EMOTIQ

Scalable Private Natural

Whitepaper v0.1

Contents

Preface

More than any technology that preceded it – even the Internet – the blockchain has the power to disrupt institutions, democratize business relationships, and create trust where no trust exists. The blockchain, as an inviolable, immutable data ledger, is both a reincarnation of the Internet's founding principles and a significant next step in its evolution.

In pursuit of practical applications, however, we have fallen short of practical solutions. Blockchain technology is not yet fully formed, and the defining innovations are still to come. What is certain is that, eventually, every industry will have either implemented blockchain technology or be irrevocably impacted by its existence.

We have a unique opportunity to define the blockchain, and provide an answer to its unresolved challenges of scalability, privacy, and accessibility. In this paper, we discuss each of these challenges and present Emotiq – a scalable, private, natural blockchain – as the solution.
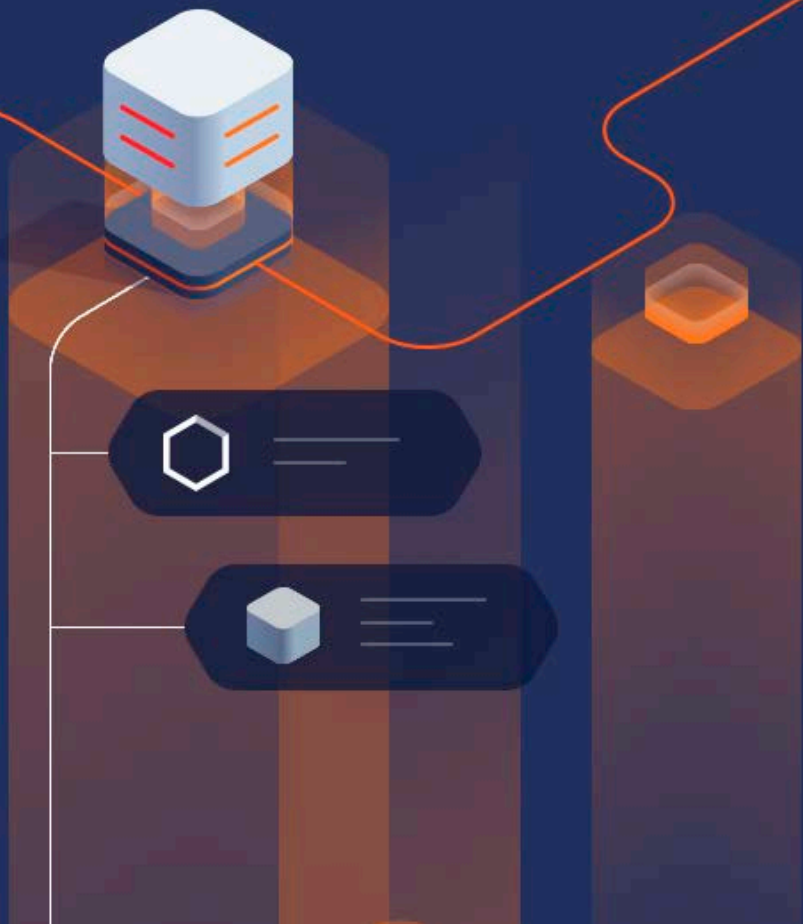
Introduction

Emotiq is a powerful, decentralized blockchain with Proof-of-Stake (PoS) consensus and natural language smart contracts. Emotiq is built on OmniLedger – a distributed ledger conceived by researchers at Switzerland's École Polytechnique Fédérale de Lausanne (EPFL) that provides horizontal scalability and VISA® and Mastercard®-level throughput, at thousands of transactions per second.

The Emotiq blockchain is designed to be scalable, private, and natural; the first through the OmniLedger horizontal scaling, or sharding; the second with non-interactive zero-knowledge proofs, ensuring transaction privacy; and the third with Ring – Emotiq's plain English smart contract language, enabling non-programmers to create smart contracts that are easy to think about and understand.

