



DEMOCRATIZING BLOCKCHAIN AND DISTRIBUTED TECHNOLOGIES WITH
NEW GENERATION SOCIAL NETWORK AND BYZANTINE PROOF-OF-IDENTITY

« Usus magister est optimus »

Practice makes Perfect

Executive Summary

This Goldpaper introduces Optima, the Swiss Altcoin that aims to address the main issue of Blockchain and distributed technologies: its democratization. We will democratize Blockchain and distributed technologies with our new generation Social Network "HARDAH One" and our consensus protocol: The Byzantine Proof-of-Identity (BPI). Optima's vision and goal is to use distributed technologies in the service of Knowledge's global diffusion, thus enabling a better understanding of the world's complexity. Optima has been built on five pillars:

1. Democratizing Blockchain
2. Performance
3. Economic Credibility
4. Regulatory Compliance
5. Swiss Quality

Optima is a new consensus Protocol developed by the swiss startup HARDAH. The company will build a simple wallet and specific use cases as well. Optima is a fast, decentralized, scalable and eco-friendly distributed technology. Optima's ecological footprint is low because there will be no mining involved, and we won't use a blockchain structure but a new distributed one. Optima will be the first cryptocurrency using macroeconomic models to ensure stability and scalability thanks to a Reserve system, transparent Monetary policies and a decentralized and automated inflation control mechanism.

By merging Social Networks and distributed technologies, Optima is one of the only blockchain/distributed technology-based projects considering Blockchain as it should be: a technology and not a product. Optima is not a finality; it's a technology usable directly with HARDAH One. Even if Optima's main goal is to democratize Blockchain and distributed technologies, it is not its only goal. Optima could be used for many other use cases. HARDAH One is an ethical Social Network improving the general knowledge of its user and the quantity and quality of information's sources.

Optima is primarily built to fight fake news and reward users for uploading data and sharing quality content on HARDAH One. Users will be paid in Optima when they are using the app. HARDAH One is the first new generation social network. HARDAH One is a fusion between an image sharing social network like Instagram or Snapchat, and Search engines like Google. Users will be able to share ALL type of contents with HARDAH One: pictures, personal videos, web pages, YouTube videos in a new kind of interface. HARDAH One is the Swiss Army Knife of Social Networks.

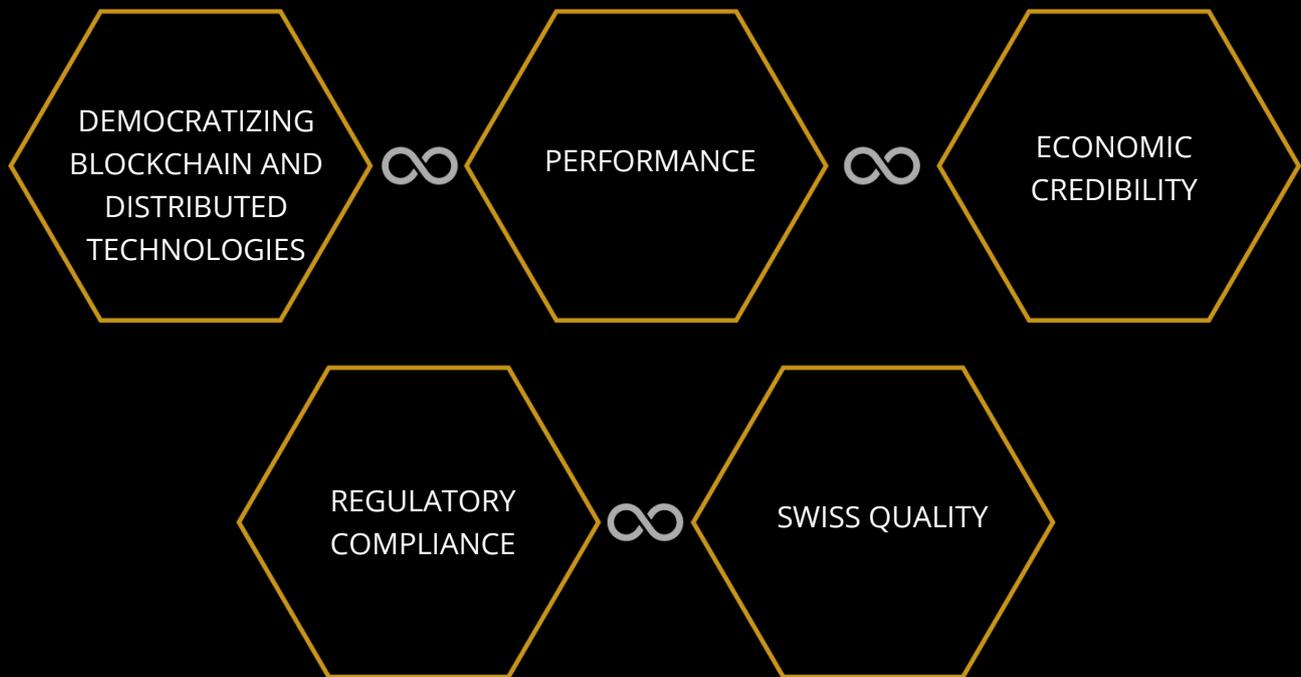
Optima consensus protocol is a mix between Federated Byzantine Agreement (FBA) developed by Stellar, new mathematical algorithms and a double Identity check possible only with our specific use case of social media. This double identity check is called Proof-of-Identity and ensures more trust and security in the distributed ledger. It guarantees regulatory compliance with FINMA's (Swiss Financial Market Surveillance Authority) newly issued guidelines. Optima is then compliant with Anti-Money Laundering laws.

