

WHITE PAPER

NEXT GENERATION OF SMART HOME



MARKET CONTEXT
Growing need for IoT solutions



PROBLEM & SOLUTION #1: SECURITY Inability to take over IoT devices thanks to the interactions via smart contracts



PROBLEM & SOLUTION #2: INTEROPERABILITY High degree of integration via VeCap adapter and Central Module



PRODUCTVeCap solution for smart homes and smart offices



TECHNOLOGYHow exactly VeCap will work



VECAP BLOCKCHAIN
Why Blockchain and how it will work in case of VeCap



USE OF INVESTMENTS



ROADMAP



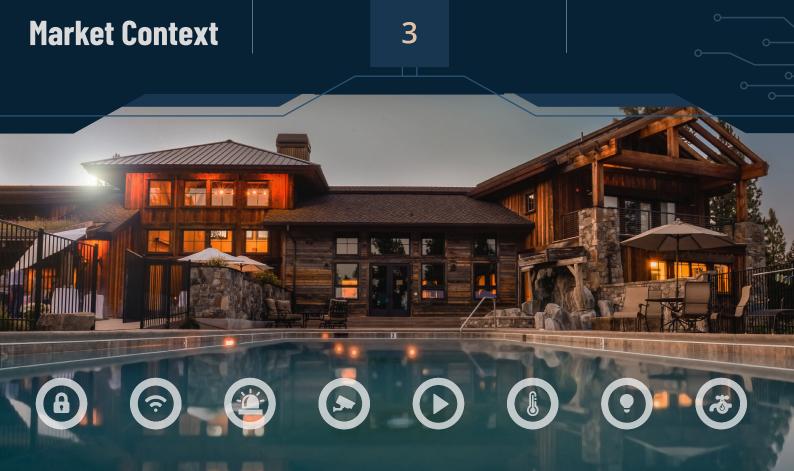
TEAM & ADVISORS



MISSION & VISION



LEGAL



Market Context

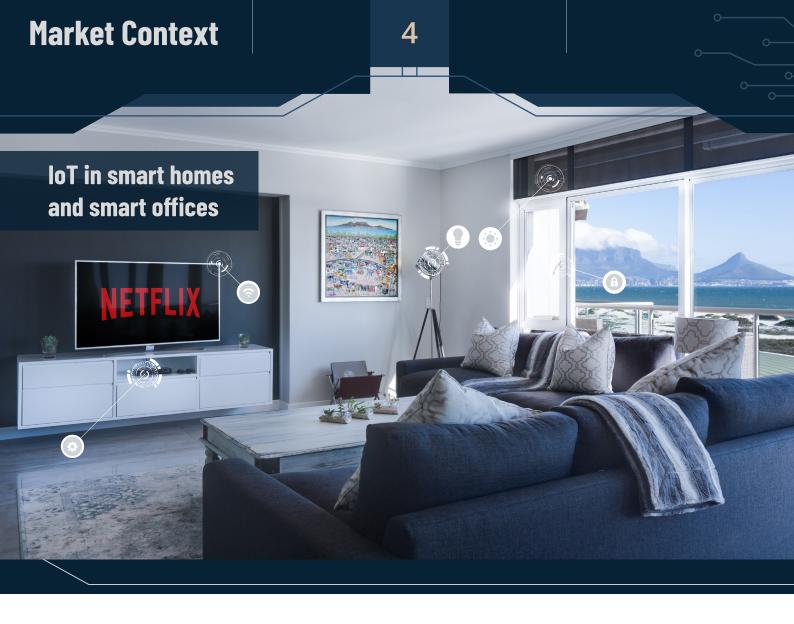
VeCap will disrupt the Smart Home and Smart Office segment of the Internet of Things (IoT) market.

IoT is a Big Thing

What is the Internet of Things?

Basically, it's a network of devices or any other physical objects connected to the Internet. This technology makes automation and remote control of these gadgets possible. The examples of IoT devices can range from smart door locks to smart sensors on the wings of an airplane.

Historically, the IoT discussion was predominantly focused on smart homes. For instance, in 2016, 40% of all online articles about the Internet of Things covered this use case¹. It makes sense given the role that homes play in our lives. With the help of IoT, they will become even more comfortable, secure and energy-efficient.



Just imagine: when you enter your house, not only will the doors unlock automatically, but the lights will turn on and the TV will start playing your favorite Netflix show.

