tagion

Tagion Conceptual Paper

Creating a Sustainable
Economic World

Tagion Conceptual Paper, v.2.0

Theis Simonsen, Kristian Vestergaard, Carsten Bleser Rasmussen,
Tobias Ambs-Thomsen, May 2020

Introduction

In a world where new technologies are transgressing borders, legacy financial systems still chain us to traditional currencies and uniform, yet disparate and incomprehensive, banking models.

As the Internet has already transformed many other industries, a new kind of disruption is now finally confronting the shortcomings of current international pecuniary systems and legacy banking networks, ready to challenge models in the global financial industry that has not changed in decades.

But this time, it is not just the Internet alone.

The new and radically different concepts behind cryptocurrencies and underlying ledger technologies are fuelling a new wave of Fintech that has ushered in a new era for all financial and monetary systems.

These new systems, platforms and protocols are powering the next era of economic infrastructural technology and are poised to bring as much change as the internet did for a plethora of other industries such as newspapers, TV, retail, music, mobility, etc.

However, technical hurdles, governance shortcomings and pricing volatility have been critical roadblocks for these nascent financial instruments from becoming commonplace and have hindered mass adoption in many cases.

This is still the early days. And it's 'Blue Ocean'[1].

Scope

The purpose of this paper is to provide an overview of the ideas and main features of Tagion. For context "Introduction to Money" can be read on the homepage, which gives an historical and conceptual basis for Money and the Tagion White Paper is available for an in-depth description of the networks' technical, protocol and governance features.

---

[1] https://www.blueoceanstrategy.com/what-is-blue-ocean-strategy/

Table of Content

Introducing Tagion

Tagion is a monetary and e-banking system with revolutionary protocols that has the potential to replace legacy banking systems and trigger a paradigm shift in the current financial ecosystem.

The purpose of Tagion is to create a sustainable economic world. This can only happen with a serious alternative to the current fiat systems (government-issued currencies that are not backed by a physical commodity, such as gold or silver, but rather by the government that issued it).

Tagion is a democratic monetary system with the currency Tagions. It is a complete monetary system that enables essential banking services such as transactions and exchanges supporting local economies.

With its unique governance model, Tagion hands the money power back to the people with a system that is both democratic and socially fair.

-

In the current fiat systems (e.g. Euro, US Dollar or Yen) the money is issued and guaranteed by a central authority such as a central bank that controls the system. Essentially this means that a small group of actors manage the given monetary policy - and are in the tempting position of using the system to their own benefit or to the benefit of incumbents.

It is not a new problem:

"The problem with fiat money is that it rewards the minority that can handle money but fools the generation that has worked and saved money"

— Adam Smith, 1723-1790

Today it is not even the state that controls the issuing of money. Instead central banks print more money for commercial banks and the commercial banks leverage the money with fractional banking by creating credits and imposing debts on lenders[2].

Yet, it is the general public that holds the risk with this economic strategy, and it is the public that must step up when the system comes short of liquidity[3]. A good example of this was the latest worldwide financial crisis. Taxpayers pay for the banks failed attempt of earning huge returns by trying to control the money issuing function in society. It is social injustice - Robin Hood turned up-side down.[4]

---

[2] The Federal Reserve is an example of such a central bank.

[3] https://www.irishtimes.com/business/economy/bank-bail-out-estimated-to-have-cost-state-41-7bn-says-comptroller-1.4035332

[4] Mellor, Mary; The Future of Money; What is Money? Pluto Press (2010), https://www.jstor.org/stable/j.ctt183h0cz.5

tagion

Money should be democratised again and seen as a common resource for all.[5] Tagion will play a substantial role in removing the conflicts of interest in the current financial system and return the money power to the people.

The Tragedy of the Commons is an economic problem in which every individual has an incentive to consume a resource at the expense of every other individual with no way to exclude anyone from consuming. It results in overconsumption, under investment, and ultimately depletion of the resource.

Elinor Ostrom won the Nobel Prize in Economics, for proving an alternative governance model and through this, disproved, the Tragedy of the Commons.

Her solution is called Self-governance of Commons, which she proved is a more efficient way of governing a common resource. Self-governance of Commons needs a governance system in place, where the beautiful part is that the governance is built to serve the users of the resource and to ensure no conflicts of interest between the actors in the system and the owners of the system.[6]

The Tagion governance model is designed and built in adherence to these principles.

With the Tagion system a cryptocurrency, Tagions, is introduced. Tagions are a non-collateralised currency, meaning that the currency is not pegged to other currencies or assets and governed by the network protocols itself. Thereby it is fully independent from other monetary systems or central entities only based on the trust, which can be seen as general adoption in society as well.

As Tagion is an independent monetary system where Tagions are issued and guaranteed by the Tagion network that is owned by its users. In short, the users of the system are also the owners meaning there is no conflict of interest.

In the Tagion network the authority is decentralised to the nodes that maintain and operate the network by a democratic governance mechanism. The supply of money is constant in the beginning and later in the process, to be taken over by algorithms that uses intrinsic variables as inputs to control the money supply to support a liquid market and trust in the value of Tagions.

Tagion is both owned and controlled by its users and yet, open and technically accessible for everyone. The source-code will be open-source and Tagion as a whole seen as a common good.

In a 1984 interview, Friedrich Hayek famously said:

"I don't believe we shall ever have a good money again before we take the thing out of the hands of government. We can't take it violently out of the hands of government, all we can do is by

---

[5] Mellor, Mary; The Future of Money; What is Money? Pluto Press (2010), https://www.jstor.org/stable/j.ctt183h0cz.5
[6] https://www.nobelprize.org/prizes/economic-sciences/2009/ostrom/lecture/

some sly roundabout way introduce something that they can't stop"

And, in Free Market Monetary System, he noted that:

"…the monopoly of government of issuing money has not only deprived us of good money but has also deprived us of the only process by which we can find out what would be good money. We do not even quite know what exact qualities we want … because we have never been allowed to experiment with it. We have never been given a chance to find out what the best kind of money would be"

– Friedrich Hayek

It resembles what Bitcoin and other new monetary systems and Tagion strives to solve. Take the money power back to the people who work in the economy and depends on its reliability, making it democratic and socially fair.

We call Tagion the world's first genuine democratic monetary system, due to its governance model. The purpose of Tagion is to create a sustainable economic world.

The impact of a trusted peer-to-peer network like Tagion can have on the financial industry is limitless. Imagine people sending money to each other, exchanging currencies, or trading in financial exchanges across borders lightning fast with nearly no cost and in full privacy. It will increase overall business efficiency to the benefit of all participants in the system. This was one of the primary objectives for early innovators and adaptors of the first decentralised networks.