The Problem

Blockchain technology has three main challenges, for which we provide three solutions.

Scaling. Currently, Ethereum can handle 13 transactions per second (reduced to 7 transactions per second for tokens), which is orders of magnitude below that required for large-scale applications. Bitcoin, meanwhile, is capable of a diminutive 7 transactions per second. Though each is exploring their own scalability solutions, none are proven.

Privacy. A trustless environment and anonymity are similarly essential to the wider adoption and use of the blockchain. We have a natural desire to keep our finances and transactions private. Emotiq is inspired by Monero and ZeroCash to provide additional privacy solutions, for example, by keeping transaction amounts hidden.

Usability. Smart contracts are inaccessible for the majority of users. They're difficult to use, hard to read, and impossible to write without the risk of introducing new security holes (as shown by the widely publicized hacks of Ethereum). It is impossible to understand the behavior of current smart contracts without using a computer to evaluate them. Legal contracts, in contrast, can be easily read and understood.

There are two sets of people: those who program by trade and those who program by necessity. The first set is small and well-served by existing smart contract languages that are modeled on programming languages, e.g., JavaScript. The second set dwarfs the first, however, and requires a completely different approach, i.e., smart contracts that can be read and understood without the need of a computer to evaluate them. Emotiq targets this second group and delivers a truly scalable blockchain with privacy features and easy-to-create applications.

01

The Solution

Emotiq is:
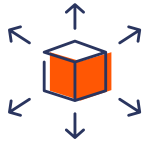
Scalable. Emotiq the first next generation blockchain to implement OmniLedger technology, a product of groundbreaking research in distributed consensus and decentralized computing. It features high transaction throughput and horizontal scaling via sharding. This is in contrast to vertical scaling, which relies upon increasing the computing resources of individual nodes in the network. Together with OmniLedger and the parallel processing of unspent transaction outputs (UTXO), Emotiq is able to process thousands of transactions per second, at low cost and with an ever-expanding network of nodes.

Private. The blockchain has created a new trust paradigm — immutable, impervious to tampering, and without reliance on third-party intermediaries. The ability to transact securely, however, should not come at the price of confidentiality. By integrating zero-knowledge proofs, Emotiq ensures that only relevant data is visible on the blockchain, while confidential data is kept private.

Natural. Scalability and privacy, while essential, are not the toughest challenges of the blockchain. Its accessibility and usefulness are. With Ring, Emotiq's natural language for smart contracts, non-programmers can easily create smart contracts to satisfy a wide range of agreements and applications and test them interactively. Ring compiles to a lower level Ring virtual machine (VM) which also runs most, if not all, smart contracts written in Ethereum Solidity. Ring is inspired by Zork — a classic interactive fiction computer game — and we intend Ring to be just as fun, exploratory, and open-ended.

Emotiq scales to VISA-level throughput. It features an innovative approach to smart contracts through Ring, Emotiq's natural, plain English smart contract language, as well as partial compatibility with Solidity to accommodate transitioning projects.

Emotiq will use its considerable expertise to pave a new path for blockchain technology, integrating research-backed technologies and actively tackling existing and future blockchain challenges. We, like many, are convinced the blockchain will change the world, and we're committed to providing the platform to make that happen.

Tech Overview

Emotiq Blockchain

Horizontal Scaling through Sharding

Blockchains are continuously growing. Vertical scaling, used by Bitcoin, is an unsustainable approach, as the hardware requirements to support larger and larger nodes are untenable. The logical way to scale the blockchain, therefore, is to scale horizontally. This is enabled through sharding.

Emotiq builds on top of OmniLedger and features horizontal scalability through sharding. OmniLedger is the first highly scalable distributed ledger that can preserve long-term security under permissionless operation, ensuring correctness across large, scalable networks of nodes.

Sharding is an innovative approach to load distribution in blockchains. It reduces the time taken to process transactions and increases processing capacity as the network expands — to a target of 5000 transactions per second. Only the nodes that contain the data required to process the transaction need to reach consensus on it, thereby decreasing transaction processing time. This additionally reduces network congestion, lowers transaction costs, and prevents gridlocks.