We're headed to a worldwhere our doors unlock when they sense us nearby. Scott Weiss,

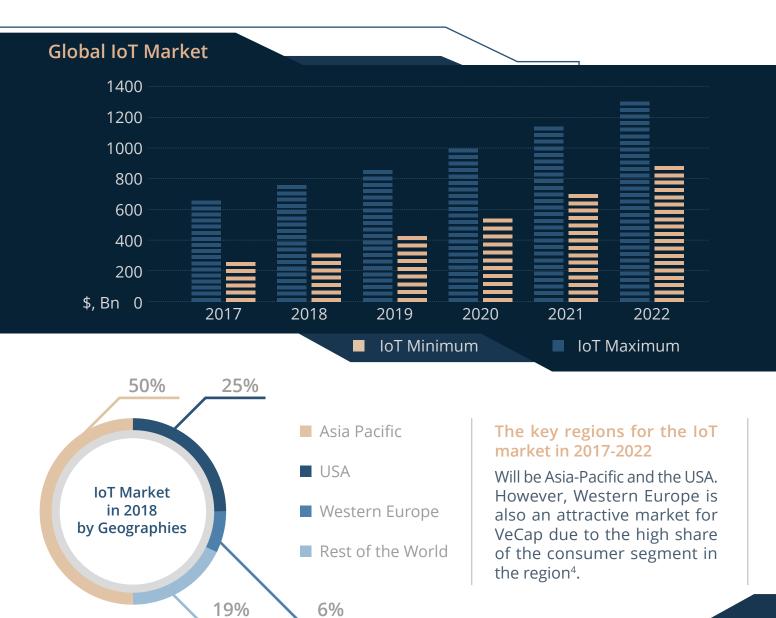
a venture capitalist from Andreessen Horowitz It is no surprise that according to a report by Icontrol Networks, consumers across all demographics are enthusiastic about having a smart home.

Hundreds of use cases related to IoT devices promise the radical changes in our lifestyle and workplace. That is why VeCap is so excited to be on the frontiers of the smart home and smart office industry.

Huge Growth

Market experts conclude that market for IoT is already significant and growing with an impressive rate. Bain² and IDC³ respectively evaluate the size of the IoT market to be between \$235 billion and \$674 billion in 2017.

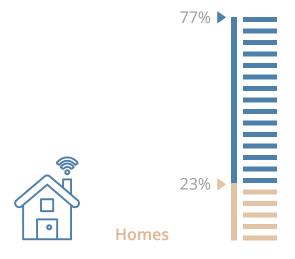
The expected size of the IoT market in 2021 will range from \$678 billion to \$1.1 trillion. CAGR is estimated to be between 14.4% and 22% in 2017-2021.



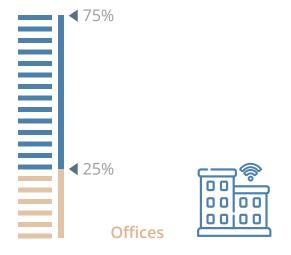


VeCap should also focus on advanced economies. The majority of the value of IoT in smart homes and smart offices will be realized in advanced economies (77% and 75% respectively)⁴.

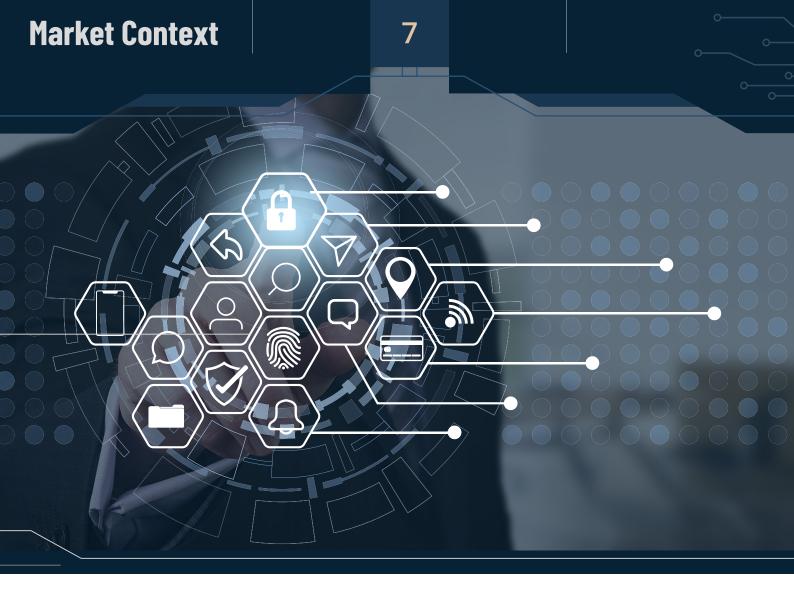
Western Europe specifically will be an attractive market for VeCap due to the high share of the smart home and smart office segment in the region⁵.



