TRUSTLESS.AI

Website:
www.trustless.ai

Product Video: Play

Incorporation: Luxembourg.

Locations: Berlin, Rome.

Stage: €150K and 12 weeks away from 8 fully-functional mockup prototypes as seen on video.

Funding to date: €150K in cash and 6 man-year, by cofounders.

Customers: Pilot & channels agreements being discussed.

Legal Counsels: George Frost, Laurent Schummer

Funding sought: €250-600K pre-seed.

Contacts:
Rufo Guerreschi, CEO
rufo@trustless.ai
+39 3357545620

COMPANY PROFILE

An Open Ultra-Secure Computing Universe for Sensitive Communications and Transactions

MISSION

We have been on a lifetime quest to advance civil freedoms and democracy in the digital age. We aim to restore the pre-digital balance between the **public sphere** - of streets and squares - and the **private sphere** - of homes and free citizens' association. We believe this to be crucial to defend and advance liberties and democracy, and later provide the basis of trustworthy AI systems.

WHAT

At TRUSTLESS.AI, we are building a new ultra-secure computing ecosystem, called **CivicNet**, designed to **seamlessly deliver radically-unprecedented confidentiality and integrity** to the most sensitive communications, negotiations, e-banking and cryptocurrency transactions of high-profile enterprises and persons; while at once solidly enabling offline, lawful and legitimate criminal investigations.

SOLUTION

CivicNet provides security through an **uncompromising transparent, democratic and economically-efficient ecosystem**, built from existing time-proven open high-assurance technologies. The endpoints and center of our trustless CivicNet ecosystem are our **CivicPods.** These standalone **2mm-thin touch-screen computing devices** will be attached to the back of any phone - adding 1mm to the average case - or within a dedicated leather wallet. Through a unique form factor and minimal features, our CivicPod enables a seamless user experience that is much **faster than today's smartphones**. CivicNet members *produce* cybersecurity by operating our CivicNodes, which run **ultra-secure anonymization nodes and blockchain nodes**. These nodes are embedded in docking stations (CivicDocks) that connect the CivicPods to the users' desktop monitor for long-form text editing.

CIVICCHAIN - OUR BLOCKCHAIN BACKEND

By the time CivicPod will go to market, at least 1000 CivicNodes will be running to constitute the **CivicChain**. These nodes will be made of the same **ultra-secure low-level hardware and software stacks** of the CivicPods. These will provide very high **authenticity** of the person actually controlling the node. Nodes will be running on a to-be-determined **time-proven and/or industry-validated blockchain platform** (e.g. Hyperledger, Tendermint) within its closed network. Core software and dApps will be certified by the independent **Trustless Computing Certification Body**.

CivicChain aims to deliver a blockchain base platform for decentralized applications that features levels of integrity and confidentiality of data, and **compliance to AML/KYC,** that are substantially or radically higher

than other leading and emerging blockchains. CivicChain will also enhance the integrity, immutability and availability of sensitive data and logs of CivicNet service. (2-minute CivicNet product video).

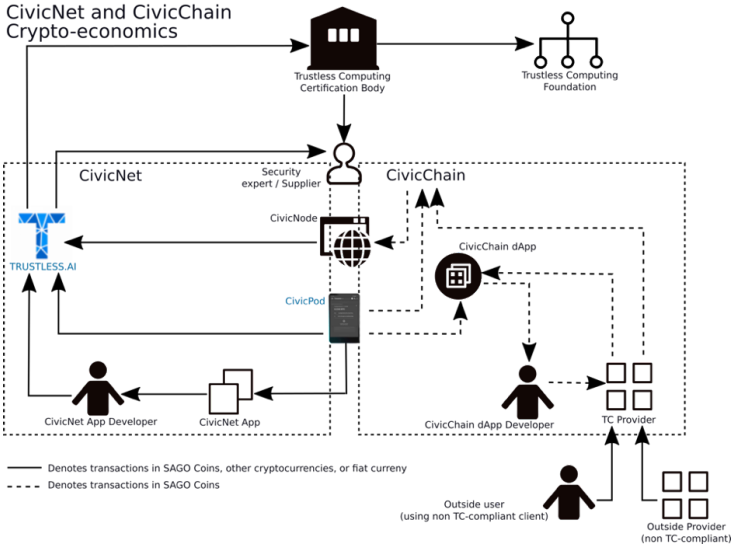
PROBLEM TO BE SOLVED

Whatever price high-profile executives or persons are willing to pay, there is no device available in the market today, that provides evidence of protection from even mid-level cybercriminals. Their attempts to mitigate espionage by competitors, financial fraud, and blackmail are largely unsuccessful; and often result in additional costs in the form of unwanted travel, self-censorship and missed business and social opportunities. While private cybersecurity spending has grown 30 times in the last 10 years to **€120 billions**, cybercrime cost will hit forecasted **€6 trillions** by 2021, with an average of **€17 million for an average enterprise**. This gap is proof to a huge unmet demand.

