Pitch Deck for R-Company

"Your online, encrypted extension of the mind private space"

"Encrypted Communications that no one can break"

"Censorship Breaking Content Delivery, including BEL"

"Based on encryption that is here to stay"

"Full Vision: Distributed, Remote, Encrypted VDI"

Presentation by Mircea Digulescu
mircea.digulescu@mail.ru

15.10.2024

MAT SOFT

The Problem: What are we talking about?

Online Private Zone

- Your Data is Secure
- Your Data is Accessible
- Your Data is Usable

Collaboration and Communication

- Sharing between Private Zones
- Secure Communications: Email and IMs
- Media and Social Network: Channels

A system that works BEL

- Censorship-free CDN
- Full online anonymity (Tor-like but actually working)

The Problem: What are we talking about? (long term vision)

Just buy a new set of laptops from anywhere in the world and connect “to the hive”

Work via Distributed VDI on remote data anonymously

When done simply wipe or physically pulverize used electronics (laptops)

The Problem: You mean like Azure or AWS?

Not really.

Azure and AWS:

- Are owned by Anglo-saxon elites and serve their interests
- You can be banned from there and censored at any time
*including losing your own data
- They do not support “encryption that works”: by design your data is visible to US gov't and others (5 eyes, etc)
- The above won't change ever
- Azure and AWS can be used by individual vendors as the Infrastructure layer for Storage and Compute

MAT SOFT

The Concept: So what's different?

- "**Encryption that works**" (provided by S-Company)

- **Features** to make data Storable, Usable and Shareable:

* Content Key Change (without decryption), Secret Sharing, Recipient/Sender anonimization, Compute Networks,

- **Features** to enable secure Sharing and Communications:

* Private Key Enlongation, Discovery, Nickname Server (all based on symmetric key crypto), CDN Networks

- **Distributed hosting** to prevent SPF and Censorship

- **Full online anonymity** (Tor-like but working)

- Ultimately: The Distributed VDI

The Competition (VDI): Anyone else doing this?

- Azure Microsoft VDIs

- AWS Workspaces (eg. DevEnv)

- Others will appear (Nutanix Xi Frame, Oracle VDI, Dell EMC VDI,)

Non western: Huawei FusionAccess, H3C Workspace (China), Alibaba Cloud Desktop Service, Tencent Cloud VDI, ZStack Cloud Desktop (China), Vinchin Backup & Recovery for VDI (China), Kylin Cloud Desktop (China), Naver Cloud VDI (South Korea)

Conclusion: Not really focused on privacy, security, censorship breaking, etc.

The Competition (VDI): Can't they veer?

They won't: Neither Microsoft nor Amazon. Nor any other Western controlled or venture backed.

- If you don't pay for the merchandise (or pay menial prices), you ARE the merchandise

- Regulatory barriers: NSA, 'special interest groups', etc.

- Same thing as fearing: Microsoft Windows going Open Source, Facebook becoming decentralized, Reddit becoming censorship free, Banks doing only BitCoin, etc.

The Competition (VDI): What about non-Western vendors?

Chinese, Russian vendors and Musk will compete.

Note: We will not recreate VDI infrastructure or anything. Hosting partners could actually individually use VDI infrastructure from any of these vendors.

Distributed VDIs: So users will work on VDIs, using the special App R-App. The R-App will emulate software and distribute the computation, sourcing, distribution and persistence of data being acted upon. R-App and Host will not see plain-text data. User burner laptop will be used for some crypto stuff and setting up a pipeline circuit.

