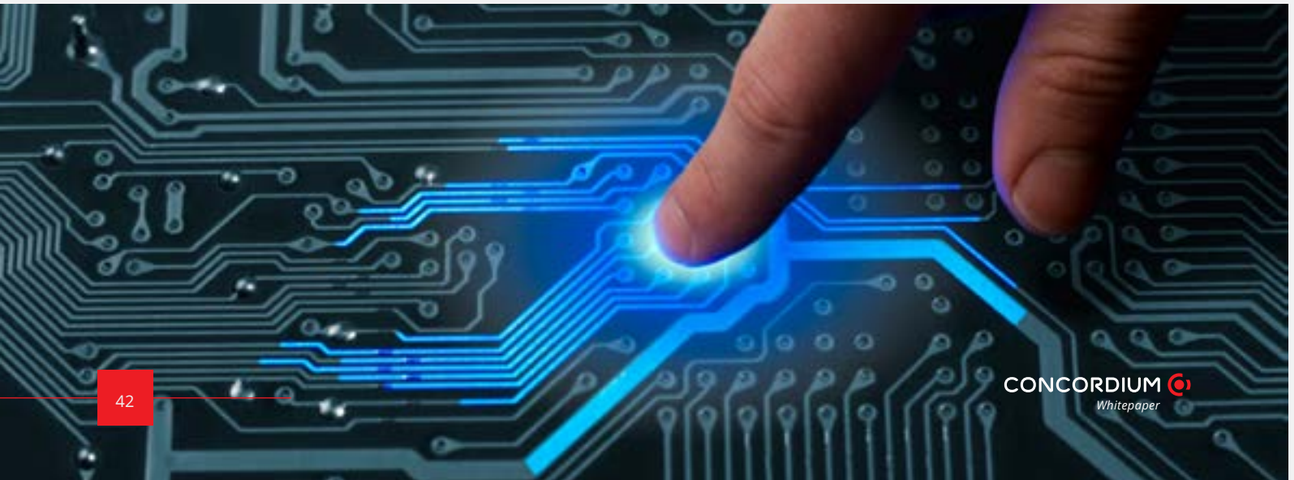
- **P2P Protocol.** Describes the format of all packets on the network, including their behavior and policies.
- **Consensus Protocol.** Mathematical description of our consensus protocol.
- **ID-layer Primitives.** Mathematical description of the cryptography used for our identity layer.
- **Privacy Primitives.** Mathematical description of the zero-proof cryptography used for privacy-design.
- **Oak Formal Semantics.** Specification of Oak nomenclature and description of Oak-compiler behavior.
- **ID-layer Protocol.** Description of ID/KYC layer functionality with blacklists, expirations, rules for revoking, format of all parameters, etc.
- **Blockchain Protocol.** Description of transaction types, binary formats, rules-of-the-game, policies, fees, rewards, stake-calculations, etc.
- **Smart Contracts Protocol.** Description of smart-contracts engine, contracts-as-pure-functions, contract functions, signatures and the Concordium Actor Model (rules for message-passing, parallel execution and resource analysis.)

## BUILDING A DEVELOPER BASE

Many thousands of programmers are already able to use Oak, Concordium's smart contract language, through their knowledge of Elm and Haskell. As the Concordium Network gets off the ground we intend to build integration kits and APIs that make it easier for developers to integrate existing software solutions with Concordium transaction logging. Today, most smart contract developers develop for the Ethereum network. We hope to show them that Concordium offers more functionality, more ease-of-programming and more ready-to-use components. An important part of this effort will be the creation of a full-scale professional developer support program that includes courses, events, help desk support, package libraries, a software developers' kit (SDK), conferences, meetups, bulletin boards and stack-overflow curated QAs. We even aim to deliver a wide range of "ready-to-use" contracts that save developers time and allow them to achieve solid results fast.

## DESIGNED-IN EASE OF USE

The lack of standards for user interfaces for clients, wallets and smart contracts has made blockchains difficult to use. That's why we're building the Concordium Design Kit—a complete UX/design manual with an integrated "approved by Concordium" component to help ensure a consistent look and feel across network applications. We also intend to create a multicurrency wallet capable of storing not just Concordium GTU tokens but also many other kinds of cryptocurrencies and tokens. As the Concordium Network progresses we intend to create and host a marketplace for Concordium smart contracts, apps, ideas and resources. We intend, over time, to grow this into a comprehensive go-to resource for everything Concordium—a place to find anything from events and courses to smart contract templates, Concordium developers or bidders for new Concordium projects.