Real Economies and Local Use

Tagion provides people with a trusted non-national currency, where the money system is owned by the participants. It means:

- Banking would not be fractional anymore, because banks cannot create money anymore, they would need to be fully solvent. It means savings accounts would start to pay interest rates again, as money would have true value based on the backing of the people using the system.
- Lending can be facilitated in a borderless economy, and as money is not leveraged anymore, and all the complex regulation that is used to secure the solvency of banks would become irrelevant. In order words, banks would not be able to lend out money they don't have anymore. Even peer-to-peer or peer-to-pool lending becomes a real option as long the credibility and collateral challenges are solved.
- Imagine markets without the intervention of central banks, as we have it today, where both stock and state bonds are bought up at large by the

central banks, to "support" the market. By which they destroy normal competition and market pricing. Further to this, markets on market terms would mean that bursts and bubbles would be limited.

In general, banking is not equal to all and there are no real "free" and efficient markets based on real economics, one could just take a look of the front page of The Economist 9th May: "A dangerous gap, The markets v the real economy". One could argue it is not a dangerous gap but a permanent split, which has been discussed theoretically before.

Marx had some points towards the relations between commodities and money. We can call it consumptions-relations. It can be C-M-C, meaning a commodity is produced and sold for money to buy another commodity. It is real demand for an intrinsic value of a commodity that drives the demand and economic, where Money is an intermediate to facilitate the trade and the real commodity is the goal. If, the market takes form as M-C-M, where money drives demand with no real underlaying intrinsic need of a commodity, then the market becomes speculative and not based on intrinsic value of the commodities - real demand. Today, we have a system that is much controlled by money - e.g. central banks and governments intervening in the markets, screwing or destroying the real demand and market economy.[7]

---

[7] Marx, K., Das Kapital, Chapter 10.

Money and Problems

"Sound money' is a product of society, not of nature"[8]

- Hutchinson

Money is something people must trust, can be honoured in trade and maintain its value - while its actual value can vary over time. One should look at it as a trust in the system or trust in the authority behind the system.[9] You need to trust that your money has the same value today as tomorrow, so you can pay for food tomorrow as well. It is a big trust-flywheel, which gains speed as more and more people uses it. Money is a social construction, nothing more nothing less, but has many subjective meanings for people because it controls the premises for our lives.

The control is very powerful that is why we need a fair distribution of the money power in society and needs to find the best properties of money by creating new monetary systems.

Crypto-currencies have pioneered this revolution and breaking the current central bank regime the last decade, but it still has some major problems to solve.

We can divide the problems into Problems with Bitcoin or similar Proof-of-Work based systems and industry level problems, which hinder adoption of crypto-based banking solutions. Bitcoin is the main innovation, but as all first versions of technology has some flaws.

Industry level problems

1. No seamless decentralised closed-loop payments: It is cumbersome, not user friendly, done by custodian central party and expensive in most cases to off- and on-ramp into crypto and exchange crypto.
2. Requires sustainable governance mechanisms that facilitates a healthy network development and that creates a stable and independent monetary system. A real independent stable coin, which is not pegged to other currencies, backed by other assets and is not centralised governed.
3. Lack of scalable systems, interoperability and performance, which can deliver the required volumes, transaction speed and technical properties of a network being able to compete with e.g. the VISA network. One main property is having a deterministic sorting mechanism enabling e.g. a real DEX with price discovery, matching and settlement possible and in general a fair network.

1. **Problems with Bitcoin**
    1. Less than 1000 people own half the market cap of Bitcoin, a centralisation of wealth that far surpasses any other currency and country - even North

---

[8] Hutchinson et al., 2002:211
[9] Mellor, Mary; The Future of Money; What is Money? Pluto Press (2010),
https://www.jstor.org/stable/j.ctt183h0cz.5

Korea. A Gini coefficient of 1.0 means that a single person controls 100% of a country's income/wealth, North Korea scores 0.86 and bitcoin scores 0.88[10].

2. A small group of companies – mostly located in Russia, Georgia and China – control between two-thirds and three-quarters of all crypto-mining activity[11].

3. Almost all Bitcoin transactions occur on centralised exchanges that are hacked on a regular basis[12]. Over the last 10 years, it's estimated that more than 1 million BTC, has been pilfered from exchanges[13]. That's about $10 billion.

4. The development and future of Bitcoin is controlled by a foundation board and a small group of core developers who, it seems, are at battle with - and under pressure from mining pools[14].

5. It is not scalable for daily transactions.

---

[10] https://www.theguardian.com/technology/2018/oct/15/blockchain-democracy-decentralisation-bitcoin-price-cryptocurrencies
[11] https://www.theguardian.com/technology/2018/oct/15/blockchain-democracy-decentralisation-bitcoin-price-cryptocurrencies
[12] https://hackernoon.com/a-huge-list-of-cryptocurrency-thefts-16d6bf246389
[13] https://news.bitcoin.com/hackers-have-looted-more-bitcoin-than-satoshis-entire-stash/
[14] https://bitcointalk.org/index.php?topic=2255631.msg22880044#msg22880044

Tagion

The team behind Tagion is building a system that addresses many of the issues that both the fiat based monetary system and DLT based systems are suffering from. Tagion is both an alternative - and a supplement - to both the current financial system and the DLT based systems.

The Tagion models are in place and a lot of the supporting technology has been built and is running in an alpha version. All code will eventually be open source with free and grant back licenses.

What exact problems and how these are addressed by the Tagion system is discussed in the following. Three main topics are addressed, which are:

- Governance
- Decentralised Exchange (DEX)
- The underpinning technology

Tagion Governance

The governance model is a set of rules that define how decisions on different levels are made and adopted. A well-designed governance model is one that represents the interests of all actors in the network. We can divide the governance into three main types:

	Purpose	Means
Node Governance	Being a non-discriminating and decentralized network creating network security and inclusion Transparency and interoperability	Proof of Community (selects trusted community nodes) Reputational Trust Scoring Model(Selects active nodes based on scoring and incentives)
Economic Governance	To instil trust in the monetary system and provide adequate liquidity	Fixed Supply first Network algorithmic controlled supply Contribution Rewards
System Upgrade Governance	Ensure the network is upgradable, stable and secure Facilitates collaboration between developers in the community	Three-layer technical governance, depending on the backwards compatibility of the upgrade.