UTXO and Proof-of-Stake (PoS)

Emotiq also features UTXO, or unspent transaction outputs, and a Proof-of-Stake (PoS) system. PoS allows Emotiq to achieve a higher throughput over Proof-of-Work (PoW) systems, at significantly lower energy costs.

UTXO was first introduced by Bitcoin and, unlike Ethereum, aggregates spent and unspent coins into a single balance. Not only does UTXO offer simplicity, but also drastically increases Emotiq's scaling capability, by enabling transactions to be processed independently and in parallel.

Non-Interactive Zero-Knowledge Proofs

Zero-knowledge proofs are Emotiq's privacy pillar. Like Bitcoin, Emotiq uses UTXO. Unlike Bitcoin, however, Emotiq uses zero-knowledge proofs to ensure transaction amounts, among other things, are not visible in the public ledger.

For example, although blockchain addresses are represented by random strings, it is currently possible for mapping software to crawl Bitcoin's ledger for spent and unspent (UTXO) coins, to identify the transactions of a single private key and determine a holder's total wealth in Bitcoin.

While non-interactive zero-knowledge proofs do not prevent such transaction graph analyses, they prevent the tracing party from seeing the amounts being transferred.

Emotiq Platform

Natural Smart Contracts

Emotiq reimagines the role of smart contracts. Smart contracts are computer programs that detail the conditions under which a transaction or transfer of tokens will occur, and executes them accordingly. They are the user interface of the blockchain. These computers programs are only readable by computers, however, not humans. On Ethereum, for example, a developer with expertise in Solidity is required to write a smart contract, and even an exceptionally skilled developer may make fatal security mistakes doing so.

This paradigm limits the usefulness of smart contracts and imposes a ceiling on their accessibility. Through Ring, the Emotiq smart contract language, we offer a ground-breaking solution for non-programmers and those obliged to program by necessity. We add a 'natural language' layer to make smart contracts readable and usable by humans. Ring, in other words, is smart contracts in plain English.

Child Tokens

Child tokens are sub-tokens within the Emotiq ecosystem. While Emotiq has a native token, EMTQ, the platform can also be used to create derivative tokens.

EMTQ tokens are used to pay for any resources consumed on the platform (e.g., sending payments, paying for services, or creating child tokens and launching ICOs). EMTQ child tokens are a simpler version of the Ethereum ERC20 token. They're easy to create, and, coupled with Emotiq's intrinsic scaling capabilities, can be used for large-scale token generation events and sales. Child tokens can be freely exchanged for EMTQ, enabled through Emotiq's built-in decentralized exchange (DEX). Emotiq also provides the capability to exchange EMTQ with BTC and ETH via cross-chain atomic swaps.
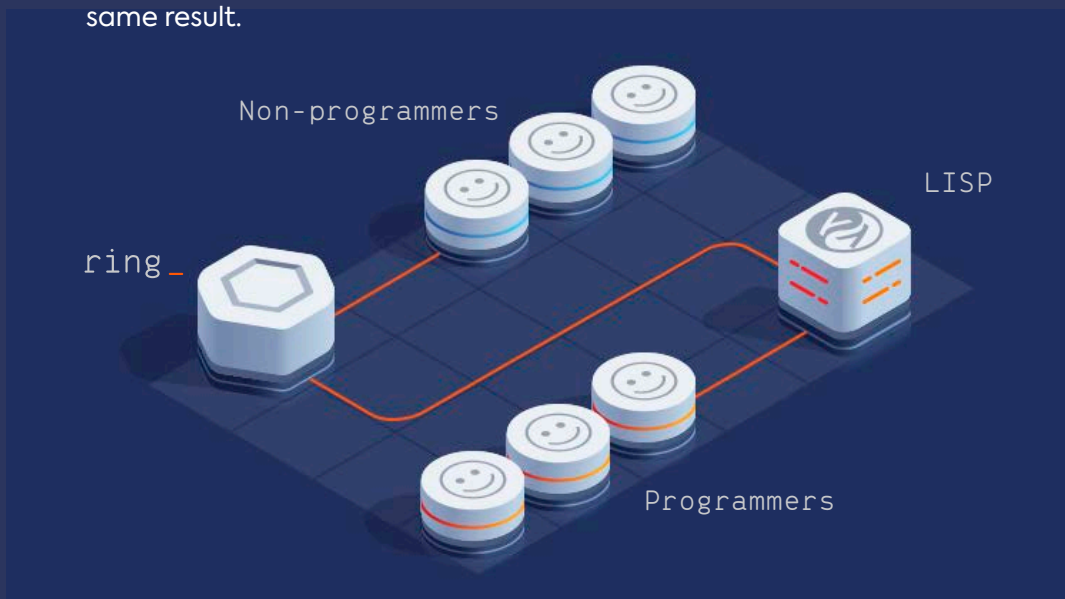
Natural Smart Contracts