UNIQUE COMPETITIVE ADVANTAGE

We reconceptualize **cybersecurity as a cyber-social governance problem**: as the by-product of the intrinsic resilience, accountability, and competency of organizational processes. Therefore, all software, hardware and processes that are *critically*-involved in the lifecycle and supply chain must be:

- (1) **publicly inspectable** in their source designs;
- (2) subject to extreme expert and ethical **security review relative to complexity**;
- (3) subject to **extremely resilient oversight** based on citizen-witness or citizen-jury-like processes.



These requirements will be assessed for compliance by the independent **Trustless Computing Certification Body** (TCCB). In fact, ultimately, the "buck" of IT trustworthiness stops at the **technical-proficiency, independence and accountability and altruism** of the certification body. Maximization of these requirements will include an innovative concept of "*continuous democracy*" that merges direct, deliberative and representative democracy, and embeds *re-constituent* dynamics to mitigate long-term governance distorsions. TCCB will be with eIDAS ISO/IEC Standard compliant, and aims to become a schema of the new E*U Cybersecurity Certification Framework*. Though it is not required by law, these same paradigms are applied to offline lawful access processes overseens and managed by TCCB, to prevent CivicNet from criminal abuse. The TCCB has been promoted since 2015 by our Trustless Computing Association - and its public and private partners aiming to provide R&D initiatives and our *Free and Safe in Cyberspace* global event series, last held in Berlin on May 4th 2018.

BUSINESS MODEL & SCALEUP

CivicNet will be offered as a *hardware-as-a-service* through **banks and telecom channel partners**. Main target segments will be privacy-sensitive individuals or enterprises that lease 15-500 units.

Once market proven as endpoint security leader - with our first batch of 10.000 units - we will then leverage our open-source IP regime, through low royalty costs and a uniquely resistant ecosystem and certification governance model to:

1. become the **World's first ultra-secure enterprise and consumer computing platform**, via an increase in apps, a reduction in price, and by embedding the CivicPod as default *ultra-secure smart backscreen* on **tens of millions of enterprise Android smartphones**, and

2. become the **standard *"root-of-trust"* for the most privacy-sensitive or safety-critical AI and cyber-physical systems.**

MILESTONES

- We are **3 months and €150K away from finishing 8 fully-functional prototypes** of our CivicPod and CivicDock, ready for demos and functional pilots to pilot clients, channels, and investors. We have relationship with leading US and EU VCs, and token sale fundraising partners since 2017.
- So far, we've invested cumulatively 7 man-years for a total of €450K in sweat equity and €150K in cash. We have put together 70% of the software and hardware technology, 80% of the user experience design. Most crucially, we have 90% of software & hardware architecture, **100% of the security-critical supply-chain** and technology partners, with over 130 pages of architectural, business, governance, feasibility and specifications; and conditional binding agreements for licensing, patenting and non-compete.
- Since 2015, we are on our way to position the proposed *Trustless Computing Certification Body,* our *Trustless Computing Paradigms*, as the **leading new paradigms for endpoint IT security,** through our *Free and Safe in Cyberspace* event series (Brussels, Brazil, New York, Brussels, last in Berlin on May 4th 2018).

FUNDRAISING

Since end of May, we opened our 1st round for **€250-600K** via an equity sale at €6M pre-money valuation. This will enable us to complete 8 fully-functional device mockup prototypes in 3 months, formalize pilot client and channel agreements, establish our narrative, and deepen our technical plans.
Our 2nd round will raise **€5-6M** in equity (and a possible large token sale) in late 2018 or early 2019. This will enable us to go to market 15-18 months later with 10.000 Pod/Dock device pairs, and break even in 9 months.

TRACTION

Over the last 15 months, we **received interest, positive feedback and active engagement** from high-profile prospective pilot clients and channel partners for our B2B2B and B2B2C offering, especially **banking** sector channel partners. Among them: Banks in Luxembourg and Germany, Telecoms in Germany and France, some high-profile non-tech corporations, and the German Armed Forces Cyber Innovation Hub. We've held off proposing formal pilot or channel client agreements, preferring to wait for the closing of our 1st round, and finalization of our mockup CivicPod prototypes. Both were delayed by time-consuming explorations of token sale and ICO scenarios, which however remains an option for our 2nd fundraising event.