1. **Tagion m**
2. **ain incentives – Contribution Rewards**
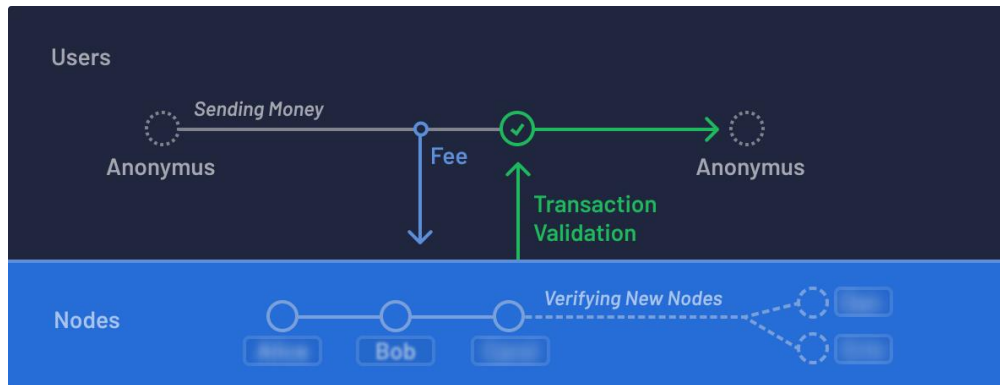
The system consists of users and nodes. Nodes run the software that is used for maintaining the Tagion ledger and are paid for providing these services. A node is owned by a user that has opted to become a node owner. Users pay to use the network that is making the transactions. Both users and node owners need to have their interests represented and balanced for the network to function.

The common problem in DLT governance is the centralisation of power, like in the case of Bitcoin[15] and Ethereum[16]. Proof-of-work and proof-of-stake are giving the power to the actors having most power, either monetary or computational power. It is neither democratic nor decentralised, as it by design facilitates centralisation, because of the needed financial resources and competencies to compete as a miner in the network. A more democratic governance model is needed, which also ensures healthy development, incentivises and secures the decentralised system.

Effective decentralisation is crucial to keep a network secure, borderless, censorship-resistant and self-governed. In the case of Tagion, it means that the system needs to be controlled by node owners, in an efficient and democratic manner. The Tagion governance model is based on ideas and design principles of Nobel prize winner, Elinor Ostrom who solved the Tragedy of the Commons[17] and on Charles Darwin's evolutionary theory[18] of how species best survive in a new environment.

Ostrom summarised the conditions needed to solve the Tragedy of the Commons[19] with eight core design principles for which she was awarded the Nobel Prize in economics in 2009:

1. Clearly defined boundaries

---

[15] https://www.blockchain.com/en/pools
[16] https://www.etherchain.org/charts/topMiners
[17] https://evonomics.com/tragedy-of-the-commons-elinor-ostrom/
[18] https://en.wikipedia.org/wiki/Darwinism
[19] https://wle.cgiar.org/content/elinor-ostrom-%E2%80%9Cnon-tragedy-commons%E2%80%9D

tagion

2.   Proportional equivalence between benefits and costs

3.   Collective choice arrangements

4.   Monitoring

5.   Graduated sanctions

6.   Fast and fair conflict resolution

7.   Local autonomy

8.   Appropriate relations with other tiers of rule-making authority (polycentric governance).

The governance mechanism in Tagion implements all of Ostrom's core design principles.

Public and Permissionless

The Tagion network is public, permissionless and has no central authority, meaning it is technically impossible to limit someone from using the network. Anyone can take part with the only prerequisite being internet access.

Roles and Incentives

The business model is that the user pay a fee for services on the network and node owners get rewarded for operating the network.

Users benefit from fast, private, cheap and uncensored transactions, while nodes benefit from the incentives offered to them for operating the network.

Node owners are public servants of the network and are identifiable through a name record in the system, where they have a pseudonym. Node owners must be socially validated to participate, this validation is performed by other node owners. A node owner gets rewards from fees and from validating other node owners and are thus rewarded for keeping the network healthy.

The network, its technology and protocols need to evolve continuously to keep both users and node owners incentivised, and to ensure upon the systems overall efficiency and security. The Tagion governance model is divided into three separate governance layers, allowing this to happen:

- Node Governance
- Economic Governance
- System Upgrade Governance

Technical details about the governance model can be found in the Tagion Technical Paper, available from https://tagion.org/tagiontechpaper.pdf.

Node Governance

The Node governance layer is the security mechanism in the Tagion network. It limits the chance and the rate at which bad actors can join the network and ensures a fair distribution of rewards.
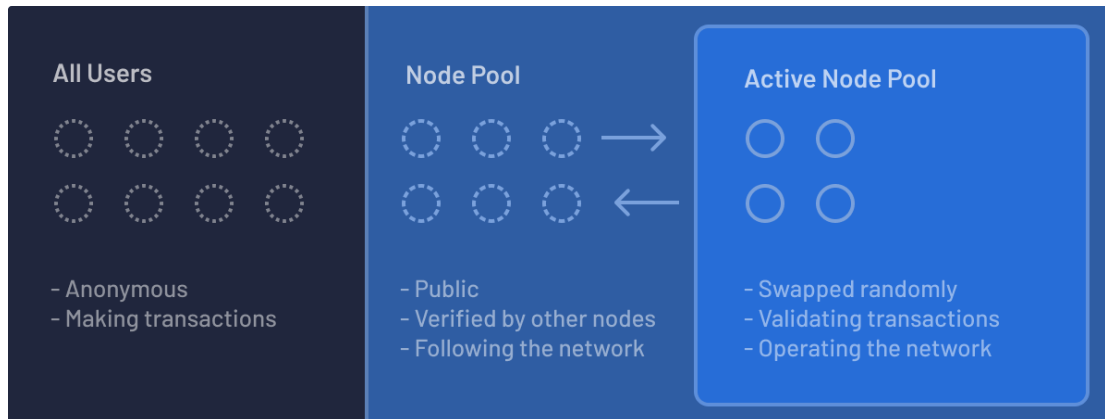
Nodes in the Active Node Pool operate the network. Nodes are swapped in and out of the Active Node Pool by an unpredictable random algorithm, making it impossible to predict how a current or future Active Node Pool is made up.

Proof-of-People

Tagion utilises what is dubbed the Proof-of-People protocol, a heuristic social protocol based on random validation and social components, to achieve a democratic principle of "one person – one node" and "one person – one vote". The social component makes it difficult to operate more than one node, while the scoring mechanism reduces the incentive of doing so even more.

Any user can apply to become a node, by following the seven main steps:

1. A user creates a name record in the system to become a public user.
2. When the name record is at least a month old the user makes a node transaction and pays a fee to become a node. The user then participates in the lottery for becoming a node. All participating users will eventually win the lottery.
3. When the user has won the lottery, the user proves to the network that activity has taken place during the past seven days. By doing this, the user also accepts to become a prospect node. The next step is for two current nodes in the system to mate and give the new user - now their offspring - a gene.
4. The prospect engages in a dialogue with three randomly chosen nodes. The three nodes need to socially validate that the prospect is an actual person.
5. The prospect nodes follow the network and earn node reward points until the minimum score is obtained.
6. The prospect engages in a dialogue with two randomly chosen nodes. They should all socially validate the prospect is an actual person.

tagion

7. The prospect is now a real node, is given a birth date and an updated gene string in the system and can become an active node.