We do not need to be an engineer to drive a car, or know what's inside an iPad to use an iPad. Likewise, we shouldn't need to be programmers to read and write smart contracts.

As the user interface of the blockchain, smart contracts have massive potential, but their current incarnations — in Ethereum's Solidity, for example — are limited. While Solidity is the most popular smart contract language, it is usable only by programmers (as it is modeled on JavaScript). There is no existing smart contract language for non-programmers, or those that program by necessity.

With Ring, the Emotiq natural smart contract language, we remedy this. Ring is a natural language that enables non-programmers to write smart contracts. On Emotiq, smart contracts are processed in Ring and compiled to Lisp and then the Ring virtual machine (VM). A smart contract may be written in either Ring or Lisp — Ring for non-programmers and Lisp for programmers — with each offering the same result.

We've made smart contracts writable and readable by humans. Users do not need to know how to code to program in Ring, and no flexibility nor functionality is lost in doing so. Through Ring, we dramatically increase access to smart contracts, accelerate the adoption rate, and, ultimately, revolutionize blockchain technology. Ring enables users to write smart contracts using familiar and fun concepts: a coin purse instead of a variable with a coin balance, for example.

Ring simplifies smart contracts. Like Zork, the adventure-based text computer game that inspired Ring, we've created a way for non-programmers to create programs and scenarios and test them in the Ring interactive environment. Zork was interactive computer fiction. Emotiq is interactive smart contracts.

Ring VM

The Ring VM runs smart contracts written in the native Ring language as well as most, if not all, Ethereum contracts machine-translated from Solidity. Those who program by trade may be well-served by Solidity, but want to leverage Emotiq's usability, functionality, or scalability.

The Ring VM is a sandbox that enables Emotiq to experiment with smart contract implementations and users to explore and preview smart contracts, interactively, prior to committing them to the blockchain.

Solidity

ring_

LISP

ring_VM

Oracles

Oracles allow smart contracts to interact with the outside world and are a vital part of the Emotiq platform and ecosystem. Oracles retrieve real-world data to provide results in answer to queries made by smart contracts. Imagine that smart contracts are formed of Lego, built within a small box, and oracles are miniature 'terminal' or 'portal' objects. For conditions to be met, and transactions confirmed, the smart contract requires a way to know what is transpiring outside of its box. This is the role of oracles – to enable smart contracts to access real-world data.

A wide and diverse ecosystem of oracles is needed to satisfy the increasingly diverse types of data required by smart contracts. A smart contract requiring weather information needs a different oracle than one requiring, for example, local traffic information. Any data requirement may warrant the creation of an oracle; as interfaces into the outside world, the oracle possibilities are practically infinite.

We further explain oracles and their role within the Emotiq ecosystem in the following Ecosystem chapter.

Oracle

Smart
Contract

Ecosystem

Emotiq's unique features and next-generation capabilities will enable an ecosystem to naturally flourish. Emotiq is more than a solution; it's a way forward. It's a means to dramatically accelerate the use of the blockchain, creating an accessible interface for all users. The Emotiq ecosystem relies upon smart contracts, child tokens, oracles, and the network effect.