Higher average spending on smart homes in advanced economies outweighs a higher number of households in emerging markets



Higher costs and wages in advanced economies increase the impact



From Hype to Reality

In the 2011 report, Cisco claimed that IoT is about to change ourselves and everything that we know to be true⁶. This was a clear indication of a hype that typically surrounds introduction of a new technology.

Today the forecasts and discussions on IoT seem to be more conservative. For instance, in 2015, IDC predicted the IoT market size would be \$1.29 trillion in 2021. In 2017, they reevaluated the prediction and now estimate the IoT market to be \$1 trillion in 2021.

The leveling off can be explained by a more realistic outlook and recognition that the further penetration of IoT devices and solutions is limited by the lack of security, universal standards, and outdated business and IT structures.

Companies that will address these challenges will have the highest growth in the coming years, and VeCap aims to focus on solving these issues in order to unlock the potential of IoT market.



Security

Opportunities for Growth

While the number of IoT devices grows, their security is still questioned. According to Ericsson, the number of IoT consumer devices will exceed the number of mobile phones in 2018. By 2022, there will be 18 billion IoT devices in the world⁷.

At the same time, the AdaptiveMobile claims that up to 80% of existing IoT devices are not adequately secured⁸. In these circumstances, the security becomes vital for the further adoption of technology.



IoT Security is indeed considered to be incredibly important by industry experts and potential customers.

According to the survey by McKinsey, 75% of global experts perceive IoT security as a top priority, yet only 16% of them think that their companies are prepared to deal with this kind of threat⁹.

Bain's survey has showed that 45% of respondents think that lack of security is the top barrier for IoT adoption, which makes it the most important barrier identified in the study¹⁰.

IoT security is perceived as a priority by 75% of experts but only 16% say their company as well-prepared.

Highest priority...

~ 75% of 400 surveyed experts say that cybersecurity in the IoT is either a top priority or important

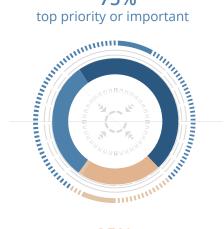
50% Top priority

25% Important

Some relevance

No relevance

~75% top priority or important



25%

... and ~ 70% of expertsexprct the priority attached to cybersecurity in IoT to increase even further

49% Increase substantially

21% Increase

Remain the same

Descrease/decrease substantially

> ~70% priority increase



~30% priority remains the

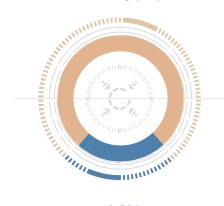
... but luck in preparedness

Only 16% of experts across the 4 survey countries state that their company is well-prepared

84% Insufficiently prepared

16% Well-prepared

84% insufficiently prepared



16% well-prepared

People will buy IoT devices

with the highest security, and they are ready to pay more for this. Respondents of the Bain survey indicated that they would buy 70% more and pay 22% more for secure devices. The market for solutions solving the problem of security is also growing.

Gartner predicts that spending on the security of smart devices will grow from \$1.18 billion in 2017 to \$1.5 billion in 2018 (CAGR = 27%).

By 2022, the spending will have reached \$3 billion (CAGR = 19%)¹¹. Therefore, it is evident that vendors focusing on security in IoT will earn more.

VeCap considers security to be a key priority of its solution.



Interoperability

Key to Market Share Growth

In short, interoperability means the ability of different IoT products and systems to work with each other. According to Bain's survey,the number of respondents who considered lack of interoperability as an important barrier to the spread of IoT was 28%¹². The IoT systems and products of the future have to be compatible.

Interoperability helps increase the market share and attractiveness of the IoT products. BCG and McKinsey claim that vendors who want to increase the smart home market share have to create ecosystems and platforms of compatible devices and applications in order to increase the stickiness of their offerings.