Each step is designed with a specific function in mind.

The first to steps create an incentive for the user to become a node (public name and recovery of the paid (stacked) fee). The one-month age requirement for the name record introduces a time-lag in the system making it impossible to spin up a lot of nodes overnight. The lottery makes it random in which order new nodes are chosen again avoiding a person to spin up a large number of nodes in a short period of time. This virtually eliminates Sybil Attacks[20].

Step 3 ensures that the user is an active participant on the network and not just an inactive lottery ticket. Two nodes verify the node and gives the user a gene by making a mating transaction.

Step 4 is another security check that ensures the prospect node is a real person. All nodes have a name record making it possible to contact each other and engage in a dialogue either by video or chat.

Step 5 is another time-lag, but also a test of commitment. At this stage the node can follow the network and in practice operate the network.

Step 6 is again a second social validation through dialogue.

In step 7 the prospect has become a node and given a birth date and a gene in the system.

Reputational Scoring Model

The Reputational Scoring Model is based on Charles Darwin's evolutionary theory of how species best survive in new environments.

One of Darwin's best-known statements, 'survival of the fittest', is that all species of organisms arise and develop through the natural selection of small, inherited variations that increase the individual's ability to compete, survive, and reproduce.[21]

Another important, but less famous aspect of Darwin's studies is the 'survival of the kindest'. Darwin argued for "the greater strength of the social or maternal instincts than that of any other instinct or motive." His reasoning was disarmingly intuitive; in our hominid predecessors, communities of more sympathetic individuals were more successful in raising healthier offspring to the age of viability and reproduction -- the *sine qua non* of evolution.[22]

Both gene-diversification and caretaking are the inspiration for the scoring model variables described below.

---

[20] https://en.wikipedia.org/wiki/Sybil_attack
[21] https://en.wikipedia.org/wiki/Darwinism
[22] https://www.psychologytoday.com/us/blog/born-be-good/200902/darwins-touch-survival-the-kindest

tagion

A node in the system has multiple reputation scores that determine its chance to earn rewards:

- The **Gene Score** improves when node mates with each other (validates), and by that perform a human-work aspect of running the node, which improves the genes. That is both gene-diversification and caretaking of the network, keeping it healthy, giving it a better node score and improving the likelihood of being chosen as an active node.
- **Contribution Loyalty** increases when the node operates the network and decreases, when not available.
- **Active time** increases when the node operates the network and decreases the chance of being an active node.
- **Node age** increases along with the node being available for the network and so does the chance of being swapped into the active node pool and receive rewards.

The active nodes earn the rewards in the system and the model controls who are active nodes. The scores determine the probability of being swapped in and out as an active node. Therefore, the model creates an incentive for being available for the network and increase node age and improve the gene scores continuously.

The node governance, Proof-of-people and the reputational scoring model are the primary governance mechanisms for securing the network. When combined, it becomes very difficult to attempt a network take-over, as it would require a lot of resources, patience and a lot of consideration towards how to ensure gene diversity.

E.g. an evil actor wants to take control of the network that consists of 10,000 nodes and 100 active nodes.

In this case the probability for the 100 evil nodes to take over the network is in practice zero, as most existing nodes would have higher availability scores now and going forward and better gene-scores. The evil actor would in other words, need to spin up just as many evil nodes as there are available nodes in the entire network … and ensure their scores outmatch that of all the other nodes.

It would be close to impossible, as the proof-of-people protocol is invoked both when becoming a node and for an on-going dialogue going forward. In the beginning it can be argued that the lower numbers of nodes make it easier to attempt a takeover, but as adoption occurs, it becomes very impossible.

The mathematical proof for the claim is detailed in the Tagion Technical Paper.

Economic Governance

It is crucial both for trust and efficiency of a monetary system to regulate the money supply efficiently. Central banks do it for fiat systems and many DLTs, such as Bitcoin, have a fixed money supply designed after scarce resource model theory[23].

Others choose to peg their currency to fiat currencies or assets by creating some kind of a collateral as guarantee, which makes the system depended on others and not a "real" independent monetary system. Pegged currencies are known as stable coins and are currently being considered as potential securities by the us regulators (the SEC).

Tagion will be an independent monetary system with no centralised group of people controlling the money supply. Furthermore, a fixed supply is not efficient for making the market liquid, as the exchange unit is scarce, and it may not be able to cope with the market demand.

In Tagion algorithms function as money supply oracles that control the supply, based on internal variables.

Rewards and fees are also controlled by algorithms that help make up the mechanism for regulating the money supply in the network.

Economic governance will be implemented in two phases in the network. In the first phase token supply will be linear and stable and have a hard cap. The second phase introduces a model for stabilising the currency based on internal variables in the network that controls the token supply.

Tagion will be a non-collateralised currency, meaning not pegged to any other currency or assets, keeping it as an independent monetary system.

Phase 1. Stable and fixed supply

In the first phase - as Tagion gains adoption - there will be a stable and known money supply, like Bitcoin. This will last for a maximum of five years or until phase 2 commences.

Price volatility is expected at first, since mass adoption does not happen immediately.

As adoption increases, along with the number of actors in the system, a single actor's transaction will become insignificant to the price, which helps price volatility to decrease. When the network is ripe, Phase 2 will be started, where algorithms will control the money supply and stabilise Tagions.

Phase 2. Algorithm controls the money supply

This is a concept on how the money issuing and burning should be controlled. It goes between two extremes of a currency backed by a scarce resource, limiting the

---

[23] https://nakamotoinstitute.org/static/docs/commodity-and-scarcity-in-light-of-bitcoin.pdf

supply which decreases the liquidity and general economic activity. The other extreme is unlimited supply, where a significant amount of money is printed and added in the system all the time, and by that destroying the measurement function of the currency.

Most importantly, money is a social phenomenon based on trust in it having future value and being acceptable as payment. Hence a money issuing function is needed that can gain trust by users over time. Trust cannot be gained, if such a function is overly complex and non-transparent or if it relies on external variables from other systems.

In general, to keep the market stable, a simple modelling of the use of money must be based on internal variables, such as velocity of money (total velocity of Tagions), adoption level, supply of money, average transaction sizes and more. The model can be used as a measure for demand on liquidity and be the basis for whether money needs to be added or removed (burned), to keep the market stable.

The system burns money every time a transaction is made, and all fees are burned per definition. Rewards are given to nodes, when consensus is reached. If the rewards sum up to more than the burned fees, there is a money increase in the system, and the sum is lower than the burned fees, the opposite is true, i.e. a money decrease.

System Upgrade Governance

Algorithms are controlling upgrades of network protocols and script functions. The aim is to foster collaboration and avoid hard forks.