The Competition: Actual parties

- **Online Private Space**: Tresorit, SpiderOak, Sync.com, Proton Drive, pCloud, iDrive, Backblaze, Acronis Cyber Protect, NordLocker, Veeam

- **Online Private Space (non-Western):** Alibaba Cloud, Tencent Cloud, Baidu Cloud, Mega (New Zealand), ZStack (China), Naver Cloud (South Korea), Cloudike (South Korea), Huawei Cloud (China), UCloud (China), Rakuten Cloud (Japan)

NONE OF THE ABOVE OFFER ACHIEVABLE FUNCTIONALITY

- **Feature deficits:** Airgapped networks support, Censorship Resilient, Fully anonymous. **Means the solutions don't actually work. They just mitigate issues.**

- **Main Issues:** Untrusted cryptographic primitives, Key Exchange over PKI and Certificates, Vendor Trust

- **Other Issues:** Cloud Storage (can be banned by Cloud Provider), Centralized (Single Point of Failure), Not Anonymous, Paywalls, End-User Product (no programmability / customization)

See also the S-Company pitch for details on why **existing cryptography products (all of them!) don't actually work**. Available on https://www.matsoft.ro/Matsoft__Startups62__S-Company_113.html.

The Competition: Actual parties

- **Online Telecommunications**: Musk, Telegram, Discord, WhatsApp (elite controlled), Signal (venture backed), Zoom (venture backed), Microsoft Teams (elite controlled), Slack (venture backed), Google Meet (elite controlled), Cisco Webex (elite controlled), Amazon (elite controlled), BlueJeans by Verizon (elite controlled).

- **Online Telecommunications (non-Western):** WeChat (China), Tencent Meeting (China), LINE (Japan), Viber (Japan, global operations), KakaoTalk (South Korea), JioMeet (India), DingTalk (China), Zalo (Vietnam), ToTok (United Arab Emirates)

NONE OF THE ABOVE ARE TRULY SECURE END TO END

- **Feature deficits:** as per prior slide plus, Anonymous discoverability, No trace communications, etc.
- **Main Issues:** as per prior slide plus, even for China: fear they will share private data with USA.
- **Other Issues:** Centralized (Single Point of Failure), Not Anonymous, End-User Product (no programmability / customization), No secure CDN.

See also the S-Company pitch for details on why **existing cryptography products (all of them!) don't actually work**. Available on https://www.matsoft.ro/Matsoft__Startups62__S-Company_113.html.

MAT SOFT

The Competition

Are really none of the existing Chat solutions really secure end-end!? Why?

- No endpoint security (airgapped or unhackable device)
- **Untrusted cryptographic primitives** (see S-Company Pitch Deck for why)
- **Key exchange over PKI** (no backward / forward security)
- **Centralized (banable) Endpoint** (AWS, etc.)
- **Centralized (banable, censorsable) Storage** (AWS, AliBaba Cloud, etc.)
- **Automatic Updates** (when no Vendor trust)
- **Weak key generation**
- Ultimately: NO CHAT APP WAS RATED RED OR BLACK ON NSA ASSESMENT SCALE (Wikileaks)
* I am not the only one to say this: https://brokencloudstorage.info (non crypto vulnerabilities) Sync, pCloud, Tresorit, Seafile

Really? So there will be no competition? If they don't do it how can we?

- No competition from Western vendors: once upon a time there was WhatsApp.. then there wasn't.
- Chinese, Russian vendors and Musk will compete: data will be accessible to Chinese/Russian govt. Can be partners in some regards, not only competition. Also – Big Market.
- **Can we do it?** Once upon a time there was Telegram. They its founder Pavel Durov got arrested in France. Then there shortly won't be. Mircea Digulescu will not travel to Western block. Nor to drone range.
- Distributed network!

MAT SOFT

The Problem: Full Need

- **Online Private Space**
- **Telecommunications**
- **Distributed VDIs**
- **Content Delivery BELs**

How?

• Endpoint Security (Provided by S-Company)
• Encryption that Works (Provided by S-Company)
•Distributed Secure Protocols: Storage (P2P), CDN, Compute
• Features, Features, Features
• Partner Networks: Storage, Compute, CDN
• Block-chain based gamification / payment (aided by K-Company)
• Block-chain based discovery
• Future: Satellites, Unmanned Bunkers, etc.

MAT SOFT

Client Profile

Individual retail: Journalists, Activists, Scientists, Privacy Enthusiasts, General Public

Individual rich & powerful: non-Tech Billionaires, UHNWIs, some sensitive millionaires, etc.