Optima is powered by the Swiss startup HARDAH. HARDAH is not a new entity. It is a Swiss startup founded by David Delmi in 2015 in Geneva. HARDAH is one of the most publicized startups in Switzerland and is active as a constant popularizer of Swiss Innovation and disruptive ecosystems.



OPTIMA
by HARDAH

5 PILLARS



« Usus magister est optimus »

Practice makes Perfect

DEMOCRATIZING BLOCKCHAIN AND DISTRIBUTED TECHNOLOGIES

The main problem with Blockchain is not the low number of transactions per second (TPS) of most cryptocurrencies, is not energy intensive cost even if it is a huge barrier to entry, is not the double-spending, Sybil or 51% attacks. The main issue with Blockchain is that it is still too complicated to create a wallet to exchange currencies. The main issue is the lack of democratization of this technology. Optima aims to change that. This topic of adoption and democratization of innovation was mostly developed in Everett Rogers' Diffusion of Innovations Theory.

Democratizing Blockchain is the core mission of Optima. We will reach mass-adoption of Blockchain if we manage to answer two challenges:

- I. A use case in which Blockchain and cryptocurrencies have a direct use and are compliant with the regulatory framework.
- II. Simplicity: simplify the use and access to Blockchain.

To answer the first challenge, we are creating the perfect use case: our ethical App, the new generation of Social Network: HARDAH One that will use our Blockchain.

To answer the second challenge, we are going to reduce and simplify the steps needed to enter and leave the Blockchain. Our wallet and approach of diffusion of Blockchain are the keys.

HARDAH One is a fusion between pictures Social Network like Instagram or Snapchat, and Browser like Google. It is the Swiss Army Knife of Social Networks. You will be able to share ALL type of contents with HARDAH One: pictures, personal videos, web pages, YouTube videos.

Our distributed technology is going to have a prominent role in HARDAH One. Thanks to Optima we would validate information sources with the distributed technology to identify fake news, their origin and people sharing it. Quality content and trustworthy data will be rewarded by being more visible and shared into HARDAH one. We will reward users of HARDAH One sharing quality content and uploading trustworthy data by paying them with our cryptocurrency Optima too. Each user will gain some Optima when uploading a certain amount of trustworthy data.

In the last part of the first Pillar of the Whitepaper, we talk about a study we have made with Swiss and French journalists about fake news. We talk about our solutions against it in the form of the Delmi-Meienberger Algorithm created by our team.

$$CQI = \frac{\left[\left(\frac{\sum BQI}{\text{Number of Bubbles}} \right) + \text{Median} \right]}{2} * CI * CII * RPI * FNI * Opus$$

CQI = Circle Quality Indicator

BQI = Bubble Quality Indicator

CI = Correlation Indicator

CII = Community Impact Indicator

RPI = Redundancy Penalization Indicator

FNI = Fake News Indicator

The CQI, FNI, and history of each Circle and the Opus (credibility indicator) of each user will all be saved on Optima, on our Blockchain. This allows complete transparency, truthfulness, and accuracy while protecting data privacy.