The system upgrade governance consists of three sub-layers:

Minor upgrades and bug fixes are adopted at a higher rate, as compatibility is maintained with current protocols.

The core and structural upgrades require nodes to operate both the new and old version of the network in parallel, until the majority of the network adopts the change.

Script function upgrades need to be approved by five out of six nodes to take effect. Script function upgrades does not impact the network protocol.

Governance Conclusion

The Tagion governance model addresses all the known issues of modern cryptocurrency, while at the same time serving as a security mechanism, completely disincentivising malicious behaviour. It is truly decentralised and represents the interests of all its users and node owners alike.

Decentralised Exchange, DEX, a cryptocurrency market innovation

Tagion solves many of the issues found in other major cryptocurrency networks – which opens the door for the creation of more effective decentralised exchanges between cryptocurrencies.

Currently, many centralised cryptocurrency exchanges offer similar exchange services such as Bitcoin to USD exchange. There is however no interexchange market between these institutions and platforms, which means that a price difference is often to be found on the same currency pair offers, opening up for arbitrage opportunities. In other words, a Bitcoin could cost 10.000 USD in one exchange, and 10.110 USD in another, a price difference that can be exploited by traders.

Decentralised exchanges and protocols such as Atomic Swap with cryptocurrencies have been created to solve this issue. However, there are still unsolved problems for this to work such as sufficient liquidity, price discovery and matching of bids and asks.

There is no collective unit-of-exchange, meaning the number of currency pairs is very high, effectively evaporating liquidity. More, the matching needs to happen one-to-one with the size and price, making both price discovery and matching difficult. Lastly there is no order of transactions in many cryptocurrency networks, making it impossible to determine a fair way to order bids and asks. The consequence is dysfunctional systems for carrying out decentralised cryptocurrency exchanges.

The Lightning Network, supporting among others Bitcoin, is a network that can route payments between two different accounts connected to the network. This is done off-chain and only once everything is in place, transactions are triggered on the blockchain. The Lightning Network can in principle be used to exchange between two different cryptocurrencies like Bitcoin or Litecoin, by two parties, providing that the exchange rate is agreed between the two. The Lightning Network is limited to routing and cannot in itself act as an exchange, as it is incapable of price discovery and price matching, both necessities for a seamless exchange to take place.

Tagion has ordering, making it possible to do fair price discovery and price matching decentralised, which when combined with the routing functionality of the Lightning Network, lets the Tagion network accomplish decentralised exchange between Lightning Network compatible cryptocurrencies (Tagions, Bitcoin, Ether, Litecoin and more). Bids and asks are placed in the network, which gives full transparency and order depth for all users, not limited by a central exchange.

The Tagion decentralised exchange, DEX, always trades alien currencies against Tagions (TGN), which helps to create high liquidity and thus heightens the matching probability. For example, a user exchanging BTC to LTC means that two exchanges are required. The first is BTC to TGN and the second TGN to LTC.

The exchange is supported by the guarantee model, where the part selling alien currency locks an amount in Tagions to their corresponding ask. If they then do not fulfil the order on their side by revealing the secret key for the Lightning-network, the guarantee amount is lost to the counterpart, which incentives for the deal to take place.

It is DEX that orders bid and asks, does price discovery, matchings and settlements. DEX utilises the needed channels and functionality from the Lightning network. It guarantees fair bid/ask price matching and fully decentralised order execution through the use of the latest innovations in the Lightning Network and Tagion that successfully solves the routing problem of the Lightning Network.

Due to the low-level system design, the order placing, and revoking will have some delay, adding friction and making price pumping by large players much riskier, resulting in a healthier balance between small and big traders.

The underpinning technology

While first generation DLT networks have expanded the possibilities to trade and transfer money and opened up for the use of Smart Contracts and the execution of decentralised applications, they have failed in becoming a practical, everyday tool for transactions, hindering mass adoption. The key areas that must improve for DLT networks to gain mass adoption are transaction and validation speed, efficient decentralised data storage, lower energy consumption, and providing ease of use such as when paying or exchanging from one currency to another.
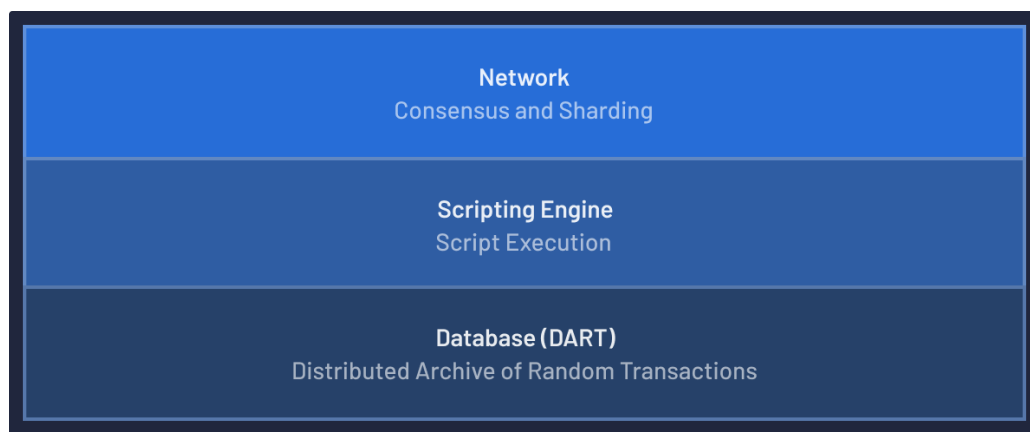
tagion

The Tagion system architecture

The Tagion system consists of different components, residing in three main layers.

It is architected so each layer - and each component within a layer - can be optimised individually, and also replaced individually when new and smarter technology emerges.

In this way the system can be kept current as technology evolves.

1) The top layer is the network. It consists of three main parts;
   a) The gossip protocol used for data synchronization
   b) The hashgraph algorithm used for consensus and ordering of transactions
   c) The sharding capability that, along with DART and the Scripting Engine, enables parallelism of transactions and provides the speed of the system.

2) The middle layer is the Scripting Engine that, based on input from the Network and DART, executes transactions and stores the output and deletes obsolete data from DART. Scripts are written in Funnel, a scripting language developed for the system, inspired by Forth[24]. Funnel is made robust and secure by limiting its functionality to be optimised for transaction execution. As an example, infinite loops are not possible.

3) The bottom layer, the database, DART (Distributed Archive of Random Transactions) stores all current bills (comparable to paper bills in a fiat system). Spent bills are deleted and receive bills are created in the database. Functionality is built in to automatically purge unused Tagions after some time, to avoid carrying orphan bills around forever.

   DART is built on design principles that are based on a licensed patent, which allows for optimisation of the execution speed a millionfold over other existing technology, by making use of an optimised sparse Merkle tree.