Private Organizations: Finance UHWN Wealth Management, Private Banking, Crypto Exchanges, Crypto Miners, Private Research Institutions (AI/ML, Biology), maybe Health Networks, Business People, Insurance, Real-estate, Prostitution Networks (where legal), Online Dating, Supply Chain, Payment Institutions (Crypto et al)

Special organizations: Trump, Wagner, Ahmat Sila, irregular Freemasonry.

Public Organizations: Official and Informal Media (Rossyia Segonya), Public Research Bodies, Military Structures, Informal Intelligence, Political Parties

Governments: Russia, China?, Turkmenistan, Kyrgyzstan, Tajikistan, Kazakhstan, Georgia, Azerbaijan, Armenia?, Iran, Syria, Iraq, UAE, Qatar, Afghanistan, North Korea, Venezuela, Cuba, Brazil, El Salvador, Nicaragua, Panama, Bolivia, South Africa, Uganda, Guinea Bissau, Niger, Nigeria, Eritrea, Saudi Arabia, Yemen, Oman, Turkey, Hungary, Slovakia, New Zealand, Mexico

Undesired but generally unavoidable: Western-backed terrorists, child pornographers (under 12 yo), drug dealers, organized crime. Can be mitigated and combated in places, but not prevented without renouncing end-to-end encryption fully. Benefits outweigh costs. No changes nor degradation of security will happen.

UNBREAKABLE ENCRYPTION THAT WORKS IS AN ABSOLUTE HUMAN RIGHT.

No contrary position of any Western-block government will be taken into account.

Development Stages

Phase 0. Blunt online storage + communications over Internet.

Phase 1. Online Backup&Restore (with Secure Key Change, etc.) - secure (AWS/Ali/Azure hosted).

Phase 2. Secure Distributed Backup & Restore (self-hosted, but partners can be invited).

Phase 3. Secure VPN (Tor-like but working): Anonymous Requests / Replies. Indirection (self).

Phase 4. Full online private space.

Phase 5. Sharing and content take-down (DMCA) [note: they have to identify infringing content first (eg. compromise or corrupt an end-user)].

Phase 6. Basic email-like secure communications between endpoints: with Private Requests / Replies: No one knows who sent a message, nor whom it was intended for. Potentially not even who actually could have seen it.

Phase 7. IM-like secure communications between endpoints. Channels. Private Requests / Replies.

Phase 8. Partner-network: Distributed Storage & Communication Providers. (selfhosted/partners)

Phase 9. Block-chain based gamification / payment (K-Chain, see https://www.matsoft.ro/Matsoft__Startups62__K-Company_113.html).

Phase 10. Full launch of distributed private, secure online services suite: For Desktop, Laptop, Mobile.

Phase 11. Gaining CDN and VPN partners: Content delivery BEL (partners do not know what and to whom they are delivering). Own CDN/VPN: Satellites, etc. (different org.)

Phase 12. Distributed VDI basic: remote data, local laptop processing.

Development Stages: Advanced VDI

Phase 13. Distributed VDI intermediate: remote data, remote (single) compute, local laptop interaction. Plain-text data visible locally. (self-hosted: AWS Lambda/Azure F.)

Models: "Give me circuit, I will compute locally", "Give me operation I will get data and give you result (encrypted)".

Phase 14. Distributed VDI advanced: laptop used to set up initial network circuit (topology, pipeline, secrets, etc.). Then all VDI computations except rendering done remotely.

Model: "VDI controller sends operation request to the hive; Hive processes operation gives encrypted result to VDI controller, puts (encrypted results) in distributed memory". So some machines see portion of plain-text data, but they don't really know for whom that plain text data is and where exactly that 32 bit word value fits in running memory. VDI controller does NOT see plain-text data at all. It just controls execution flow (instructions). It does NOT know who processed the op (except that it was authorized to do so). Client laptop processes INTs and some sensitive OPs. (NB: Each operation has type: MUL SUB ADD ROR, INT, etc., data source, data target; actual data is encrypted; machines ask for translation of some encrypted address to their local key, etc.; not all details relieved).

Phase 15. Pseudo-FHE-like Distributed VDI.