A. The user is travelling to Rome and take a picture.



B. After taking the picture a Circle is going to appear.



C. User fill the Circle with some content: webpages, pictures, videos related to the Colosseum.



D. On the user profile you only see the first picture like the cover of a book.



E. When you click on the picture, the Circle appears bringing the full experience.



F. Press Play to launch your multimedia Story. Even webpages are going to open inside the Story.

PERFORMANCE

There is in one classification that really matters in distributed technologies. The classification of distributed consensus generations. Traditional Blockchains like Ethereum, Bitcoin and Neo are the first generation of this classification. They are using the well-known blockchain system linking one block after another. The second generation of distributed technologies is the one creating other mathematical solutions than traditional blockchain to ensure decentralization. Hedera is one good example. They are not using a blockchain structure but a Hashgraph structure with a gossip-to-gossip protocol. Iota is another project using a DAG (Direct Acyclic Graph) instead of a Blockchain structure. Stellar might be considered in this generation as well.

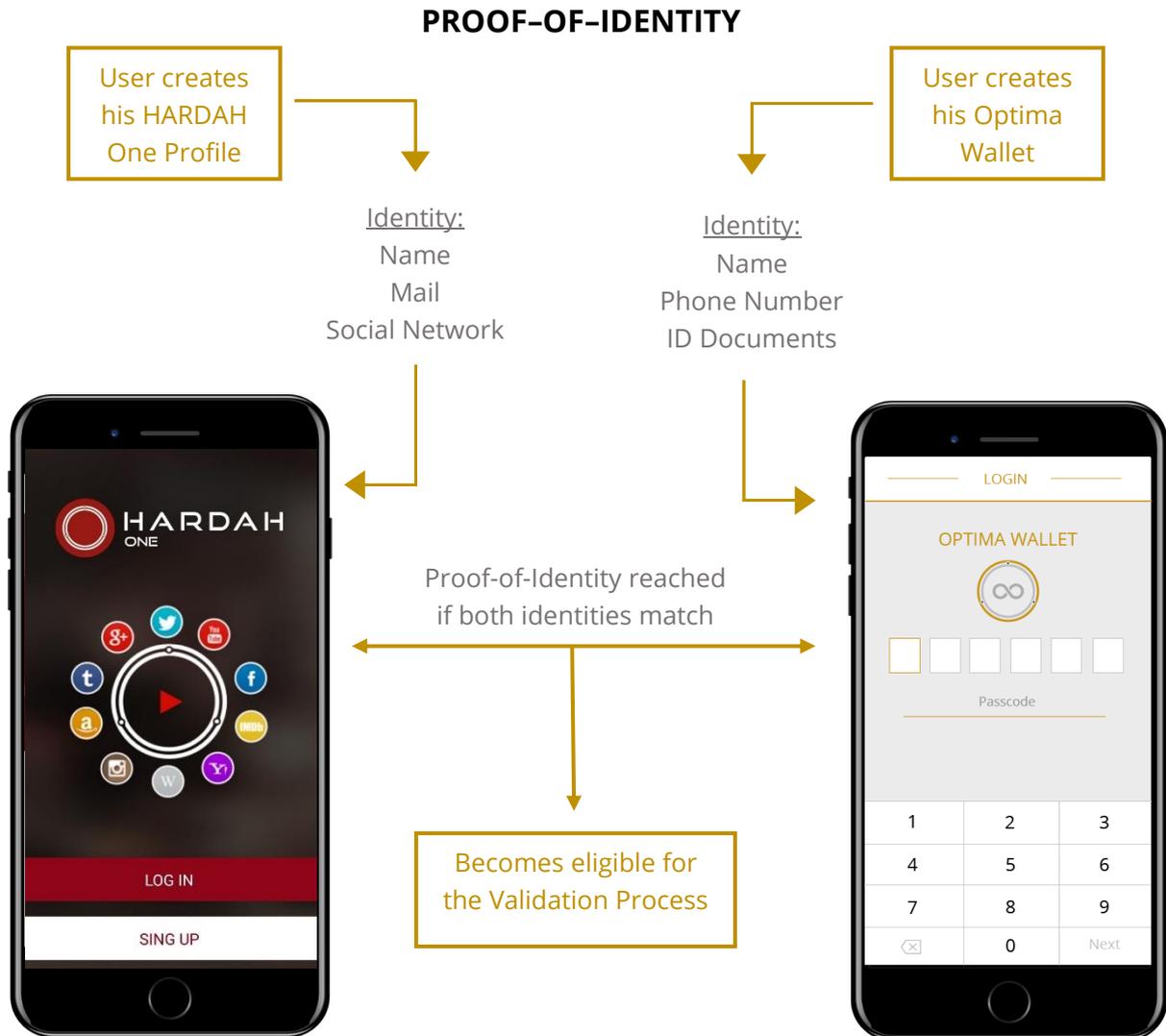
Optima is built by modifying Stellar core and implementing a more regulatory compliant consensus protocol: Byzantine Proof-of-Identity. BPI is roughly a merge between the Federated Byzantine Agreement (FBA) from Stellar and our Proof-of-Identity. Optima has at minima the same block time and TPS features than Stellar. By partially using Stellar's source code, Optima chooses as basis a decentralized Federated Byzantine consensus protocol (consensus that is robust to traitor nodes sending conflicting messages leading to incorrect results) far better than Proof-of-Work (consensus in which people/miners with big computational power have influence) or Proof-of-Stake (consensus in which people owning big stakes in the Blockchain have influence). But this is just the start. We are increasing the Turing completeness of the system too.