## CONCORDIUM PROJECT TIMELINE

### CURRENT: PLANNING AND PROOF OF CONCEPT

- Researched market needs and sketched out the required solution
- Assembled a world-class team of scientists, developers, marketeers, business developers and advisors
- Created cryptography and rails for our network, described in white papers to be published with our proof-of-concept
- Currently writing P2P-network (done), consensus protocol, finalization protocol, Oak language, wallet, client and smart contract protocols

### JULY 2019: PUBLIC BETA FOR DEVELOPERS

- Test network running including P2P, consensus protocol, finalization protocol
- Key network server and developer tools
- Identity layer
- Installable and fully functional network server
- Oak language, including formal semantics
- Smart contract engine including code library repository
- Wallet with plug-in system
- Software IDE (integrated Oak development environment)
- QA department and developer support help desk up and running
- Network tweaking station (network optimization solution)

### JANUARY 2020: RELEASE CANDIDATE 1

- Onboarding and identity issuance availability
- Installable network server availability for Linux, MacOS and Windows
- Fully operating and stable running network
- Smart contract engine, libraries, packages and templates
- Formal verification framework for smart contracts
- Resource analysis for pre-calculation of gas

### SHARED FRAMEWORK INVITATION

The Concordium Network intends to invite newer science-based blockchain networks—such as Cardano, Tezos, Zilliqa, Rchain, Dfinity and Algorand—to develop common standards for software verification. We propose setting up a shared Blockchain Engineering Task Force (BETF) that will work to create shared standards, starting with formal verification practices, exactly like the IETF (Internet Engineering Task Force) has done for the internet with standards such as HTML, DNS, IP, CSS, Java-script, MIME, URLs, RSS and XML.

*Please note that legal and regulatory review may impact our project timeline.

# THE CONCORDIUM ORGANIZATION

How do you best organize yourself if you want to build something that can have global impact? From the outset it has been pretty clear to the founders of Concordium that succeeding means succeeding in every arena: science, development, marketing and business development. And we realize that to build and launch a pervasive and ubiquitous blockchain network capable of gaining rapid adoption by both businesses and the public sector requires outstanding management skills, a very solid grip on recruitment and human resources as well as demonstrable heavy-duty organizational skills.

The Concordium project and the Concordium Foundation differs from many other projects in bringing together solid domain expertise in management, human resources, marketing, development and science from the outset. Our founders are successful business people, world class cryptographers and extremely skilled software developers.

**CONCORDIUM AG ZURICH**
- Science review and liaison
- Protocol implementation
- Use Case Group
- Security Proofs
- Group HQ

**CONCORDIUM FOUNDATION ZUG**
- Project Management
- Partnership Development
- Financials

**ETH ZURICH**
- Science Review Team
- Science Advisor
- Science Liaison Office
- Security proof Methodologies

**CONCORDIUM SA MARBELLA**
- Network Server Design
- PSP Transport Layer
- Infrastructure Design
- Internal IT

**CONCORDIUM LTD LONDON**
- Oak-development
- Wallet Development
- Project Management
- Marketing

**CONCORDIUM AARHUS**
- Cryptography
- Privacy Design
- Network Protocols
- Concordium Labs

**AARHUS UNIVERSITY**
- Key Science Team: Focus on cryptography, privacy design and formal verification

**CONCORDIUM DEVELOPER PROGRAM, LONDON**
- Developer Program
- Developer Support
- Smart Contract App Store

**CONCORDIUM USE CASE LABS, LONDON**
- Bespoke smart-contract design and coding for specific use cases

**CONCORDIUM STANDARDS AND VERIFICATION, AARHUS**
- Formal Verification Team: Develop shared standards for key blockchain functionality

**CONCORDIUM BLOCKCHAIN RESEARCH LABS, AARHUS**
- In cooperation with Aarhus University. Focusing on protocol level cryptography, zero-knowledge proofs and multiparty computation on blockchains

# THE CONCORDIUM FOUNDATION

The thrust of setting up the Concordium Network will be run through a nonprofit Swiss foundation with a mission statement that directs it to work in the best interests of the network. The generated code—and with it the actual Concordium Network—will become open source and be available in the public domain. The Concordium Network will belong to its users and the Concordium Foundation will not own it, although the Concordium Foundation will retain ownership of trademarks and intellectual property generated for or purchased by the foundation.

The Concordium Foundation is managed by a board of directors that are designated by the chairman of the Concordium Foundation. The sole interest of the board of directors as well as of the chairman in regard to the Concordium Foundation is to stimulate the growth and adaptation of the Concordium Network as a global backbone for transaction logging.

The first batch of Concordium GTUs created by the Genesis Block will initially be owned by the Concordium Foundation and the foundation will deliver agreed portions of these GTUs to early purchasers, key personnel, advisory board members, etc. The remaining amount of GTUs will be placed in the Concordium Foundation's treasury and as per the Foundation's mission statement used to further enhance and develop the Concordium Network.