Smart contracts

Emotiq features smart contracts understandable by humans, not machines. Ring is the heart of Emotiq and enables us to offer something no other blockchain can: easy and natural use. In addition, by providing partial compatibility with Solidity contracts, Emotiq accommodates those relying on existing platforms out of necessity, rather than desire.

A natural language approach to smart contracts will attract the millions of individuals unable to make use of Solidity, but who envision a use for the blockchain. This market is impossible to measure, but the Emotiq concept will conceivably appeal to every blockchain user, whether an enterprise, speculator, or developer. A technology's mass-market adoption is always catalysed by its first accessible user interface. Ring is the next-generation user interface of the blockchain.

Child tokens

Child tokens allow ICOs and TGEs to be created and run on the Emotiq blockchain, to leverage the platform's unique features and capabilities. These tokens are exchangeable back and forth with EMTQ through Emotiq's built-in decentralized exchange (DEX). Child tokens provide developers with access to immense crowd-funding opportunities on a scalable platform, for example, to support the creation of distributed apps or the sale of virtual goods.

It's essential that we provide an environment for unrestricted growth, with minimal obstacles. With Emotiq's built-in exchange, child tokens may be used and exchanged immediately. Significantly, child tokens are indirectly exchangeable for Bitcoin and Ether through cross-atomic swaps, enabling the exchange between EMTQ (for which child tokens may be exchanged) and Bitcoin/Ether.
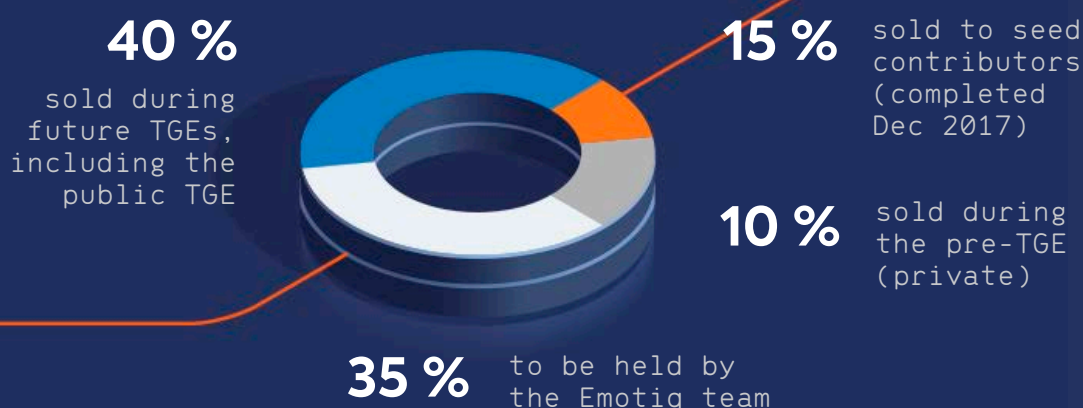
Oracles

Smart contract creators place oracles as pre-built components into their 'Lego box'. Developers are incentivized to create new oracles through a pay-per-transaction model (i.e., each time an oracle provides an answer, the developer of the oracle is paid). We aim to gather a library of oracle components to satisfy an ever-broadening scope for smart contracts, similar to how the Unity 3D Asset Store provides a database of 3D characters for game developers.

Scalability and the Network Effect

Emotiq, with its in-built scaling capability, easy smart contract access, and partial compatibility with Solidity, is designed to appeal to a broad spectrum of users — both those served by current solutions, but who desire more, and those that have hoped for a more scalable and easy-to-use blockchain. Its unique features and functionality will begin a 'snowball effect'; as adoption increases, so too will its functionality (e.g., with an ever-expanding oracle asset repository).