Model: Neither VDI controller nor execution machines touch plain-text data. Occasionally machines ask client laptop to trim dimensionality / convert encrypted data to different keys. Finally: Even this step is done remotely. Client laptop just renders and decides OPs like CMPZ. Locally client does NOT store memory data (except video/audio mem). Stores ids, keys, transition keys, [symmetric key] certificates, etc.

Phase 16 [pending future research]. Full FHE-like Distributed VDI (over SKREM FHE not existing).

Model: Client laptop connects to some VDI controller. VDI controller emits SAT/RM circuit to execute based on Client data formulas over plain-text data (circuit equivalence necessary condition). Client approves circuit (can be skipped). Client laptop authorizes (and potentially incentives execution machines to execute VDI controller processing). VDI controller executes SAT/RM circuits over the distributed network. The distributed network itself emits RENDER Ops which the client laptop receives and processes. All data acted upon AND VDI circuit are encrypted. No secrets leaked at all. Remote (encrypted) data does not touch client laptop – it sees just the results of emitted RENDER Ops.

Even more advanced VDI / hive scenarios

- You have **your own online sub-hive** (private encrypted Cloud) that is **autonomous** and **continuously running**
  - Kept up by **occasional cryptocurrency injections** from you (operated via some burner laptop)
  - Ultimately it can even make (earn) its own crypto (your own hive) thus ensuring longer even financial autonomy (pay for its own gas). Example: Offering online services.

- You **only occasionally connect to the hive** (via some burner laptop) to:
  - Refresh execution network circuits: given symmetric key nature of SKREM, created authorizations will be spent and need recreation. This step can be semi-automatic, but ultimately if you are to retain personal control, once in a while you need to reauthorize / refresh everything.
  - Download content / network product. Exemples: New crypto wallet private keys (for an automatic miner hive), Trained AI model (for a hive AI/ML trainer), private data/communications (Borg-like sync with "the hive").
  - Recycle content keys / re-upload censored (eg. DMCA mechanism abuse) content with new keys.
  - Backup / Replicate important content (potentially over a separate hive / with different keys).

- **Your sub-hive can interact with other independent sub-hives**. Examples: Cross-border commerce between large actors. Financial Clearing. G2C services at scale. Inter-govt sync: military ops, intelligence ops, central bank clearings, etc.

MAT SOFT

Network Evolution

Stage 0. Everything self hosted (meaning on AWS/Azure/Ali)

Stage 1. Everything self hosted but distributed (independent nodes can be added in principle)

Stage 2. Distributed but owned exclusively by R-Company (self hosted in various availability zones)

Stage 3. Discoverability and Sync operations over some existing BlockChain like BTC.

Stage 4. Some external partners availability zone agnostic (over Internet): mainly BTC miners, other Crypto exchange operators, etc.

Stage 5. Some partners for Storage in critical availability zones: Russia, China, North Korea?, Vietnam, New Zealand, UAE, Armenia, Georgia, Turkey, Cyprus, Uganda, Niger, Netherlands, Bolivia, Venezuela, Mexico. Eg. 5-of-7 secret sharing (7 splits, 5 required).

Stage 6. More & more CDN/VPN partners for all 6 continents +Oceania.

Stage 7. More and more sophisticated partners and own capabilities for storage and CDN/VPN/Crypto services: LEO Musk like satellites, GEO satellites (with self-wipe on proximity/panic heartbeat failure), Stratospheric Drones, Low Altitude Drone Swarms, Bunkers, Covert Private Networks, etc.

Stage 8. More and more compute / VDI partners as per Stage 5-7 above.

MAT SOFT

Projected Company Value (rough own estimates)

Up to **Phase 7**, up to **Stage 3**, **no gov't** clients: **$1-10 Billion**.
Up to **Phase 12**, up to **Stage 6**, **no gov't** clients: **$10-50 Billion**.
Up to **Phase hive**, up to **Stage 8**, **no gov't** clients: **~$100 Billion**.