As the Concordium Network becomes operable, network servers, baking nodes, etc. will be eligible for GTU rewards and these will be created algorithmically, as described in this document, at a rate that we believe will be between 2% and 6% per year of the initial creation of GTUtokens.

When the Concordium Network's transaction numbers begin to grow, users of the network will need GTU tokens to transact. We believe this will increase the demand for GTU tokens.

Funding of the Concordium Foundation and of the work carried out to date has been undertaken by the Concordium Founders.

## CONCORDIUM AG

While the Concordium Foundation defines the functional and technical requirements of the Concordium Network the actual development and programming effort will be undertaken by Concordium AG—a commercial software development company created by the Concordium founding team and operating under contract with the Concordium Foundation to deliver the Concordium Network as specified. Concordium AG is paid by the Concordium Foundation for this service at fair market value. Concordium AG currently has office presence in London, Zurich, Marbella and Aarhus. Headcount in Concordium AG is expected to increase to around 40 people for the initial release candidate of the Concordium Network, with time split between developing P2P network, consensus protocol, network server, implementing cryptography, designing the Oak programming language and implementing our smart contract framework, wallet, server application and setting up our DevOps environment.

Software development in Concordium AG is based on Agile/Scrum Epic development, meaning that a large body of work like the Concordium Network can be broken down into a number of smaller "stories" and "initiatives" that are delivered via a set of sprints. These involve extensive use of product roadmaps, action plans, huddles, storytelling, reporting frameworks and shared views allowing teams to focus on the task at hand, yet still interact across the floor to assemble the code and deliver epics.

Project managers work with software development teams to coordinate journeys leading to on-time delivery of in-scope components and ultimately a complete network, which is on time and on brief. Simultaneously, our managers ensure a consistently high standard of code documentation, which over time leads to much quicker reiterations and rebuilds as new features are added.

Key programming languages currently used in Concordium Network development by Concordium AG are Rust, C, C++, Haskell, Ocaml, F*, COQ/Gallina, Scala and Elm. We are looking to hire additional development resources with skills in these languages.

## THE CONCORDIUM SCIENCE TEAM

Building a global backbone for transaction logging that is fast, secure, robust and scalable requires rock solid foundations. The Concordium Network—whether considering our ID-layer, privacy management, consensus protocol or finalization layer—is built on cutting-edge cryptography delivered by a world-class science team that includes some key players in the space.

Our science team contracts directly with the Concordium Foundation—either individually or through their respective universities where we contribute funding to set up postdoctoral fellows to work on our science packages.

Our current science partners hail from Aarhus University (cryptography, consensus mechanism design, zero-knowledge proofs and formal verification design) and ETH Zurich (verification and science package reviews). Our current science team consists of 13 people and we expect this number to grow around 40 as we move towards the launch of release 1 of the Concordium Network.

Our Chief Science Advisor, Ueli Maurer, is a professor of computer science and head of the Information Security and Cryptography Research Group at the Swiss Federal Institute of Technology (ETH), Zurich. He is also a board member of the Concordium Foundation.

## MAKING THE WORLD EMBRACE CONCORDIUM

The Concordium Foundation's marketing strategy is extremely simple—we aim to build quality software that matches business needs, make sure developers understand the power we can put into their hands, make sure businesses understand how they can harness this power to create new efficiencies and introduce stepped-up levels of security, and tell the world about what we are doing—on our own website, on YouTube, at conferences, trade fairs, universities and conventions.

We believe that the many new ideas we are about to launch into blockchain space—from programmable accounts and hyper-transactions to privacy cloaking and pre-execution gas calculations—will all write their own headlines.

As we move forward, interested users, businesses, developers and the general public will be able to follow us on Telegram, Slack, Twitter, Reddit, Github and Gitter as well as on our own website and blog. Weekly mailers with news and updates—including all matters in the blockchain business space—will be sent to interested subscribers and we will offer monthly briefings to key partners, investors and potential investors, too.

## WHERE THE ROAD AHEAD MIGHT LEAD US

Creating the Concordium Network is a big and audacious idea—big enough to change the world if we succeed to the extent we hope and believe we can. We believe that our initial team has the experience, the skills and the pedigree to step up to the challenge and deliver what we have planned and explained in this document.

We also realize that this will be a long journey and that success hinges not just on the team we have today but on our ability to attract and integrate the best resources available into every function of the Concordium project.

Likewise, we understand that to succeed we need to keep moving and to set our aims at goals that are extremely ambitious. In essence, we intend to create the best platform of its kind with the power and functionality to operate and log transactions at a global level—and to base our every effort on creating a network that is rock solid, unbreakable and reliable to the extent where it can gain the trust of the world—for logging transactions, settlements, finalization and much more.