COFOUNDERS

Rufo Guerreschi*, Cofounder & CEO*. Created the Trustless Computing Association, with world-class partners and advisors. Founded and exited an e-democracy startup, ParTecs. Launched a leading-edge global event series, Free and Safe in Cyberspace. Brought the valuation of a planned EU's 2nd largest tech/IT park from €3M to €21M. Sold a +€10M java mobile app store system to Telefonica. (*LinkedIn*)

Roberto Gallo*, Cofounder & Security Architecture Lead.* He designed: (a) the world's 1st secure CPU inspectable in HW & SW designs, deployed since 2014; (b) the security architecture of 400,000 Brazilian voting machines (c) the ASI-HSM of the Brazilian PKI-root CA. He built Kryptus in a 50-strong leader of HW security in LatAm. (*LinkedIn*).

Quirin Blendl*, Cofounder & Head of Business Development.* Berlin-based cybersecurity policy and market expert. Director Cybersecurity and Digital Policy for Germany's Association of Technical Inspection Associations; Formerly: Senior Manager for Cyber Security and Data Economy at the Federation of

German Industries (BDI); Analyst at the German Council on Foreign Relations. (non-public till closing of round).(Linkedin)

Joonyoung Park. *Cofounder &* EVP *Engineering.* Led 30-staff team in Palo Alto at Kudelski, a global leader in IPTV and cybersecurity, for the design of new devices concept-to-manufacturing. Co-managed and exited in 2018 JRC, a family-owned 200M€/yr 7-sigma electronics manufacturing plant (EMS) in South Korea. Was Chief of Engineering Staff for B2B Solution Development at LG Solutions. Was Principal Staff System Engineer at Motorola. (Linkedin)

Udit Dhawan*, Cofounder & Endpoint Security Lead*. Formerly senior research scientist at Intel Labs, Technical Lead at Samsung R&D in Bangalore. Formerly, Lead Student Architect for 3 years on the US DoD DARPA CRASH/SAFE project, aimed at a clean-slate co-design of the entire computing stack for secure computation. (LinkedIn)

As spin-off of the *Trustless Computing Association*, we have aggregated a strong complementary team of cofounders, supported by a **unique global community of advisors and technical partners** of the Association, with globally-rare expertise in open-licensed high-assurance IT, along the entire supply chain.

WHY WE ARE MOVING TO BERLIN/GERMANY

- Graduated from **Berlin-based Hardware.co 2016 acceleration program**, hosted by Deutsche Bahn and Bosch.
- Three of our technical partners are German companies: **KernKonzept**, **DFKI** and **Lfoundry**.
- Great pool of relevant IT security talents in Berlin and attention to digital privacy.
- Many tech-savvy and security-conscious prospective channel partners and enterprise customers.
- Ongoing interest from Berlin-based leading VCs and angels.
- Of the cofounders, Quirin is Berlin-based while Rufo, Roberto and Riccardo are ready to move there at the closing of Seed round. Rufo's daughters attend German school in Rome since kindergarten.
- Multiple preliminary discussions with one of the top 2 German teletelcos, and one of the top 2 German banks, for strategic or channel partnerships.
- **German Armed Forces** Cyber Innovation Hub requested a 200K€ proof-of-concept proposal for a dual-use version of CivicPod and TCCB, currently being assessed.
- German Ministry of Interior, German Armed Forces and Deutsche Telekom, among others, participated to our last public event in Berlin on May 4th 2018 to discuss our *Trustless Computing Paradigms* and *Trustless Computing Certification Body*.

ROADMAP

07/2018 - Closed a €250-600K equity fundraise.
09/2018 - Engaged in 18+ target pilot/channel partners for market validation, and sign 2-3 LoIs.
09/2018 - Widened partners & consensus on Certification Body & new Manifesto/Position Paper.
10/2018 - Finalized 8 initial CivicPod functional mockup prototypes, with complete physical, UI and UX look and feel (South Korea/Belrin) for €95-110K.
10/2018 - Closed 300-600M€ fundraise, via "rolling close" (possibly in part through crowdfunding portal, e.g. Companisto, Seedrs).
11/2018 - Engaged pilot and channel partners in: several "lean process" product iterations, user acceptance and usability tests. Market validation analysis. Produce a video with actors and physical devices.
12/2018 - Signed 3-4 Pilot Purchase Agreements (some w/advance payment) with target customers, and LoI with prospective channel partners (banks or telco).
Q1/2019 - Closed a €5-6M equity sale (possibly via a 25M€+ token sale, e.g. "ICO").