Early adopters of smart homes, who are still quite limited in the application of devices because of the interoperability issues, cannot agree more on this. VeCap is focused on solving this problem, thus increasing the number of potential IoT use cases exponentially.

Decentralization

A decentralized ecosystem of interconnected devices: Future of IoT

Current IoT systems are centralized and ineffective. Devices initially have to connect to the central cloud server even if they are approaching other devices in their vicinity. The operation and maintenance of such systems are costly, and their existence additionally increases the risk that the entire network will break in case of the failure of the service providers.

The adoption of a decentralized approach helps to solve these problems. It gives a green light to the high-load IoT systems of the future that will require efficient connections between millions or even billions of devices.

Moreover, this structure will decrease the possibility that the entire network will fall in case of a failure of one node of the system. The decentralized IoT ecosystems will be based on Blockchain.

Blockchain

Internet of Things

Blockchain solves the problems of low security and outdated centralized IoT systems. Blockchain cuts the risk of hacking the devices by reducing the potential points of entry and enabling systems to protect themselves. It also makes the decentralized IoT systems real.

By 2019, 20% of all IoT deployments will have basic levels of blockchain services installed, and VeCap is going to be one of the first Blockchain IoT providers on the market¹³.



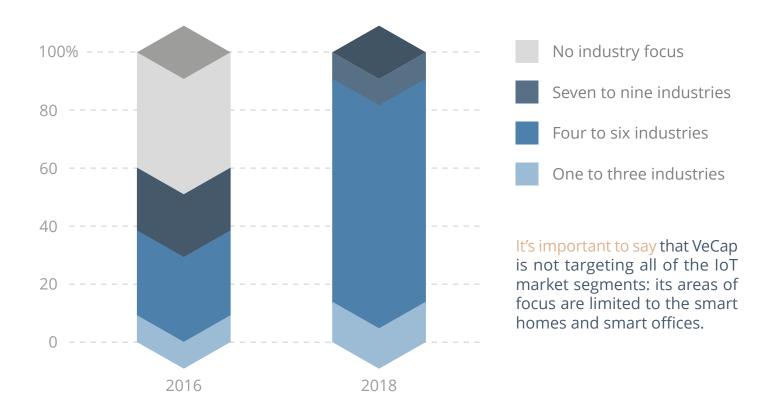
A growing need for specialization

In 2018, the market should expect IoT companies to focus on a limited number of segments of IoT market.

Based on its experience with previous technology cycles, Bain concludes that companies who would focus on two to three segments of IoT market will gain the expertise and competitive advantage over generic offers of huge Cloud Server Providers (CSPs) like Amazon, IBM or Microsoft¹⁴.

To this day, more than 80% of vendors still target four to six segments of IoT which limits their ability to gain expertise rapidly.

Percentage of industries in which a vendor is investing at least 10% of IoT R&D budget



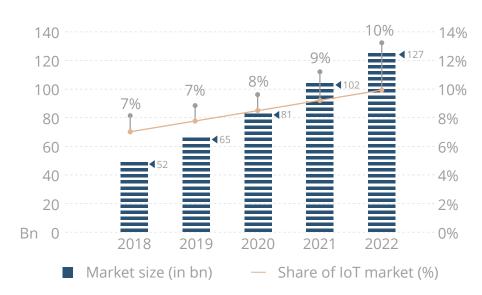
Sources:

Bain loT vendor survey, 2016 (n=158);

Bain IoT vendor survey, 2018 (n= 182).

Smart homes market

One of the key segments of IoT market are smart home devices. The smart home segment is huge and is growing faster than IoT. In 2017, this segment's share was 7%, but in 2022 it will occupy 10% of the entire IoT marketplace. It will equal \$127 billion in 2022 and will have a CAGR of 25.3% in 2018-2023, according to Mordor Intelligence¹⁵.

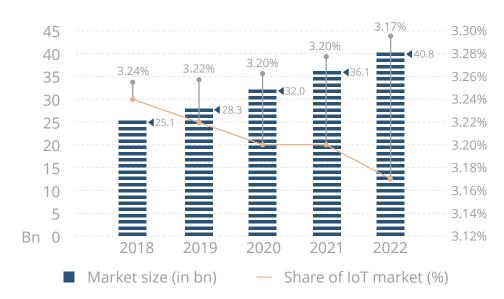


Smart offices market

are devices for smart office. According to Report Buyer, by 2022 smart office market will be \$40.8 billion (CAGR = 12.9% in 2017-2023). During this period its share of IoT market will be approximately 3.2%. The growth will be mostly driven by the demand for office security and

energy efficiency.