And while the mission statement of the Concordium Foundation mandates a sharp focus on developing the best possible solutions for the Concordium Network—and for launching this network into the world—we also realize that to continue evolving the network and to remain at the forefront of decentralized network development it is crucial that the Concordium Foundations science team engagement does not stop with the development of our current planned network but, in fact, carries on into the future by providing research into numerous new areas of applications that can be run on the Concordium Network.

At the same time we are entirely cognizant of the fact that in science, competition and cooperation go hand in hand—and while we intend to make every effort to see the Concordium project succeed we realize that a crucial part of that effort will be reaching out to other projects to build bridges, define interoperability and agree common standards aimed at delivering consumer choice in a setting that enables shared growth in this crucial area of endeavor.

## TEAM AND ADVISORY BOARD

When we began constructing this project in January 2018 we quickly realized that success would hinge on the quality and pedigree of the team we assembled. An undertaking of such global scope requires high-powered minds with the experience, vision and tenacity to deliver—but not just that. We needed a team capable of unifying science, development expertise and business savvy, amalgamating them into a single, solid product. That is the only way to deliver a project of this magnitude.

We have assembled a core team of scientists to build the cryptography, lead software engineers to run the development effort and key business experts to sit in and ensure that our solution is not just smart and secure but also practical and easy to use, and an advisory board with a global pedigree of the highest caliber.

Please note that the list of resources presented here includes only our C-level personnel and key science team members. We have not included our full roster of currently employed programmers, project managers, etc.

Our discussions have been unfolding over many months through research, test beds, science reviews and more research. We have continued to recruit, constantly on the lookout for the best and brightest to fill the gaps in our rapidly growing team. Our early prelaunch token offering will provide the resources to augment our already imposing staff portfolio with more programmers and scientists whom we have already identified.

# CONCORDIUM: CORE SCIENCE TEAM

## PROFESSOR UELI MAURER

ETH ZURICH, SCIENCE ADVISOR AND CONCORDIUM BOARD MEMBER

Ueli Maurer is professor of computer science and head of the Information Security and Cryptography Research Group at the Swiss Federal Institute of Technology (ETH), Zurich. His research interests include theory and applications of cryptography, information security, theoretical computer science, information theory, and discrete mathematics. One of his long-term research goals is to establish a constructive theory of cryptography and to apply it to the modular design of provably secure cryptographic protocols, especially in the blockchain space.

Professor Maurer is known for his work on information-theoretic cryptography, the security analyses of the Diffie-Hellman protocol and the RSA system, the invention of the indifferentiability concept, his extended work on secure multiparty computation, a universal randomness test, and more. He has served as editor-in-chief of the Journal of Cryptology from 2002 to 2010 and as associate editor for the IEEE Transactions on Information Theory and for the Journal of Computer and System Sciences. He is an IEEE Fellow, an ACM Fellow, an IACR Fellow, and a member of the German Academy of Sciences (Leopoldina).

Maurer was the 2000 Rademacher Lecturer of the Department of Mathematics at the University of Pennsylvania and received the 2013 Vodafone Innovation Award for Mobile Communications, the 2016 RSA Award for Excellence in the Field of Mathematics, and the 2016 Theory of Cryptography (TCC) Test-of-Time Award.

He has served many companies and Swiss government bodies as consultant, both at the management and the technical level. The list of customers includes many of the large Swiss financial institutions. He has also served many companies as board member, including Tamedia, a leading Swiss media company where he served on the audit committee from 2002 to 2008. He co-founded the security start-up Visonys, which was sold to Phion in 2008 and he is a member of the scientific advisory board of PwC Switzerland.

## PROFESSOR IVAN DAMGÅRD

AARHUS UNIVERSITY, CRYPTOGRAPHY LEAD

Professor Ivan Damgård holds a PhD in Computer Science from Aarhus University (1988). He is one of the top cited and published researchers in cryptography, fellow of the IACR and received the 2015 RSA Award for Excellence in the Field of Mathematics. He has managed numerous research projects and holds an advanced ERC grant. As is well known to the blockchain community at large, Professor Damgård is a co-inventor of the Merkle–Damgård-construction, which is the principal cryptographic hash function that every blockchain in existence relies upon in some form or another.

He is a co-founder of Cryptomatic, a software and consultancy company in secure e-business as well as of the companies Partisia, Sepior and Secata. In 2017 Damgård was awarded the Villum Kann Rasmussen Annual Science and Technology Award, the most prestigious science award in Denmark.