---

[24] https://www.forth.com/forth/

An important aspect of the Tagion system is that it only stores the output from transactions. The consensus data contains mere intermediary calculations.

The data flows as follows; a user creates a transaction, which a node puts into an event as a transaction script. The event is gossiped to the network and consensus is reached. The transaction is then executed by a node's scripting engine and the output is stored in the DART.

The Tagion system solves a number of issues that are inherent in most other DLTs. These are:

1) Volume of transactions
2) Speed of transaction validation
3) Energy consumption
4) Inefficient use of data
5) No ordering – unfair, discrimination and sequential execution
6) No sharding

3. Volume of transactions

Bitcoin processes 3-7 transactions per second. VISA does around 1,700 transactions per second on average (based on an average of 150 million transactions per day)[25], and the network can handle peaks of up to 65.000 transactions per second. For everyday use of cryptocurrencies to happen, it is the properties of VISA that should be the aim, and not the properties of most of the current DLT systems.

Tagion uses hashgraph for consensus, which in the Tagion implementation, makes it possible to process more than 20.000 transactions per second[26] per Shard. Tagion is architected to be able to scale to hundreds of Shards that operate equally fast in parallel.

4. Speed of transaction validation

Bitcoin uses 10 minutes on average to validate a transaction. On the VISA network validation takes place in two to three seconds. Transactions are validated in two to three seconds in the Tagion system, putting it on par with VISA in terms of validation speed.

---

[25] https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44
[26] https://www.hedera.com/blog/pulling-back-the-curtain-on-the-hedera-consensus-service

The fast validation time is reached by use of hashgraph for consensus and an efficient patent pending gossip mechanism. The hashgraph algorithm and the accompanying mathematical proof was discovered by Leemon Baird[27].

It solves the Byzantine Generals' Problem, a term that takes its name from an allegory developed to describe a condition, where actors must agree on a concerted strategy to avoid catastrophic system failure, whilst some of the actors are not trustworthy.

The algorithms makes sure that if more than two-thirds of the nodes in the network follows the same consensus rules, all will, in finite time, reach the same order of events – confirming and validating any action on the network such as a money transfer, money exchange, or data interactions.

The gossip mechanisms optimise data exchange between nodes to happen most efficiently. This mechanism is patented, and a perpetual license has been given to the Tagion project.

5. Energy consumption

In the world of cryptos it is well known that the most popular networks, such as Bitcoin and Ethereum are anything but energy conscious, as they lean against the proof-of-work protocol[28]. Tagion's proof-of-people protocol uses insignificant, close to zero, energy compared to proof-of-work.

The hashgraph consensus mechanism, DART, and the lean script executions allows Tagion to be operated on low powered commodity hardware, such Smartphones. In comparison, banks are settling transactions with other banks by use of multiple mainframe-based systems and proof-of-work based cryptosystems are demanding an ever-increasing share of the total power consumed world-wide.

6. Inefficient use of data

Most DLTs uses a decentralised immutable database for storage. The blockchain data structure is immutable meaning all data should be stored forever and cannot be deleted. This means that every network participant (usually referred to as miners or node owners) have a full copy of the database; processing, storing and exchanging huge amounts of data. The security in the blockchain lies in the whole chain, thus you cannot just delete old irrelevant data if you want to do a full validation, because then you cannot prove the data integrity with cryptography.

Tagion uses a distributed database for storage, meaning a node only stores a part of the data. DART gives away with immutability and only the output of a transaction is stored, while input and calculations are omitted, helping to reduce size. The innovation in terms of data utilisation is however that once a bill becomes irrelevant, it is deleted, rather than kept forever.

---

[27] http://www.leemon.com/
[28] https://cacm.acm.org/magazines/2018/7/229045-why-cryptocurrencies-use-so-much-energy-and-what-to-do-about-it/abstract and https://cacm.acm.org/magazines/2018/7/229045-why-cryptocurrencies-use-so-much-energy-and-what-to-do-about-it/abstract

Tagion utilises a licensed patent pending validation mechanism to validate transactions stored in DART. A license has been given to the Tagion project. The mechanism transforms a problem that is burdened with an exponential workload in other systems into a linear workload, which saves vast amounts of CPU power.

7. No ordering – unfair, discrimination and sequential execution

Proof-of-work systems are probabilistic systems with no ordering, there is no accurate timestamp on each transaction. The miners decide on which transaction to put in a block and validate the transaction. It is usually decided by price but can also be chosen freely by the miner. It means, it is not necessarily the first to submit a transaction, which gets it approved first. It is also means it cannot function for ordering of bids and asks sorted by timestamps, do price-discovery and fair matching.

Another consequence is that everything is sequential, because it is a block in a chain a new block needs to be added, before new transactions can be worked on, where all are racing to solve the same problem. This is also related to the non-distributed data, which is a hindrance for parallel execution.

Tagion uses the Hashgraph algorithm to achieve fairness, because it has exact ordering of all events, transactions in the system. It is a deterministic system, meaning it has a finality, where the order is fully settled for all in the system. By having both a truly distributed data storage, which stores the outputs from transaction scripts and ordering it allows for parallel execution of transactions.

8. No sharding

Bitcoin, Ethereum and most other DLTs comes without sharding. Sharding allows for a network scale with more shards to increase overall system performance. By splitting the network into smaller parts greater scalability and performance can be reached.

tagion

Adoption

Tagion offers a number of innovations and services that are on par or surpass the services available in existing monetary or cryptocurrency systems, supported by a solid democratic governance model and non-collateralised e-money. To gain adoption actual services for users need to be developed and marketed to gain adoption. The Tagion system is merely an enabler, which will have no adoption by itself.

Along with essential services, such as a Consumer Wallet, Merchant software, and the capability of doing decentralised exchanges, Tagion is a complete offering for basic monetary services - transactions and exchange - from the outset.

Tagion is an alternative to the existing systems, and the team has chosen to focus on driving adoption with a bottom-up approach. With this approach, merchants and consumers would be the key stakeholders to reach for the Tagion network to get utilised, as the power of the payment infrastructure is in the hands of the consumer, so to speak.

The strategy for driving real use of the services in the Tagion ecosystem is to offer value added services, either directly or through ecosystem partners that will compete on real utility, price and stability.

Offering a functioning monetary system decoupled from political influence and banks will also by itself drive use. The incumbents rely on the existing ecosystem of services, which can be seen as a major advantage in mature markets.

However, decentralised systems provide new types of services that are not possible to operate in existing systems. This is especially true for Tagion, which due to its openness, low cost, and non-discriminating nature, fits very well into markets where the current digital banking systems do not thrive.

As an example, anyone with internet access can become a Tagion user. Tagion needs to support, facilitate, educate even part-fund applications that creates user value and adoption. A developer community is key to develop and create partners from.