	Bitcoin	Ethereum	VISA	Optima (1st step)
Average Transaction Confirmation Time	10-60 minutes	3-5 minutes	Over 24 hours	3 to 5 seconds
Average Transactions Fees (May 2018)	\$2 per transaction	\$0,4 per transaction	1,4% -2,4%	\$0.01 for 300 000 transactions
Transactions per Seconds	7	15	3 500	3 000
Energy per Transaction	850,000 Wh	64,000 Wh	1.69 Wh	0.03 Wh
Co2 Emission per Transaction	416.28 kg	21.08 kg	0.00083 kg	0.000015 kg

In Stellar banking network, nodes can trust anyone because the nodes inside the network are potentially known and checked as real banking institution or *designating trusted participants*. It is not the case on an open Social Network. Validators should have a basic trust based on a decentralized validation approval like in the Stellar Network. We called this basic trust level the Proof-of-Identity.

If we want to use distributed technologies in Social Networks to fight against fake news and to ensure a safe decentralization, we need real known validators. This is the concept of Optima's semi-anonymous system. A user can stay anonymous if he wants but if he does so, he will be in the **Anonymus (Latin for "unknown") Node Pool**, and he won't be eligible as a validator. If he decides to prove his identity with our double identification's system through his Optima Wallet and HARDAH One, he will be an eligible node-validator in the **Probatio (Latin for "proof") Node Pool**.

Actually, the main goal is to create a tech paper describing the new mathematical consensus protocol used in Optima. We plan to create a new generation of distributed ledger architecture going even further than the Hashgraph of Hedera. Creating a new distributed ledger protocol is one of the most valuable activity.



The decentralization is kept because nodes can trust anyone in the validation process after that. Flexibility in designing nodes will be secure and decentralized. The Proof-of-Identity is transparent too. No central entity impacts or decides whether a node succeed his Proof-of-Identity or not. Only a successful algorithm-based match between the user's Wallet identity and the user's HARDAH One identity validate the Proof-of-Identity. When you enter the Probatio Node Pool, each node will have the same power of validation. PoW or PoS can lead to centralization of consensus in the hand of the miners with the biggest computing power or the bigger stakes. It is not the case with Federated Byzantine Agreement used in our Byzantine Proof-of-Identity.

Protocols	Decentralized control	Low latency	Flexible trust	Asymptotic security	Consensus finality	Identity checked
PoW	✓				Probabilistic	
PoS	✓	maybe		maybe	Probabilistic	
Byzantine		✓	✓	✓	Immediate	partially
SCP	✓	✓	✓	✓	Immediate	partially
BPI	✓	✓	✓	✓	Immediate	✓

ECONOMICS CREDIBILITY

Optima has the potential to be a true digital currency and digital asset thanks to its specific use case. If a Social Network used daily by even just one million users were employing and distributing a cryptocurrency, the credibility and trust of this currency would be high.