## PROFESSOR JESPER BUUS NIELSEN

AARHUS UNIVERSITY, CHIEF SCIENTIFIC ADVISOR, CONSENSUS PROTOCOL

Professor of Computer Science at Aarhus University and the author of more than 70 scientific publications, Professor Jesper Buus Nielsen holds a PhD in Computer Science from Aarhus University (2003) and has also worked at ETH Zürich as senior researcher. He is a leading expert on secure multiparty computation and has been a program committee chair for both the Theory of Cryptography Conference and the Eurocrypt Conference.

Professor Nielsen has managed a number of research projects and held an ERC Starting Grant. He is a co-founder of the Insight Network and a co-founder of the cryptography companies Partisia, Sepior and Secata. He is a co-author (with Ivan Damgård and Ronald Cramer) of Secure Multiparty Computation and Secret Sharing, a seminal work on privacy in distributed computing environments.

## ASSOCIATE PROFESSOR BAS SPITTERS

AARHUS UNIVERSITY,
CHIEF SCIENTIFIC ADVISOR,
FORMAL VERIFICATION

Professor Bas Spitters heads our formal verification team. Formal verification is a technique to prove, with mathematical certainty, that software meets its formal specification, thus making sure it behaves as desired. It is the highest level of software quality.

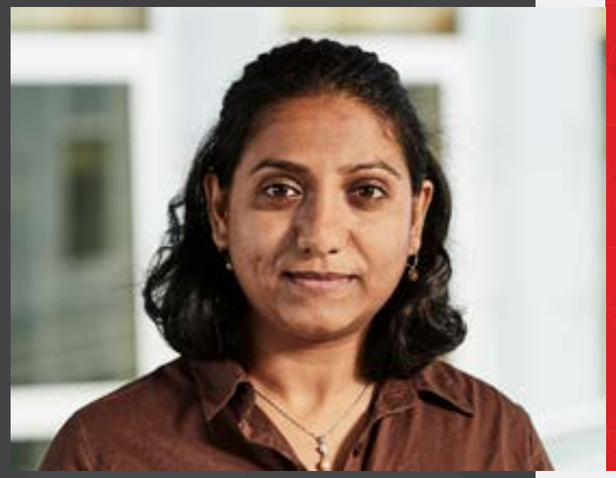
Spitters, who holds a PhD in mathematics from Nijmegen University (2003), has received an elite Veni grant by Dutch NWO and was recently awarded a US Air served as work package leader of an EU project to make the formalization of mathematics feasible at scale, and has written close to 40 refereed publications. A leading researcher on type theory, categorical logic and computer-aided proofs, Bas Spitters has held positions in Nijmegen, Chalmers, Paris-Sud, CMU and was a member of the Institute for Advanced Study in Princeton. He has been a member of 26 program committees.

## ASSOCIATE PROFESSOR CLAUDIO ORLANDI

AARHUS UNIVERSITY,
SCIENTIFIC ADVISOR,
CRYPTOGRAPHIC PROTOCOL DESIGN

Professor Claudio Orlandi holds a PhD in Computer Science from Aarhus University and heads our cryptographic protocol team. He is the author of more than 30 scientific publications in cryptography and security, and a leading researcher on secure multiparty computation and zero-knowledge protocols. He has managed a number of national and international research projects, and has served as chair of CryptoAction, a European network for research in cryptography (2014-2018). Claudio Orlandi has received a prestigious Danish DFF Starting Grant (2016) and an ERC Starting Grant (2018). He has also worked as a postdoctoral fellow at Bar-Ilan University, Israel.