Up to **Phase 7**, up to **Stage 3**, **with gov't** clients: **$10-50 Billion**.
Up to **Phase 12**, up to **Stage 6**, **with gov't** clients: **~$100 Billion**.
Up to **Phase hive**, up to **Stage 8**, **with gov't** clients: >**$1 Trillion**.*
(essentially replacing home workstations with the hive)

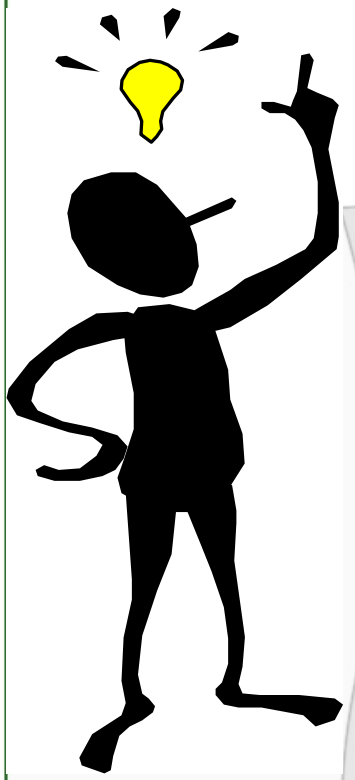
Note: There exist ample non-technical risks: including life threats to founder Mircea Digulescu, etc. Completion of R-Company up to hive phase is by no means guaranteed.

Your capital is at risk. This is not investment advice.

Consider any money spent/invested/donated as 100% lost. There are no refunds.

MAT SOFT

R-Company: Why raise capital?

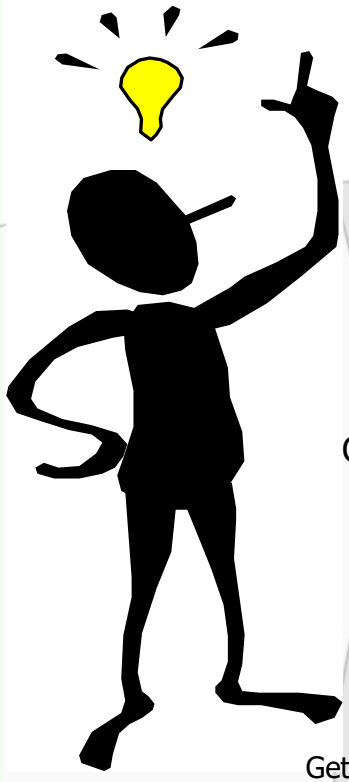


In a nutshell:

- I need money for **development team**, even for Phases 0-7
- I could do it myself but **bootstrapping would be very very slow**
- There is clearly a first-mover advantage here. **TTM is valuable**.
- I need **money for hosting** (operations): AWS/Azure is not free.
- I need **money for promotion** (advertising, events, etc.)
- I need **money to get initial partners** (Storage, CDN/VPN) for Stages 4-8.
- I need yet **more money for development** for Phases 8-hive.
- I need **money for soft roles**: recruiters, psychologists, managers, etc.
- I need yet more money for **promotion and branding** for Phases 8+
- I need yet more money for **Sales costs** to court and get govt clients.
- I need money to **ensure safe harbor** for myself (founder), team and some partners: **political and financial costs**. **Security costs**.
- No hiding: **I want to actualize some of the benefits**. I want to start living well-off TODAY, not in 10-20 years when R-Company gets valued at $1 Trillion. I am already 39 years old.

MAT SOFT

R-Company Financials



Seed Investment: $10 million.

Covers setup, some initial team. Demonstrate ability to function towards Phase 7, Stage 3 and maybe complete Phase 3, Stage 2 fully.
Should take 1-2 years. I will take $1.2 million per year myself.

Series A: $30-50 million.

Covers basically everything up to Phase 7, Stage 3. Demonstrate a clear capacity to continue towards Phase 12. Should take 2-3 years. Might include acquisitions. I will take ~$2-3 million per year myself.

> around end of Series A / start of series B first users / paying customers appear <

Series B: $50-100 million.

Covers basically everything up to Phase 12, Stage 6. Grow the partner network, promote aggressively, establish partnerships, networks, etc. Will include some acquisitions. Regular paying customers should appear / wide base of nonpaying users. Should take 3-5 years. I will take $3-5 million per annum myself.