Token Generation Event (TGE)

Emotiq plans to raise $100MM (million) in a two-phase token generation event (TGE). The TGE target has been carefully selected to enable us to reach our development milestones and jumpstart the Emotiq ecosystem. In total, Emotiq will generate one billion EMTQ tokens, distributed as follows:

40 %
sold during future TGEs, including the public TGE

15 % sold to seed contributors (completed Dec 2017)

10 % sold during the pre-TGE (private)

35 % to be held by the Emotiq team

Emotiq will follow strict KYC/AML procedures during all phases of the TGE. Funds raised during the TGE will be used to, among other things:

- Expand the the Emotiq ecosystem through educational programs;
- Build a world-class in-house research team;
- Explore the different implementations of smart contract languages and their usability, to accelerate blockchain adoption across the mass-market and enterprise; and,
- Provide venture funding for early projects on the Emotiq blockchain.

Emotiq will aggressively pursue development, acquire the best talent, and explore new solutions. Its vision is ambitious, with equally ambitious goals.

The pre-TGE (private sale) will raise $15MM from institutional and large private contributors. It will be limited to two weeks and start on February 13. The public TGE will commence three to four months after, and will raise at least $69MM (at a per-token price at least 15% greater than that of the private TGE). Combined, the TGEs are intended to raise $86-100MM.

Tokens will be purchased in ETH. The price per token will be fixed at the end of the private sale, e.g. as soon as the target is reached, and will be linked to the current ETH/USD exchange rate. During the pre-TGE, the price will be equivalent to $0.15 per token. The price for the public TGE will be at least 15% higher.

- Team tokens will be locked up for 18 months.

- There is no lockup for seed or private sale contributors.

Any tokens unsold after the TGE will be kept in reserve by Emotiq and sold in small quarterly batches on the open market, to avoid drastically affecting market stability.

Emotiq will set up a temporary ERC20 token within 30-60 days after concluding the TGE. The lockup period will start from the time that the temporary ERC20 token is released. Emotiq intends to launch a testnet in the summer of 2018 and the mainnet at the end of 2018, at which point the temporary ERC20 token will be converted to EMTQ, the native Emotiq token. Emotiq will endeavor to ensure that both the temporary ERC20 and the EMTQ tokens will be listed on third-party exchanges. Listing on exchanges is beyond the control of Emotiq, however, and cannot be guaranteed.

Roadmap

Q1 2018

Expand development team to 20+ by acquiring an existing software development company

Q4 2018

Release testnet

Q2/Q3 2018

Release mainnet

Q2 2018

Conduct private and public TGE, release temporary ERC20 oken

Q1 2019

Convert temporary ERC20 token to native EMTQ

Future Development

Emotiq's development will continue — and accelerate — beyond launch.

- **User-friendly UI.** We will develop an interactive, user-friendly GUI for Ring and a development UI for the Emotiq blockchain, with easy access to application development tools.

- **Purging of old transactions.** With the blockchain's growth, and Emotiq's anticipated growth, it will be necessary to purge old transactions. We will develop a cryptographically-secure way to do so.

- **World-class research team.** We will build an in-house team of top Ph.Ds and industry leaders in distributed computing and cryptography, and collaborate with world class universities to access, develop, and implement cutting-edge research.

- **Enterprise.** Emotiq will provide the tools for the development of secure and scalable enterprise applications.

Everything else. We will not stop until Emotiq is the most powerful, scalable, and accessible blockchain. With formidable foundations, the future is bright.

Conclusion

Emotiq presents a unique opportunity. Every technology goes through stages. iPhone was not the first smartphone, and yet it delivered smartphones to the mass market. Emotiq is not the first blockchain, and yet it delivers a new standard of blockchain, with smart contracts programmable by everyone — interactively, and in plain English.

Emotiq is private, scalable, and natural. Research-backed and supported by a team of heavy-duty developers and hackers, we will deliver a next-generation blockchain with unique features. We will move fast, adapt faster, and explore together — in a blockchain adventure that has only just begun.
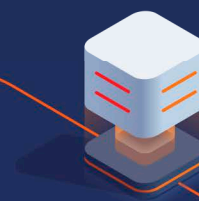
Team

Joel Reymont

The Buck Stops With Me!