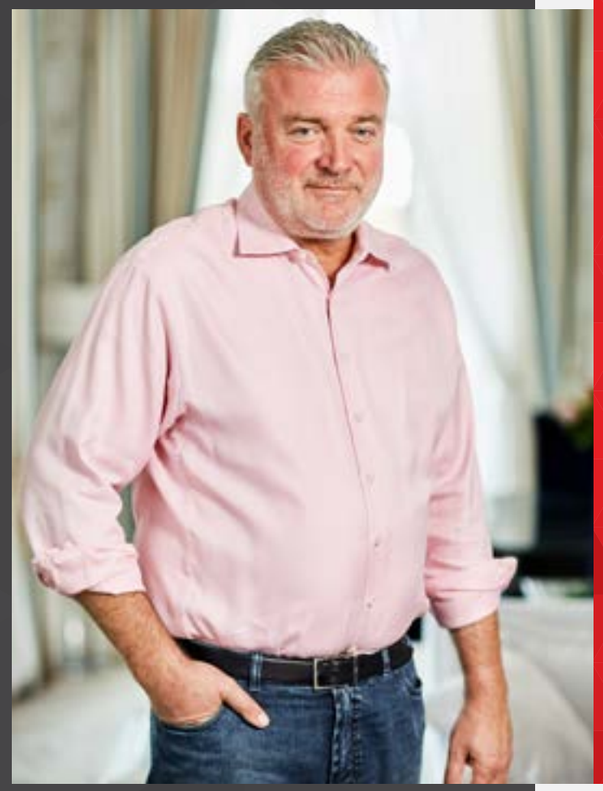


## CHAYA GANESH, PHD

AARHUS UNIVERSITY,
SCIENTIFIC ADVISOR,
ZERO KNOWLEDGE PROOFS AND PRIVACY DESIGN

Chaya Ganesh is a postdoctoral fellow at Aarhus University. She received her PhD from New York University under the supervision of Professor Yevgeniy Dodis. Her research is in cryptography and she is particularly interested in secure computation and zero-knowledge protocols. Chaya Ganesh was awarded the Henry MacCracken Fellowship by NYU during her doctoral studies. She also has experience with research in the industry and has completed internships at Microsoft Research, Bell Labs, and Visa Research. She has published several research papers in top conferences, and has served on the program committees of CANS and SEC.

# CONCORDIUM: CORE EXECUTIVE TEAM



## LARS SEIER CHRISTENSEN

### CONCORDIUM FOUNDATION CHAIRMAN

Lars Seier Christensen co-founded Saxo Bank, a pioneer in FX and derivatives trading, in 1992. He served as co-CEO of the bank for more than 20 years before stepping down in 2016 to focus on other investments. During his years at Saxo, the bank grew to 1500 employees, spread across more than 20 locations around the world. SaxoTrader, the bank's flagship online trading offering was first launched in 1998 as one of the first online FX trading platforms ever. Since then SaxoTrader has grown to become one of the world's most complete multi-asset platforms. Mr. Christensen experienced first-hand the major regulatory changes transforming derivative trading services to private clients and smaller institutions, and this practical experience is incredibly valuable for understanding the regulatory roadmap ahead for cryptocurrencies and financial blockchain applications.

Mr. Christensen took an early interest in the area of blockchains and cryptocurrencies and he holds strong views about the need to firmly integrate full compliance in foundational blockchains. He considers this a fundamental requirement to enable mainstream business adoption, while at the same time advocating staying true to the blockchain DNA of distributed consensus and avoiding the many single points of failure that has destabilized the established financial system throughout history.

Mr. Christensen's business acumen and skills, with regards to streamlining and mainstreaming the Concordium offering, is at the heart of the project's broad appeal to multiple business and public sector applications. Prior to founding Saxo Bank, he spent several years in the financial sector in London in various trading and advisory capacities. Through his personal investment company, Seier Capital, he has invested in many early stage companies, particularly in the areas of technology and lifestyle.

## MATEUSZ TILEWSKI

### CHIEF TECHNOLOGY OFFICER

Mateusz Tilewski began programmin g at 8 years old and started his first software consultancy boutique at 16. Today, at 39, he is a successful entrepreneur with several exits behind him. An engineering student from the University of Aalborg, Mr. Tilewski has set up and run software development teams for the past 20 years. He has been involved in a variety of projects in different industries, from creating and selling financial software to Willis corporation in 2009, running his own mobile phone company, Flexphone, and working extensively in the InfoSec industry.

Mr. Tilewski has been involved in blockchain from the very beginning and created what was probably the world's first Bitcoin payment gateway as well as the world's first on-chain voting system. Extensive experience in software architecture and development has made Mr. Tilewski a much sought-after senior software consultant. He has been helping several major corporations structure and execute Big Data, AI and blockchain projects over the last five years.

## SOREN KENNER

### CHIEF MARKETING OFFICER

Soren Kenner co-founded Medialog, a pioneer in integrated marketing, in 1994. He sold the company to McCann Erickson MRM (NYSE:IPG) in 1997 in what remains the largest agency deal in Scandinavia to this day. Following the sale, Mr. Kenner became Chairman of McCann Erickson MRM EMEA with responsibility for more than 1500 European employees.

During his tenure as chairman, he serviced a wide range of global accounts including Coca-Cola, Mastercard, L'Oreal, Nestlé, Motorola and Lucent. After leaving McCann in 2002, Mr. Kenner turned his attention to the startup community and, over the next few years founded, co-founded and invested in a number of companies including Hello Group, which grew to become one of Scandinavia's largest advertising agencies; and Zecco, an online trading company, which was sold to Ally Financial for US$275 million in 2016.

Mr. Kenner is widely recognized as an expert in online marketing and community building with a proven track record of delivering rapid and successful market entry and boosting for the companies he works with—a skill set crucial to Concordium's outreach to community members, partners and allies in the blockchain and cryptocurrency arena.