Tagion ecosystem

-

Initiatives such as those initiated by IMF and Facebook (Libra) are not seen as competing, as these solutions are not actual independent monetary solutions, but a way of adding some of the wanted features from DLT on top of the existing system, without solving the underlying issues.

Both rely on bucketing assets or currencies to support the value of their cryptocurrency, meaning they rely on the current monetary system and are hit by costs and issues such as infrastructure cost, transfer fees, inflation and deflation, exchange commission, market exposure risks etc.

The introduction of these systems by world-wide actors is actually an asset for Tagion. The fact that household names enter the DLT-sphere has lowered the bar of acceptance for end-users.

With Tagion being fully and democratically controlled by its users, it is the epitome of a democratised financial system - something the IMF and Facebook's DLT's have a hard time comparing to.

There are other crypto-projects that should be acknowledged such as Hedera, NEM and IOTA projects. Each of these projects solves some of the issues heighted

earlier, but none of them solves all of the issues collectively. Tagion does have an edge in the market by providing a new monetary system that is non-collateralised.

-

Two basic key ecosystem enablers need to be available in the Tagion network before any adoption can start happening; DEX (decentralized exchange) and a wallet application.

DEX is one of the first features that will be released once the test network is fully implemented.

The wallet application makes the utility value of cheap transactions and DEX accessible for consumers, merchants, and traders etc. who would want to use the network. The wallet is also suitable for both for consumers and merchants, to use and store their Tagions.

DEX features will be added to the wallet application, making it possible to do seamless exchanges between supported cryptocurrencies, directly in the app.

The wallet (and other transaction services) will be very low cost in terms of transactions and enable seamless exchange between DEX supported cryptocurrencies, in practice allowing for creating multi-currency applications.

Tagion is currently developing a wallet solution with a third-party supplier.

-

DEX and the wallet will help to drive up liquidity and provides the basis for user uptake.

They do however not cut it on their own. Several initiatives will be launched, alongside the go-live of the test network that will help to drive real world usage.

Here, limited trials with partners are planned for testing of the system capabilities on local markets such as in Ukraine and Denmark, where the current teams are located.

Ukraine is haunted by high inflation (14.4% in average, 2008 to 2018[29]) and high corruption rates (Ukraine is in the wrong third of all countries in the world, in terms of corruption in the public sector, according to Transparency International[30]).

Denmark is the opposite end of the spectre in terms of inflation and corruption rates (although parts of the Danish banking sector appears to behave in dubious ways[31]).

By starting test in two such diverse countries, several thesis's for adoption can be tested in vastly different environments. The test aims to both drive actual users onto the technology (wallet, DEX and the Tagion network itself), and to test a geo-

---

[29] https://www.worlddata.info/europe/ukraine/inflation-rates.php
[30] https://www.transparency.org/country/UKR
[31] https://danskebank.com/about-us/corporate-governance/investigations-on-money-laundering

based incentive model that helps drive community building and that is applicable worldwide, once battle tested and adjusted.

Another vehicle for driving adoption is the partner ecosystem or developer community. The Tagion team is working on securing a number of partnerships for services such on and off ramping of fiat to and from cryptocurrencies (e.g. e-money license holders), of integration into e-commerce payment solutions and for development of the consumer wallet and the decentralised exchange.

Developer tools and open-source

Another corner-stone of creating adoption by creating superior user value comes from the creation of a healthy developer community.

Tagion will create a development package including a set of development tools and the executables that will allow developers to run a virtual network and build applications on top of this by using the interfaces for the system. The first package will be released in December 2019 and this will allow the community to begin to build on the core technology. Tagion is committed to drive and support the community in every way.

The Tagion network will eventually be totally open sourced. The open source license type is not fully determined yet, but it will be along the lines of GNU GPL.

When open sourcing begins in the near future, the Tagion team plans to have adequate resources available to properly support building a Tagion coding community, as the intention is for the community to assist in setting the direction for future development and to drive innovation on top of the system.

Tagion, the past, present and future

The first lines of code in the Tagion git, tagion_core main branch, dates 07-16-17, at the time of writing more than 1026 commits have been made and 75 pull requests.

Besides the core projects, external projects for debugging and visualization of the network has been developed and a beta edition of a wallet has also been developed. The main components such as the scripting engine, HiBon, the gossip mechanism, the consensus algorithms, DART, multiplex network API with SSL etc. are implemented and tested. A live broadcast from a demo network can be seen at https://tagion.org/about/network. The demo network has been live since December 2018.

Tagion was born in March 2017 and had the first two full-time employees since later Summer 2017, growing ever since with both more full-time resources, advisors and partners. Tagion has from the outset been funded by the management team focusing on delivering solutions to current problems from the start instead of selling hot air and creating paper tigers.

The management team has in various settings always worked with delivering solutions to prove ideas and concepts, leading to finalising complete products. For Tagion the team has been focusing on the development of not only concepts and theories, but also the practical implementation and testing of the core technology. The approach has been to get the most difficult challenges out of the way first, in order to prove that it was at all possible to achieve the technical vision for Tagion. The most difficult issues are solved and tested.

In September 2017 Leif Block Rasmussen joined as an external consultant and advisor on governance. His main contribution was the development and input to the governance thoughts.

In April 2018 it was proven that the team was combining technology in a completely new way as a thorough legal due diligence on existing patents on related technology was made. The diligence revealed that no existing patents are violated by the technology used in the Tagion system.

In December 2018 the first 0.9 conceptual whitepaper was done, including the main technical components and governance. This formed the foundation for the Tagion project.

On September 5th, 2019, a patent on DART, a distributed database tailored for the Tagion network, was filed.

With a demo network up and running, which includes all core components, patents filed, and a robust advisory network in place, the team is finally ready to introduce Tagion to the world. The Technical paper and the Whitepaper (this) have been written to document the solutions in depth and on a more general level including ideological opinions.

With the support of the Tagion entity, the plan is to launch an open test network in December 2019 with a developer package to enable developers to build applications on the network, or to run a local copy of the network. The build-out of the network happens continuously and will evolve into a beta network that is expected in Q2 2020, including a beta wallet. From here, the main network will become operational and later the DEX functionality will be added.

The governance mechanisms will be thoroughly tested and adjusted as the network becomes available and testing is possible. The network will slowly start to open up for the community to run their own nodes as the network matures.

The code will start to be open-sourced when the code has been documented and Tagion has resources to support the open-source process for the community. It is expected to be sometime in 2020, latest 2021.