Money is defined by its three functions: medium of exchange, unit of account and store of value.

The first function of medium of exchange is not reached for cryptocurrencies yet. They are dependent on the voluntary adoption by the market participant. Currently, they are more used as a speculative asset than an exchange medium. We want to change that with Optima. Our Social Network's use case and our macroeconomic strategy aim to encourage exchanges.

The second function of money is as a unit of account and cryptocurrencies have two main issues there. First their volatility, and secondly their high price that results in several decimal unintuitive prices (example: 0.00000356 BTC). Optima answers the volatility issue with our Stability strategy and our direct use case. It is possible to use Optima directly to buy a HARDAH Business account or to pay for advertising on HARDAH One.

To deal with the unintuitive decimal prices, Optima will issue many more coins than Bitcoin or Ethereum, and a few more than Stellar so the price of one Optimum will never be at 10'000 US\$. The idea is to reach parity of 1 US\$ = 1 Optimum.

Finally, the third and last function of money is store of value. The issue with cryptocurrency is that traditional currencies are inflationary. Bitcoin, for example, isn't. There is no inflationary supply for Bitcoin, and this could lead to massive hoarding and decrease of exchanges. Optima answers this issue with our inflationary supply explained in our Scalability strategy. To do so, we can use the quantity theory of money developed by Barro in its model of gold price formation to determine Cryptocurrency price formation.

$$P_t^B = \beta_0 + \beta_1 P_t + \beta_2 Y_t + \beta_3 V_t + \beta_4 b_t + \beta_5 a_t + \beta_6 m_t + \epsilon_t$$

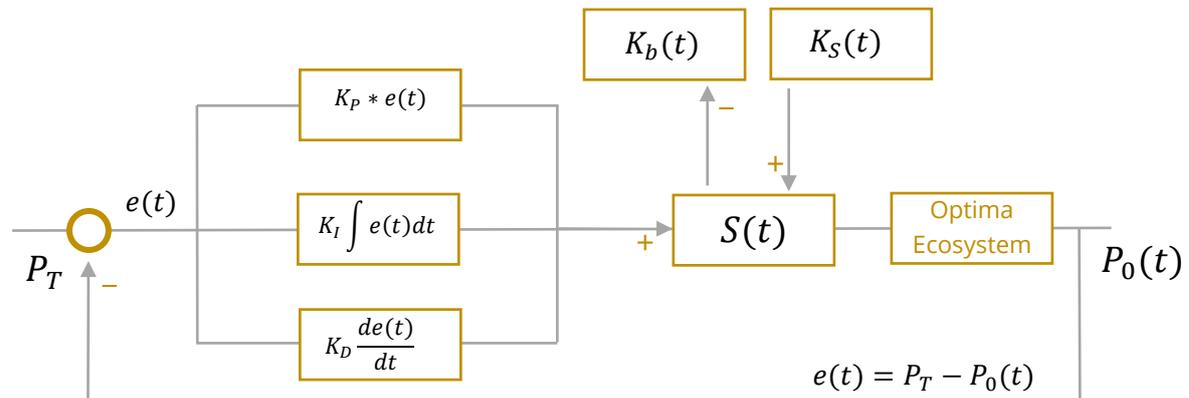
Empirical results show that market forces (mostly b the stock of coins and v its velocity of transactions) have an impact on cryptocurrency price. It could be then explained in a standard economic model of currency price formation. The coin supply (b) being exogenous, the number of coins is then primordial.

Optima protects its users with its Reserve. The Reserve is there to ensure stability and fight against abusive speculations. The only monetary rules will be the one possible in a decentralized system. The Reserve composition will be very risk averse and will serve to do mostly two operations:

- Sell some Optima if the market price is speculating to high so it can stabilize itself and reduce the risk of a Bubble.
- Buy some Optima if the market price is crashing down without clear reasons to protect Optima holders of massive devaluation of the market price.

To do so and to be sure to have a better and efficient impact we will use Forward Guidance.

The main issue with cryptocurrencies scalability perspective on the economic point of view is simple: crypto money deflationist model. Optima is answering this issue with its inflationary supply mechanism filling the Pretium Pool. To keep transparency, the mechanism will be open-source, decentralized and automated thanks to a dynamically set supply via a closed loop feedback control mechanism. This control mechanism is a Proportional-Integral-Derivative (PID) mathematical device controlling the inflationary supply of the Pretium Pool. A transparent and decentralized inflationary supply is then possible to fill the Pretium Pool.