Another important segment



VeCap offers a specialized BIoT solution for smart homes and smart offices that addresses the key concerns of customers. The company has a deep knowledge and expertise in the smart home and smart office segments of IoT which will help it gain its share of the market rapidly.



Brand new world of loT cyber attacks

In the fall of 2016, the world was struck by a sequence of DDoS attacks. Some people directly linked those events to the upcoming Presidential elections in the US and thought that the attacks were nation state backed.

The reality appeared to be less James Bondish but incredibly concerning: the malware used in DDoS attacks was created by an undergraduate student and Minecraft player, Paras Jha. He came up with a very simple, yet smart idea: the malware searched for IoT devices that still were protected only by default passwords. Thus, after 2016, we started to live in a new world where huge botnets could be generated by amateurs.

The new method was used to generate a botnet called Mirai that was exploited in various record-breaking DDoS attacks. Anonymous hackers attacked French hosting company OVH in September 2016.

The attack peaked at the bandwidth of 799 Gb/s, which made it the biggest ever reported. Later, Jha published the code of his malware in open source making it available to anybody.

The size and scale of recent DDoS attacks has far exceeded what the industry thought was the upper end of the spectrum.

Carl Levine, Sr. Technical Evangelist for managed DNS provider NS1

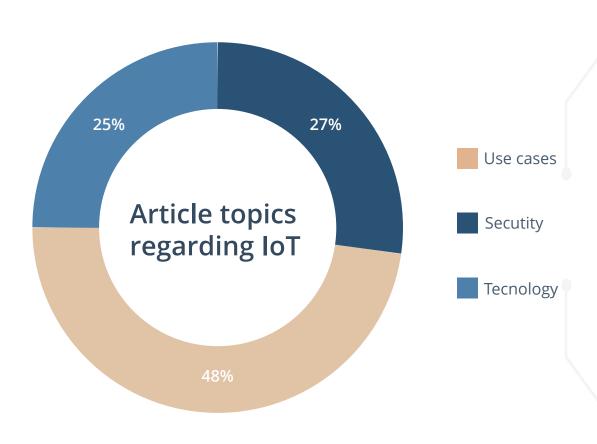




The next incident happened less than a month after and targeted an American infrastructure provider, Dyn. As a result, sites like Amazon, SoundCloud, Reddit, Spotify, etc. became unavailable.

It is no surprise that security of IoT devices is undoubtedly the top concern for the market. According to a study by Quid, a company specializing in text-based data analysis, 27% of all discussions about IoT on the Internet are centered around the security.

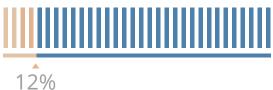
Since 2016, the amount of IoT-based attacks and their strength has only grown. In last 3 years 20% of all companies faced at least one cyber attack on IoT devices in last three years¹⁶. On top of that, 97% of risk specialists believe that potential cyber attacks on unsecured IoT devices might be catastrophic for their organization¹⁷. The potential losses for businesses might be as large as 13% of their revenue.



B2C clients are also concerned with the threat of cyber attacks. According to the poll by ReportLinker, the majority of consumers, 82%, believe that cyber attacks are becoming more a threat that they were 5 years ago.

Base: 539 online respondents representative of the general US population. Interviews were conducted on october 4th 2017







More a threat then they were 5 years ago?

The same threat then they were 5 years ago?

Less a threat then they were 5 years ago?

B2C clients are in danger of eventually finding their smart TV involved in Bitcoin mining or DDoS attack and having their smart homes controlled by anonymous hackers.



Existing IoT devices, specifically operated and offered by cloud service providers, are insufficiently protected. They have serious breaches in their security systems: insufficient encryption, weak authentication requirements (e.g. auto-login or default passwords), and the possibility of external connections via VPN that make access without consent possible.

It takes hackers less than a minute to get access to smart home devices¹⁸. Devices with zero-day vulnerabilities can be hacked as soon as the breaches become known. Manufacturers are not able to update all vulnerable smart devices instantly.

On top of that, IoT systems have plenty of entry points. An average smart homeowner has several smart devices, and a single unprotected one is enough to compromise an entire network¹⁹. In 2020, each home will have an average of 50 interconnected products which will make the risks even higher.