Tagion is planning to scale the organisation to add more resources on core development and scientists on governance and economy, but Tagion is self-funded at the moment, which puts some restrictions on the projects. The aim is to obtain external support and funding in the future from partners that can contribute to the project.
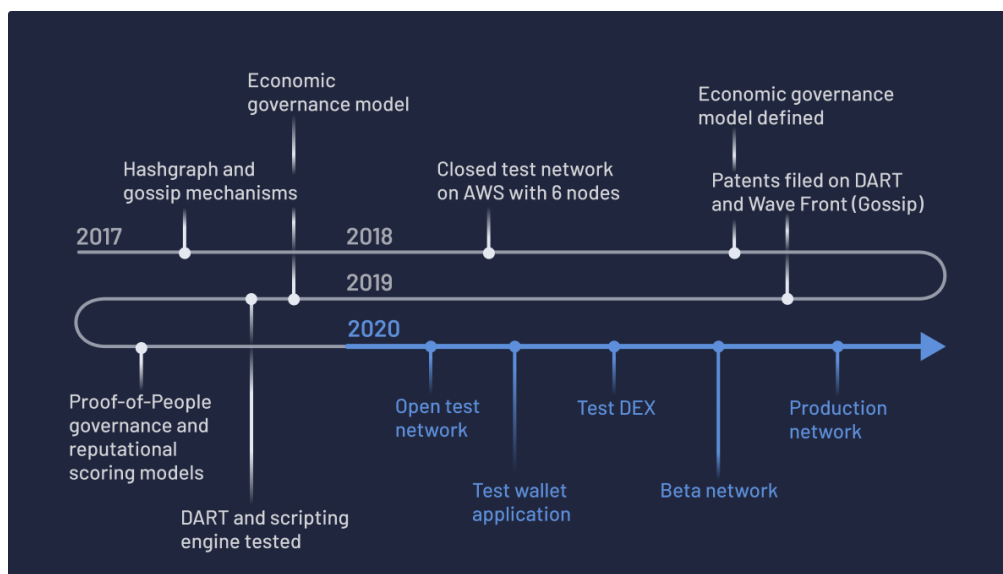
Tagion Entity

To create a genuinely democratic and decentralised monetary system, the team behind Tagion has placed the project in a non-profit company, Tagion.

Tagion entity owns the Tagion™ Trademark, the source-code (until open sourced) and is the legal entity behind the project. Tagion is run by a number of competent guarantors who are tasked to ensure that the right decisions are taken in order to pursue the goal of an economic sustainable world. The direction is formulated in Tagion's purpose, which is to "Fund initiatives that maintain and improve the network, as well as to "initiate, drive, and fund projects that further the adoption of the network".

Founders and core team

Theis Simonsen - *CEO and co-founder*

in https://www.linkedin.com/in/theis-simonsen-32035313/

Theis is an experienced strategist, developer, lecturer and executive. Prior to Tagion, Theis served as a senior consultant at KPMG and an external lecturer at Copenhagen Business School. He has driven and founded other companies as well.

Theis received an M.S. in Information Technology from I.T. University of Copenhagen.

His drive and passion for actually making a difference in the world and democratising the financial system make him a perfect spearhead for Tagion.

Kristian Vestergaard - *CCO and co-founder*

in https://www.linkedin.com/in/kristian-vestergaard-a59b4a/

Kristian brings 20+ years of experience as an engineer, software architect and leader to the team. Having started in an IBM's call centre, he quickly raised to software engineer and analyst before working as an external tutor and consultant for IBM and PwC.

His desire to seek new adventures brought him to audio world leader Jabra serving as a Director, Digital Strategist and Architect in Jabra. His knowledge of the informational structures and business understanding earned him a seat at the GN Netcom board.

In the early days of the Tagion journey, he simultaneously worked as GDPR consultant and Enterprise Architect at the largest power producer in Denmark, Ørsted.

His commitment to the project is best reflected in the sacrifices he has brought to the project by working two jobs to fund not only himself but also four further full-time Tagion team members.

Carsten Bleser Rasmussen - *CTO and co-founder*

in https://www.linkedin.com/in/carsten-bleser-rasmussen-80699915/

Carsten is the technical cornerstone of Tagion and responsible for low-level architecture and core network concepts – with more than 20 years of experience in low-level programming and ASIC design it is hard to find a person more capable of the task.

Before his Tagion days, he was co-founder and CTO at Polaric Semiconductor, specialising in design and engineering of NFC and Bluetooth microchips and leading an international team of over 15 engineers and chip designers. Prior to Polaric, he designed ASIC chips for Nokia.

Carsten received an M.S. in Electromagnetic Field Theory from the Technical University of Denmark.

Carsten has a brilliant ability to combine deep technological understanding with visions for everyday applications. A talent that made him part of the Giga core team. Giga that later was sold to Intel in one of the biggest acquisitions in Danish business history.

Tobias Ambs-Thomsen – *CMO*

in https://www.linkedin.com/in/tambsthomsen/

Tobias has over two decades of experience in visual communication and marketing in a variety of roles in advertising agencies and large companies, including creative lead, and marketing director.

Stirring a marketing department in growth is no strange thing to him. Before he turned to decentralised networks, he was Marketing Director at ACT.Global. A company that during his stay grew from 10 to 70 employees and moved from one to international seven markets as diverse as India, Thailand and Germany.

Tobias has a degree in graphical communication from Danish School of Media and Journalism and is probably one of the few kids that used to swap away from TV-shows in favour for commercial blocks.

In Conclusion

Decentralised monetary systems are on the rise, but the currently available DLT based monetary systems are facing various challenges which hinder mass adoption.

Tagion provides a solution to these challenges through a number of innovations, where to governance and money supply is key. The technology is an enabler of the system.

Tagion is a common good and governed as a common resource. The genuine democratic governance is secured by applying the principle of *one person one node*. Tagion reputational scoring model and proof-of-people protocol incentivises nodes to serve the network loyally. This approach leapfrogs the governance mechanisms in other 'decentralised' systems.

Tagions is a non-collateralized currency of the Tagion monetary system. The money supply is controlled intelligently to create an efficient market, where no central authority controls the supply. Instead, Tagion provides the basis for an algorithm, a kind of decentralised oracle, that controls the money supply by measuring on intrinsic variables to express velocity of money, adoption etc

Tagion's technical innovations include:

- Transactions volume and settlement speed on-pair with credit card systems
- Very low energy footprint
- The DART database, a truly distributed database enabling parallel execution in the network and efficient use of data.
- Use of hashgraph to provide fast consensus and correct (fair) ordering of events; transactions.
- A decentralised exchange, DEX, that allows for full order depth, fair matching and price discovery.

These features make it possible to make both exchanges and transfers fast and at a very low cost enabling microtransaction and giving an edge over current expensive legacy systems.

In summary, Tagion is an alternative to the current state backed monetary systems - the world's first truly non-discriminating democratic peer-to-peer e-money, built for everyday use.

The Tagion Team, October 2019.