Series C / public / bonds: ~$100 million

Grows the network further. Ensures political and technical stability. Develop Phases 13-15 and hive.

Get to Stage 8. Grow customer base. Start intense monetization. Get profit. Get more profit. Rip benefits!

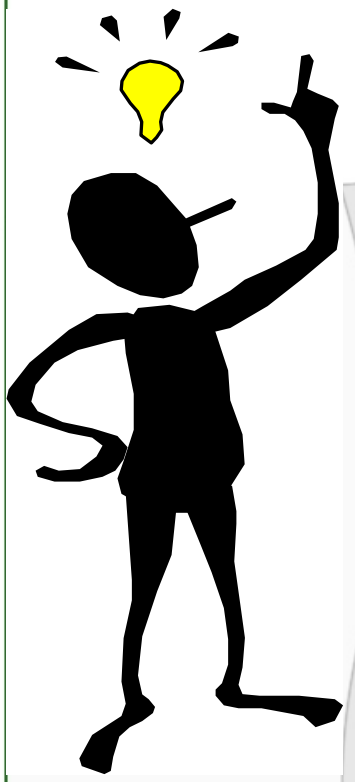
MAT SOFT

R-Company

Can we really? Yes, we can.

- Scientific Questions answered for all Phases 0-15. Engineering largely clear also (at least that it is feasible)

- Partnerships and commercial-"political" plan feasible



Why didn't others do it already then?

- Because they don't want to / can't [western regulations]

- Because the older ciphers are just now becoming obsolete

- Because doing something like this is not easy.
Pavel Durov can do it. Tourist / Peter can do it (maybe). Snowden could not do it. Steve Balmer could not do it. Maybe another 5-15 people worldwide have the skill set and context (technical, scientific, entrepreneurial, determination, etc.) to realistically attempt something like this. This is not WhatsApp.

Interdependencies

- R-Company relies on technology from S-Company.

- R-Company uses K-Company's K-Chain for gamification and monetization.

- Both S- and K- Companies have independent monetization and investment plans.

- Both S- and K- companies need to advance (can be in parallel) not full ideal product.

R-Company

It MIGHT get it done anyway, but without investment unlikely: don't wait until it is more advanced "to invest only then". You will be missing out or if no one invests (unlikely), R-Company might not happen at all. Investors reasonably approached at an early stage perceived to be unreasonably declining us, will not be reached out to again at later stages. I am selling risk, not certainty. You as investors, you have the money and can afford to pay for the risk, not me.

Disclaimer: Neither investment/donation/advance buy is any 100% guarantee anything will get done. I might get killed, married, embedded in some non-Western structure, etc. However, getting money exponentially increases the probability at least SOMETHING will get done. Nothing in this presentation is nor should it be regarded as investment advice. Your capital is at risk. Only donate/invest/advance buy amounts you can risk and which you consider are lost forever when sent. Donate only for appreciation of myself, not as an investment nor advance buy. Advance buy presents risks the product might never occur. There are no refunds.

Note: The above is mainly to deal with hostile investors/donors/buyers - like groups and people actually seeking to have product NOT become a reality. But it is not only for that purpose, so please read, acknowledge abide by it.

R-Company Team Plans

Team Plans with money:

- Mircea Digulescu: CTO (science stuff, work breakdown, code review, guidance and specs, leadership) and CEO (vetting people, company initial culture and tonus, company direction) initially.
- About **3, 5, 15 senior software engineers** backend (1-2 DevOps), **1, 3, 5 frontend / mobile** (Seed, Round A, B).
- About **$5, $30 million in acquisitions** are envisioned (Round A, B).

- Soft hands (up to end of Round B):
1-2 psychologists, 1-2 recruiters (except externalized), 2-3 soft. delivery managers.