## BJORN KROG ANDERSEN

CHIEF LEGAL ADVISOR

Bjorn Krog Andersen is a partner of the law firm Moalem Weitemeyer Bendtsen in Copenhagen, Denmark. Mr. Andersen has extensive regulatory and compliance experience and advises fintech, regtech and blockchain companies in his practice, in addition to doing both VC and PE-related M&A work. Mr. Andersen was General Counsel of Saxo Bank Group for six years, heading its legal, regulatory and compliance departments globally. This experience provides Mr. Andersen with a deep understanding and insight into regulatory concerns and worldwide obligations within ID/KYC and investor protection-related topics. Mr. Andersen serves as chief legal advisor to Concordium and coordinates all legal and regulatory issues with its outside advisors.

## DANIEL TSCHUDI

PHD, SCIENCE LIAISON OFFICER

Daniel Tschudi is a postdoctoral fellow at Aarhus University. Mr. Tschudi holds Bachelor and Master's degrees, both in Mathematics, from ETH Zurich. He did his PhD in Computer Science at ETH Zurich under the supervision of Professor Ueli Maurer. His research has been in cryptography with a focus on secure computation protocols. He maintains research interest in cryptocurrencies and anonymous communication. He has published several research papers in leading IACR conferences and distributed computing flagship venues. Mr. Tschudi has rich experience in teaching and mentoring and has served as an external reviewer for top tier conferences. He is a co-author on many recent influential papers on the formal treatment of Bitcoin's ledger and rational analysis of the Bitcoin protocol.

## CONOR RINGLAND

CHIEF OPERATING OFFICER

Conor Ringland has worked in capital and financial markets in London for over 30 years, spending 12 years in the futures and FX markets as an analyst managing traders, working through the open outcry era into the digital era across all asset classes. He spent seven years at E*TRADE building their derivatives platform and B2B business, following which he joined Saxo Bank to head up their UK commercial proposition that focused on digital platform strategies to key accounts such as CITI, Barclays and TD Waterhouse. After eight successful years at Saxo, Mr. Ringland joined Lloyds Commercial Bank to head up their Financial Markets digital proposition across their credit rates and FX businesses. More recently he was the CEO at an FCA registered broker, and also involved in developing fintech and regtech businesses. Mr. Ringland is passionate about how digital markets will challenge and optimise themselves to offer access, transparency and value to all users globally.

## JØRGEN HAUGLUND

CHIEF FINANCIAL OFFICER

Mr. Hauglund has extensive experience in the fields of financial planning, accounting, budgeting, controlling and reporting from positions in a number of large Danish corporations, including Saxo Bank, ISS, Sydbank, A.P. Moller–Maersk and the East Asiatic Company. He has worked for a number of years as a consultant focusing on financial management, shareholder value concepts and corporate documentation/compliance. In addition, Mr. Hauglund has held senior management positions in investment companies focusing on shipping and real estate transactions. He holds a Master of Science in Economics and a Business Administration degree from the Copenhagen Business School and an Executive MBA from the same institution.

# CONCORDIUM: ADVISORY BOARD

## ANDERS FOGH RASMUSSEN

FORMER SECRETARY GENERAL OF NATO

Anders Fogh Rasmussen served three terms as Prime Minister of Denmark from 2001 to 2009 after which he served five years as Secretary General of NATO. As prime minister of Denmark, Mr. Rasmussen was at the helm of a long period of continued growth and prosperity. In 2002, taking over the rotating presidency of the EU, Mr. Rasmussen headed the negotiations for expanding the EU eastward, leading to the EU membership of 10 new member states including Poland, the Baltic nations, Malta and Cyprus in 2004.

After stepping down as Secretary General for NATO in 2014, Mr. Rasmussen founded Rasmussen Global, a political consultancy dedicated to issues regarding democracy, security policy, the EU and economic development. In 2017, Mr. Rasmussen founded the Alliance of Democracies, a nonprofit organization dedicated to the advancement of democracy and free markets across the globe. He is also a senior advisor at Boston Consulting Group.

## LONE FØNSS SCHRØDER

VICE-CHAIR VOLVO, IKEA AND AKER BOARDS AND FINTECH EXPERT

Mrs Fønss today serves as Vice Chairman of the board of Volvo Cars, is a board member of Ingka (IKEA GROUP) and Aker Group and is the co-founder of the Bank Fin-tech Cashworks. She also served as a senior advisor to Credit Suisse. She was a Senior Vice President at AP Møller Mærsk, one of Denmarks largest conglomerates and have previously served on the boards of Saxo Bank, Valmet, Handelsbanken, Vattenfall, YARA and WWL. She has extensive banking and auditing experience and substantial capital markets experience from a large number of IPO's, delistings and bond issues. Mrs. Schrøder has significant board experience from financial institutions, fintech, transportation, energy, shipping, aviation, production and the automotive sector. She brings a razor sharp business focus and an unparalleled business network to the Concordium Advisory Board. "

## HANS-OLE JOCHUMSEN

FORMER VICE CHAIRMAN OF NASDAQ

Hans-Ole Jochumsen has served as president of global trading and market services at Nasdaq from 2008 to 2017, where he became vice chairman. In his role as president, he oversaw cash and derivatives within the area of equities, fixed income, commodities and currency trading.