Joel is a seasoned hacker and blockchain pioneer. He started his career on Wall Street and brings twenty-five years of diverse software engineering and management experience to Emotiq. Joel was previously Chief Technology Officer at a Top 100 cryptocurrency and blockchain company, where he earned a reputation within the community for his fearsome execution power. Joel has acted as Director of Prime Brokerage Technology at Deutsche Bank, has run offshore development teams, and has built many scalable and fault tolerant systems over the years. He now smashes technological boundaries and ventures deep into the unexplored frontiers of crypto to bring unique opportunities to Emotiq contributors.

Vladimir Lebedev

Chief Operating Officer

Vladimir has over twenty-five years of experience in managing technology in fintech, telecom, and media companies. His pioneering credits include creating the first FidoNet node in Soviet Union, the first remote banking application using asymmetric keys cryptography in Russia, and the first ISP in Western Siberia. Vladimir was CTO of the Russian stock exchange, where he created its trading system and network infrastructure. Vladimir has held executive roles at VEON (a telecom company with over two hundred millions subscribers), Sberbank (the biggest bank in Eastern Europe), Moscow City Telephone Network, Orange Business Services, Lucent Technologies, and Mail.Ru Group (the biggest Internet-media company in Russia). Over his career, he has led and successfully delivered many cutting-edge projects, in addition to launching his own companies, CPM and Cybertonica.

David McClain, PhD
Chief Rocket Scientist

David is literally a rocket scientist. Trained in theoretical and observational astrophysics, in addition to computer science, he brings an incomparable and extraordinary five decades of unique programming expertise to the table. David has served as a Principal Scientist in the aerospace industry where he built airborne LIDAR systems for underwater mine detection, and was a Senior Scientist on the Raytheon ExoAtmospheric Kill Vehicle (EKV) program. He is a true expert in numerous computer languages, including Lisp, and an authority on signal processing, image processing, guidance and navigation, radio-frequency and infrared target detection systems, and target tracking. He has twice addressed the European Common Lisp Meeting.

Shannon Spires
Agent Hacker

Shannon is a systems engineer who enjoys working on multidisciplinary projects. He spent much of his career as a research engineer at a national laboratory in the US, where he worked on a variety of applied research projects. He was the Chief Developer of several technologies, including robotic teleoperation controls, real time FPGA-based video signal processors, and intelligent electric power conversion devices. Much of Shannon's work has been focused on distributed agent-based systems. His areas of expertise include machine learning, AI, Common Lisp programming, functional languages, cyber security, and data mining. His research interests include the design of systems with inherent security and robustness, and navigation and categorization in ultra-large graph-based data sets with decentralized semi-autonomous agents.

Paul Tarvydas
Electronics and Microprocessor Guru

Paul's career has spanned three decades of working in microprocessor electronics, compiler and operating system design, and running his own highly-successful software consultancy. He has taken part in projects with companies such as IBM Canada, Mitel Corp, Cognos, and several start-ups, including Design Recovery Inc., Innovative Systems Group, JetLetter, Sable Technologies, and Alacrity Inc. Paul has written papers for the ACM and IEEE on techniques for optimizing concurrency, and has open-sourced his work on converting diagrams to code using AI techniques. Paul's research interests include software engineering, visual languages, diagrammatic languages, and reactive software. Paul has been working at Emotiq AG since January 2018.Paul has been working at Emotiq AG since January 2018.

Mark David
Senior Software Architect

Mark brings over twenty-five years of professional Lisp programming experience to Emotiq. He is a seasoned results-oriented software developer, architect, and technology leader with decades of hands-on entrepreneurial, technical, and management expertise in advanced software and product development. Mark was a cofounder of Gensym and a co-architect of its main product, G2, one of the most commercially successful AI/Expert Systems products of all time. In recent years, he has worked as a software developer and architect on many innovative projects, including an airline reservations system, a portable Internet satellite terminal, and a natural language understanding system.