VeCap's Solution

VeCap protects all devices in a smart home and office by uniting them in a decentralized network. Transactions between IoT devices will be recorded in blockchain as smart contracts. A hypothetical hacker will have over 51% of the network to hack a specific device, and the completion of this task is almost impossible: all blockchain records would be duplicated on millions of IoT devices in tens of thousands of smart homes and offices.



No standards

The lack of interoperability was historically caused by a focus on individual devices and single-purpose applications²⁰. Software companies and device manufacturers wanted to promote their own solutions rather than agree on unified standards.

This tendency is typical for introduction of new technologies: energy outlets are still not standardized around the world up to today, VHS didn't become the standard for videotapes instantly.

Governments recognize the problem

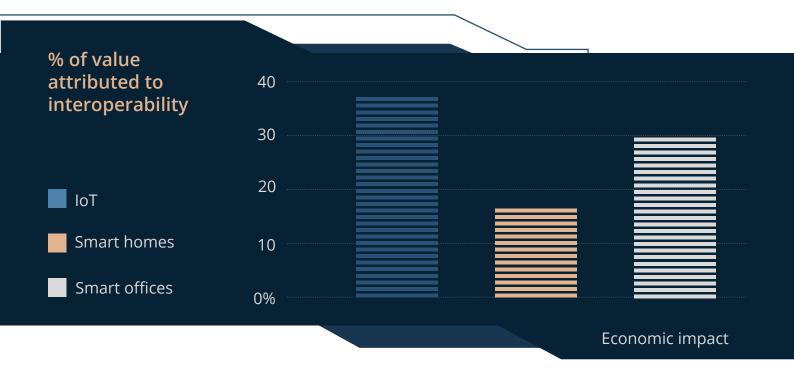
The problem of lack of interoperability is recognized on the government-level. European Commission in 2017 approved the amendments to the legislation that is designed to force companies to pay more attention to the interoperability problem in IoT²¹.

Potential

Unleash full potential of Smart Homes and Offices

Vendors need to create ways to integrate different IoT technologies to unleash the full value of IoT solutions for home and office and to attract more customers.

In home and office environments 17% and 30% of total value of IoT won't be realized without interoperability in 2025. These findings are presented in McKinsey's report "The Internet of Things: Mapping the Value beyond the Hype"²².



Potential

Unleash full potential of Smart Homes and Offices

According to ReportLinker,

63% of respondents are unlikely to purchase smart home solutions. About 26% of them don't see the benefits of Smart Home solutions²³.

The root cause of perceived low utility is the interoperability failure — current smart home systems consist of single islands of interoperable devices.

Only in case of being connected these solutions could provide more value at smart homes and offices and convert skeptics into customers.

In a near future, to what extent would you be interested in buuing a home automation solution?



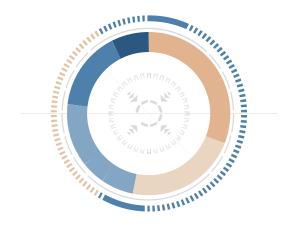
31% Somewhat likely

21% Somewhat unlikely

6% Likely

42% Very unlikely

Why won't you be interested in such smart home solutions



More expensive

26% No benefits

Have privacy concerns

14% Other

6% Complecated to install and monitor



Value of Interoperability

In home environment interoperability will have the biggest impact through linking chore automation with energy and security systems and by increasing customer satisfaction through pleasing experience of using compatible devices²⁴.