Mr. Jochumsen has played a major role in Nasdaq acquisitions including the US$400 million purchase of Chi-X Canada and the US$1.1 billion deal for International Securities in 2016. From 2010–2013 he served as president of the Federation of European Securities Exchanges. As an advisor to Concordium, Mr. Jochumsen delivers an unparalleled understanding of regulatory issues relating to exchanges and trading.

## LARS CHRISTENSEN

MONETARY ECONOMIST

Lars Christensen is an internationally renowned Danish economist specializing in international economy, emerging markets and monetary policy. He accumulated more than 20 years' experience in the public sector and banking before founding his own consultancy, Markets and Money Advisory, which helps governments around the world craft economic policies. Mr. Christensen made his name with a series of groundbreaking analyses as the head of emerging markets research at Danske Bank in Copenhagen. In 2006–2008, he warned of an impending economic downturn in Central and Eastern Europe.

Mr. Christensen is a senior fellow at the Adam Smith Institute in London, sits on the advisory boards of the Maghreb Economic Forum in Tunisia and Swicorp. He is a regular contributor to the Danish business daily Børsen and Geopolitical Intelligence Services. The world's main financial media seek out Mr. Christensen for quotes and commentary which can be found in the Financial Times, The Telegraph, Bloomberg News, Thomson Reuters and Dow Jones Newswires, among others.

## STEEN JAKOBSEN

CHIEF INVESTMENT OFFICER, SAXO BANK

Steen Jakobsen has more than 25 years of experience within the fields of proprietary trading and alternative investment. After finishing his studies in Economics at Copenhagen University in 1989, he started his career at Citibank N.A. Copenhagen from where he moved to Hafnia Merchant Bank as Director, Head of Sales and Options. In 1992, he joined Chase Manhattan in London as VP, Head of Scandinavian Sales, and then the Chase Manhattan Proprietary Trading Group. From 1995–1997 he worked as a proprietary trader and Head of Flow Desk at Swiss Bank Corp., London. In 1997, he became Global Head of Trading, FX and Options at Christiania (now Nordea) in New York until he joined UBS in New York in 1999 as the Executive Director in the Global Proprietary Group. He joined Saxo Bank in 2000 and after a brief departure to Limus Capital Partners, where he was Chief Investment Officer for two years, he returned to the bank in 2011 as Chief Investment Officer.

## CLAUS NIELSEN

FORMER HEAD OF MARKETS, SAXO BANK

Claus Nielsen served as Head of Markets for Saxo Bank for 15 years from 2003 to 2018. He was responsible for all global trading and execution-related activities (including product development) run out of Saxo Bank's headquarters in Copenhagen as well as the Singapore office. He was also responsible for Risk Management, Saxo Prime (API), Sales Trading and SaxoStrats (research and analysis), Markets services +35,000 OTC and listed instruments via a wide range of banks and trading venues. Prior to Saxo Bank he worked in various trading positions in FX Spot, Options and Futures and also worked in Research and Sales at Handelsbanken and at Jyske Bank.

# HOW TO CONTACT US

## THE CONCORDIUM FOUNDATION


**Attn: Lars Seier Christensen,**
CHAIRMAN

lsc@concordium.com

Concordium Foundation
Zugerstrasse 32
Postfach 1350
6341 Baar/Zug
**Switzerland**


## CONCORDIUM AG SOFTWARE DEVELOPMENT


Concordium AG
Löwenstrasse 29
8001 Zurich
**Switzerland**




## TECHNICAL INQUIRIES


Mateusz Tilewski, CTO
mt@concordium.com


## PR AND MARKETING CONTACT


Soren Kenner, CMO
sk@concordium.com


## HIRING AND HR


Conor Ringland, COO
cr@concordium.com


## SCIENCE AND RESEARCH DEPT


Ueli Maurer, CSA
um@concordium.com


## FINANCIAL INFORMATION


Jørgen Hauglund, CFO
jh@concordium.com


## OFFICE ADDRESSES


Concordium ApS
Aabogade 15
8200 Aarhus N
**Denmark**

Concordium Spain SL
Avenida puerta del mar 15
29680 Estepona
**Spain**

Concordium Tech UK Ltd
8 Devonshire Square
London EC2M 4PL
**United Kingdom**

# KEEPING TRACK OF THE WORLD'S TRANSACTIONS

CONCORDIUM