- Marketing (up to end of Round B):
2 community manager (marketing and tech), 1-2 other marketing folks, lots of externalization

- Legal (up to end of Round B):
1 internal jurist, lots of externalization

- Glue roles and investor relations: 1 office manager, 2 office assistants, 1-2 economist (investor relations)
- Upper management: Mircea Digulescu retains full control, but by Round B late, day to day leadership taken over by someone else as CEO (Mircea will do other more valuable things).
- About **$0.5, $1, $10 million spent on academic partners** (University partners) (Seed, Round A, B).
- **Physical security** expenditures (externalized): Armed taxi, Armed security for events, critical leadership

R-Company Team Plans

Team Plans with money:

"Plans are approximate"

"A good plan today is better than a perfect plan tomorrow"

"The battle field will tell the exact plan"

"Founders underestimate their needs 10x"
(with careful financial controls, I think 1-2x should suffice here)

Some spending can be related
to political and financial stability of company (even Seed-Round B)

Investors could also provide some political and network support, but this is not strictly required

The Founder: Introducing Mircea Digulescu

Mircea Digulescu is a Leader, an Anti-imperialistic Libertarian Social Activist, an Independent Entrepreneur, Computer Science Researcher, Software Engineer, Military and Intelligence Enthusiast and Amateur Writer.

- See https://www.matsoft.ro/ for details on him in all these regards.
- Did found a $1.5 million company MAT SOFT TECHNOLOGY in 2009 (raised $300k from 3F) and later sold it in 2014.
- Speaks Russian, English and German fluently.
- Activist, politically opiniated and activist: libertarian ("good 1789 communist").
- Published peer-reviewed papers in Computer Science: https://www.matsoft.ro/Matsoft__Research62__Computer_Science_113.html.
- PhD (ABD - All but Dissertation) in Applied Computer Science from FMI UniBuc Bucharest.
- Professional Diploma in Management and B820 - International Strategy from OUBS (Milton Keynes).
- Lobachevky SU (1 semester, 2019), Nizhny Novgorod.
- Accepted but did not attend: SKOLKOVO Moscow School of Management (2013) and Cornell University (2004).

MAT SOFT

The Founder: Introducing Mircea Digulescu

Reached Div1 Coder on Codeforces.com (2022 max score): profile mircea85.

Built up Bolt.eu (Taxify)'s Bucharest Software Engineering office 2018/19 with Google experienced SSEs.

Had leadership roles (Team Lead, Manager)

Did presales.

Did very briefly LATOKEN crypto.

Socializes with diplomats and state bodies (Russia, China, Venezuela, Iran) and has political activity.

Was guest of Bolivarian Government in 2020 and promoted political speech in Caracas.

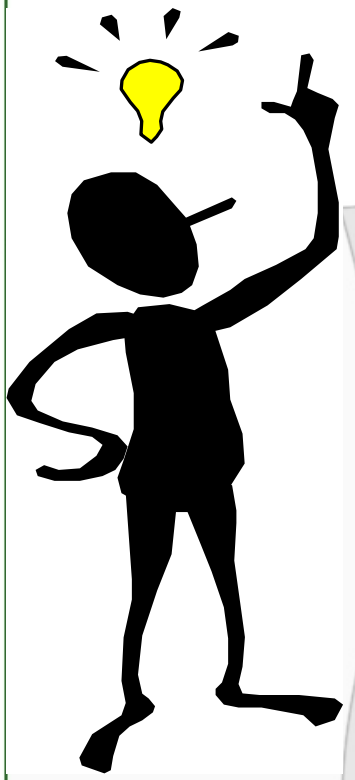
Is frequently visited by security services from across.. when they learn about his whereabouts

Was visited by CIA and whole of AUKUS in Germany in 2022.

Got Assanged 2 days later and barely managed to escape with his life and unharmed in 2023. Barely, but did manage, so he is "alive and kicking" and will even more vigorously complete his projects.

MAT SOFT

R-Company: The Deal



- How do you get it? For Seed Round, ~3-5% of the company.

- I aim to garner a joint commitment for both Seed + Round A (if Seed goes OK). So investor set should commit to Round A financing, but they can stop the involvement after Seed in case it doesn't progress enough in the 1-2 years allotted (but NOT if they had a change of heart, other opportunities arose for them, are having second thoughts, etc.). Ideally for the entire Seed+Round A+B+[C].

- Up to end of Round B, I plan to put up around 10-20% of the company for investors.

- For Round C and beyond, up to 25-33% total (so another 5-13%), at higher valuation.