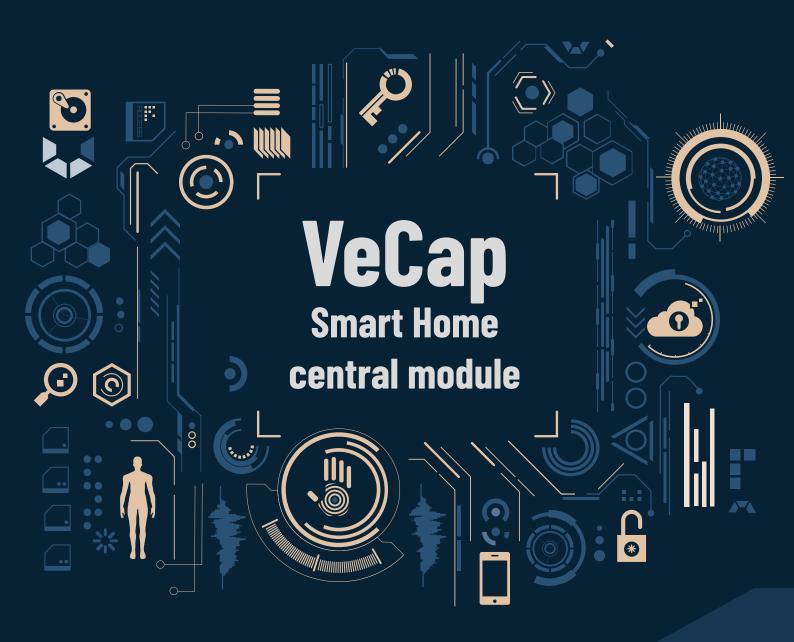
Interoperability will mostly affect offices through enhanced energy management and security in buildings and the productivity increase achieved by offering the workers ideas on how to better their performance and making office a more comfortable place to be²⁵.

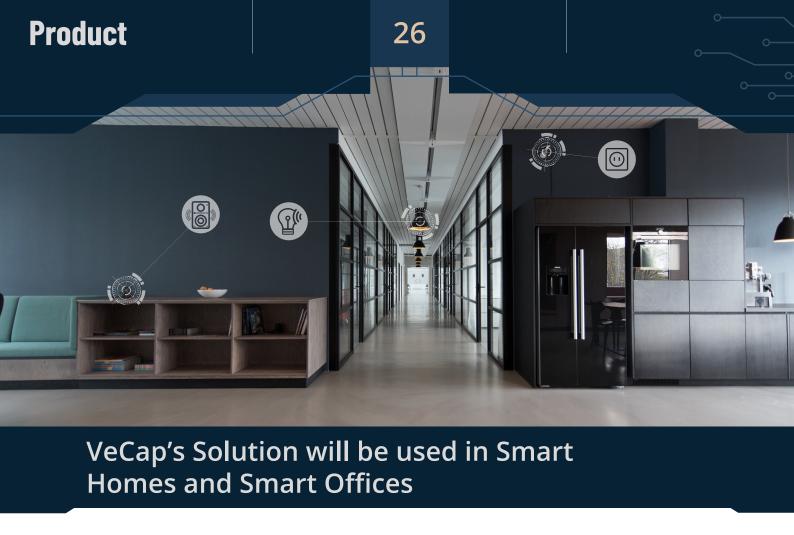
However, to this day there is no universal solution on the market that could make these benefits come to life. VeCap is going to offer this solution.

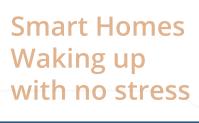
VeCap's Solution

VeCap certified devices will be automatically added to the blockchain ecosystem that allows them to interact with each other directly or via VeCap Smart Home and Smart Office Central Module.

VeCap will also create an adapter to connect uncertified devices manufactured by other companies. Adapter enables a tighter integration of the smart objects in the home via blockchain ecosystem allowing all smart devices to work together.







If the time is between 7 a.m. and 8 a.m.

And It is not weekend
And Owners are at home
And smartwatch
detected that the owner
is at the perfect dream
cycle to wake up

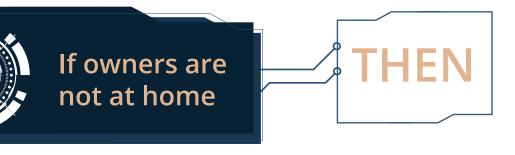
Smart curtains open to let the sun light in

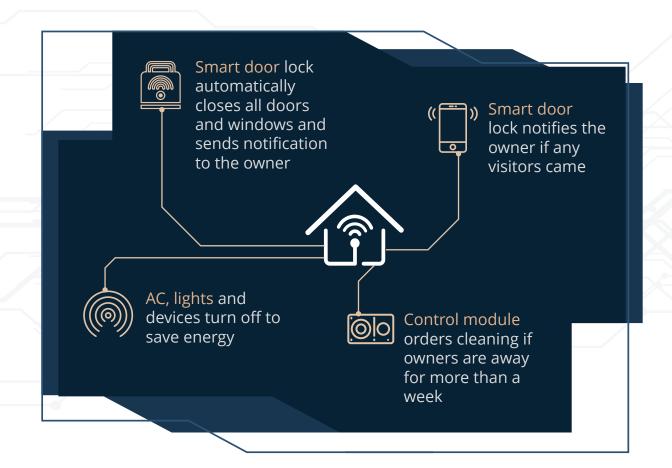
Music center turns on active music to wake you up