The inflationary supply $S(t)$ is applied based on the equation:

$$S(t) = K_P e(t) + K_I \int e(t) dt + K_D \frac{d}{dt} e(t) + K_S(t) - K_b(t)$$

Based on Facebook's 2017 Q4 quarterly report the average revenue per user (ARPU) of Facebook is \$US 6.18. The annual ARPU is then $6.18 \times 4 \approx 25\$$. The right to claim a part of it is then the reward. On traditional social network, users could have in the best-case scenario 30% or less of this annual individual 25\$. Let's be generous and settle it at 100%, so an annual 25\$ reward per user. This is the global basis reward each user should have based on this best-case scenario. Influencers are being paid in Optima as well for their quality content. Let's say that on person over a thousand is an influencer and that the average revenue per influencer is 20'000 \$US. The Pretium Pool inflationary supply could then be calculated:

$$\text{Inflationary Supply} = \text{Number of user} * 25 + [(0.001 * \text{Number of user}) * 20\,000]$$

We have done some test, and our use case results pointed a 0.9 to 1% inflation rate, thus ensuring the scalability of the mechanism.

REGULATORY COMPLIANCE

The Swiss Financial Market Supervisory Authority (FINMA) was the first national financial supervisor to issue a concrete guideline to ICO's and cryptocurrencies. The FINMA classifies tokens and coins in three categories: Payment Tokens (mostly cryptocurrencies like altcoins), Utility Tokens (provide digital access to an application or service), Asset Tokens (equivalent to equities, derivative or bonds). Based on this classification we think Optima will be considered as a Payment Token.

As seen in the second Pillar of our Federated Byzantine Proof-of-Identity, a double validation process needs to be done to integrate a validator in the Probatio Pool. The double identity check is done on HARDAH One and our Wallet. It will be the first easy-to-use wallet similar to an e-banking app.

We will not issue any tokens before contacting FINMA. Optima wants to develop a strong long-term relationship with FINMA as we value their supervision. Anti-money laundering (AML) laws apply to Payment Token. We will go even further because we want to be compliant with AMLA even during our pre-financing roundtable when Optima are considered as securities. Our lawyers are financial intermediaries and will check and validate the source of each investment. Our unique Federated Byzantine Proof-of-Identity ensures a more trustworthy system. The double identity check helps to fight against money laundering and apply the Know your Customer (KYC) process compatible with AMLA.

SWISS QUALITY

Optima is powered by the Swiss startup HARDAH. We already have three years of existence in Switzerland and Optima is not our first project. HARDAH One and HARDAH Business are two complete and complex tools to code and develop. We have the experience in product launch and innovation. HARDAH wants to position itself as the European innovative digital company offering top notched products and aiming to empower user's digital life.

We launched the first version of HARDAH Business in March 2018 during a special private event at the Tesla Store of Lausanne with politicians, journalists, top executives and important actors of the Swiss innovation ecosystem.

We even made a joint venture with an engineer plastic-to-fuel company, GRT Group, to create EcoPlast. EcoPlast Finance SA has been created to finance the development and construction of the industrial plants using the technology to transform non-recyclable plastic waste into fuel. The company will create EcoPlast, an Optima-based Token (digital asset). This is a concrete use case and a strong joint-venture. And this is Optima's main goal: to spread distributed technologies in a 100% legal, eco-friendly and scalable way into concrete use cases.

HARDAH is not an unknown new entity. It is a Swiss startup founded by David Delmi in 2015 in Geneva. HARDAH is one of the most notable startups in Switzerland (RTS, Bilan, AGEFI, Le Matin Dimanche, startupticker.ch, Couleur 3, Migros Magazine, Léman Bleu, TV5 Monde, 20 Minutes, Bilanz, Handelzeitung, Le Temps, etc.). HARDAH is active as a constant popularizer of Swiss Innovation and Swiss disruptive ecosystems.

David Delmi founded HARDAH in 2015 when he was 21. He is the youngest graduate of an Executive Program of IMD Business School and was awarded as one of the 100 most important Swiss in Digital World. He is specialized in blockchain, digitalization, design, user interface, strategy, entrepreneurship, macroeconomics and business development.