Mark Evenson
Senior Software Architect

Ever since cobbling together a distributed system to process data reduction on unused nighttime nodes of the Cornell astronomy network in the late 1980s, Mark Evenson has been involved in plumbing the depths of what is possible to compute across the Internet. From modeling multi-party business process execution orchestration in description logic to hot-patching the hosting infrastructure for surging web traffic across the Western hemisphere, his work has repeatedly combined a future sketched by academic wizardry with the needs of the pragmatic now. He is excited to solve the problems inherent in developing and deploying a decentralized, planetary-scale sharded ledger.

Kieran Costello
Chief Wordsmith

Kieran has written for the market's leading tech companies and start-ups, and has been a core contributor to numerous ground-breaking blockchain projects. As a writer by habit and trade, he specializes in creating stories and brand identities for 'edge companies' – those innovating in uncharted spaces and offering new solutions to legacy problems. This naturally led him to focus on blockchain-based solutions, and specifically to Emotiq.

Emma Cooper
Community Wrangler and Cat Herder

Emma is the Community Manager for Emotiq. Prior to joining the team, Emma worked for many years in front-line counterterrorism for the US Department of Homeland Security, before which she was a lawyer in the US, focusing primarily on private placements and corporate law.

Anna Movchaniuk
PR Maven

Anna is a proactive, dedicated, and detail-oriented corporate communications practitioner with extensive public relations experience in Europe and Canada. She has worked on projects in industries as diverse as finance, sporting events, and film.

Legal Disclaimer

No part of this white paper constitutes legal, financial, business, or tax advice, and you should consult your own legal, financial, tax, or other professional adviser before engaging in any activity in connection herewith. Emotiq AG ("Emotiq"), its affiliates, and the Emotiq team members shall not be liable for any kind of direct or indirect damage, loss, or liability whatsoever which you may suffer or incur in connection with accessing this white paper or any other materials published by Emotiq. There is no official translation of this white paper from its original English, and recipients of foreign language translations are strongly cautioned that any information contained therein may conflict with the information in this white paper.

By accessing this white paper or any part thereof, you represent and warrant to Emotiq, its affiliates, and the Emotiq team that you acknowledge, understand, and agree that: (a) the EMTQ tokens (the "Tokens") described herein may have no value, there is no guarantee or representation of future value or liquidity for the Tokens, and the Tokens are not intended for speculative investment; (b) Emotiq, its affiliates, and the Emotiq team members shall not be responsible for or liable for the value of the Tokens, the transferability and/or liquidity of the Tokens, and/or the availability of any market for the Tokens through third parties or otherwise; (c) in any decision to acquire Tokens, you have not relied on any statement set out in this white paper; (d) you will and shall at your own expense ensure compliance with all laws, regulatory requirements and restrictions applicable to you; (e) the information contained herein shall be subject solely to Swiss law, and the place of jurisdiction shall be Zug, Switzerland; and (f) you are not eligible to acquire any Tokens if you are a citizen, national, resident (tax or otherwise), domiciliary and/or green card holder of a geographic area or country (i) where it is likely that the sale or distribution of the Tokens would be construed as the sale of a security (howsoever named) or investment product, and/or (ii) in which access to or participation in any token distribution event or the Emotiq platform is prohibited by applicable law, decree, regulation, treaty, or administrative act.

This white paper shall not be construed to be an invitation or solicitation to enter into an investment or participate in the sale of a security (howsoever named) or investment product in any jurisdiction. The information in this white paper is given for general illustrative and discussion purposes only, and Emotiq does not provide any warranty as to the accuracy and completeness of this information. Emotiq reserves the right to change the information contained herein at its sole discretion. The information set out in this white paper is not legally binding upon Emotiq, its affiliates, and the Emotiq team members. The agreement for any issuance or distribution of the Tokens shall be governed by a separate agreement setting out the terms and conditions thereof. In the event of any inconsistencies between such an agreement and this whitepaper, the terms and conditions of the agreement shall prevail.

EMOTIQ