- I plan about 10-15% for staff equity share

- I will retain complete control of the company until after Round C. Agreements that initial investors can't block capital events will be in place. I will also retain 51% of it for myself until end of Round C. For safety, IP and brand will be co-owned by myself and the company.

- Where does of the R-Company juridical entity reside (appropriable):

  * Brand, Relationship network (Partners), IP (Code), IP (Patents/Know-how), Client Base, Reputation, First-Mover (ie. Early Mover), Architecture Relationships (Govt, Academia).

  * Software R&D Company in Cryptography, Telecommunications and Virtualization

R-Company: The Deal

- What WON'T you get for the $10-$250 million?

  * I will not give control of the company/entity to you. I will ensure legalize protects my IP, brand, etc.

  * I will not introduce backdoors

  * I will not politicize operations nor focus on monetization before end of Round C (Phase 15/hive)

  * I will not abandon the idea nor its implementation

  * I will not give brand to you

- Anything else?

* R-Company can easily become bigger than StarLink / Telegram / etc. In part it expands Pavel Durov's potential initial vision. Unfortunately he will no longer be able to materialize it (Western arrest trap).

* K-Company will maintain the K-Chain. This chain will be designed so that it gives some value to the founder's address (me). Some benefits can be shared with K-Company stakeholders.

* Both R- and K- companies are possible once S-Company is a (near) reality. So S-Company investment investment/donation should be in place. Taken together, the S-, K-, R-, E- and F- Companies, and thus the M-Company holding group definitely have the potential to become yet another major corporation, bigger than Uber, with major tech ramifications. This means $1 trillion dollar company, yeah.. and of all the most valuable is R-Company. Warning: It can also all just fizzle miserably, so your capital is at risk. Consider anything sent/invested/donated/paid as certain losses. This is not investment advice.

* Investor advice and involvement is both sought and desired: full control does not mean unilateral, rash or emotional decision by myself: sovietsky soyuz (we advice each other and listen to one another).

MAT SOFT

Conclusions: R-Company in brief

- Solves a real problem (full e2e encryption): something others won't / can't.
- Leverages technical innovations by Mircea Digulescu: SKREM-like ciphers and their applications, security and web protocols, etc.
- Will be worth and valued at like $100 billion – $2 Trillion when successful
- Offers strategic advantage to its controller
- Gov't relevance ensures political backing for its controller

The Deal

1. You invest/buy/donate about $10-50 million upfront, for Seed, Round A. In ~3-4 years, another $50-$100 million raised for Round B (preferably also from initial investors committing), and ~5 years later another ~$100 million for Round C.
2. In circa 7 years the project has its moment of truth. In circa 9-12 years project is complete and the ripping of benefits enters full scale mode.
3. In circa 10-15 years exit opportunities and valuations of >$100 billion. Potentially >$1 Trillion or more.
4. Can also fail miserably. Your capital is at risk. Consider any money donated/sent/invested as full lost. There are no refunds. This is not investment advice.

110 over 70

Regarding any 110/70 questions on Mircea Digulescu:

- My blood pressure is 120 over 60.

MAT SOFT

Thanks for your consideration!

Contact Mircea Digulescu now at mircea.digulescu@mail.ru or via WhatsApp/Telegram/Viber at +40736.617.391, for investment, donations, technical details or anything!

Please consider Donating. It will be great if, instead of boot-strapping, support from smart donations such as by yourself could be leveraged. Please see **Contact Mircea** to donate: BTC and fiat transfers in RUB are accepted. A BTC donation of 100-200 USD will mean a lot to him and his activism. Especially if you were able to repeat the gesture once in a while.

To donate in use the following BTC address: **bc1qtgt8ctz3ffd95dwxux3wed6nlq3r5mhhzg98zp**.

bc1qtgt8ctz3ffd95dwxux3wed6nlq3r
5mhhzg98zp

To donate in RUB use the following MIR card number: **2202 2023 9828 3287**.

To donate in any other currency, please use an online service such as Telegram Wallet, Binance or others or make use of an offline exchange or BTC ATM machine, like for example cryptoatm.ro to donate in BTC to the address above.