Bathtub starts filing

Control module orders breakfast from a favourite nearby restaurant and a taxi to work in one hour THEN

Be in charge of your home when away





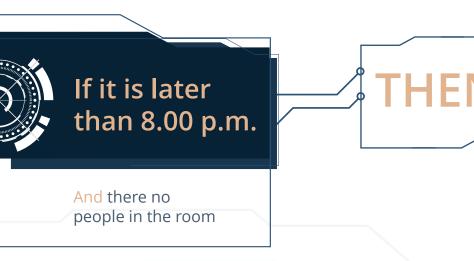
Smart Offices

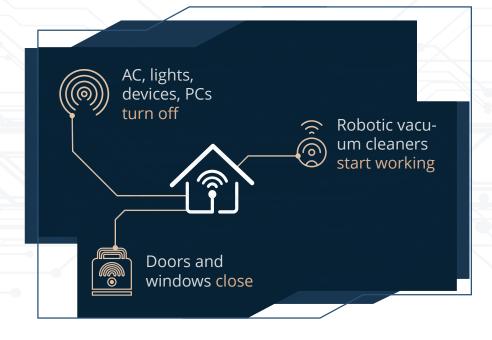
If the new employee comes into the office building





Preparation for a night





All of these use cases will be possible thanks to the VeCap Smart Home and Smart Office Central Module, VeCap certified devices and VeCap Adapter distributed through VeCap Ecosystem.

VeCap Central Module

VeCap Central Module will be in charge of the device network. Through central module users will be able to set up the rules for smart home and smart office.

The majority of VeCap devices will be able to interact with each other without the intervention of central module which will make the system more resistant to possible technical problems with it.



However, the most generic devices will have to always connect to it due to the limitations of their processing power.

VeCap certified devices

The central module will connect directly to VeCap certified devices. VeCap will produce only the minimal number of basic IoT devices.

The majority of them will be produced by other vendors. To make sure the security and interoperability of all devices in the system, VeCap will set up a Certification Process.

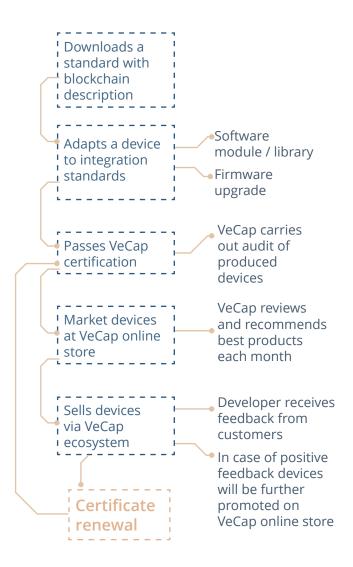
The certification process will consist of analysis of the VeCap standard by third-party vendor, adaptation of a device to the standard and VeCap certification committee.

Standards include information about the hardware and software requirements for devices.

After the successful certification, selected devices will be marketed and sold on VeCap online store.

The devices that have positive feedback from users will be additionally promoted by VeCap each month.

There will also be a constant certification renewal process to make sure the alignment of existing devices with updated standards.





VeCap Adapter



VeCap do recognizes the fact that some consumers have already purchased the devices that are not certified by VeCap. To attract these people and companies and to make VeCap's offer more sticky for them, VeCap will produce a VeCap Adapter.

Basically, it will be a device that will connect open standard IoT devices that were not certified by VeCap to the Blockchain system. Thus, the barriers to joining VeCap Ecosystem for consumers will be lower.

VeCap Ecosystem

VeCap Ecosystem will be a marketplace where hardware producers will be able to promote and sell their products, crowdfund their future undertakings and communicate with customers. The ecosystem will also feature a VeCap Fund for supporting producers initiatives.

Ecosystem cornerstones

Online hardware store

Hardware producers will be able to promote and sell their products via VeCap's store.



Crowdfunding platform



Each producer can apply for crowdfunding of a new product to speed up development process and meet customers demands

Community

Social media platform to increase engagement of producers and create additional interactions with customers



VeCap's fund for supporting producers initiatives



VeCap will act as an investor for development of the most promising products

Tokenomics

The transactions on blockchain-driven ecosystem of VeCap will be paid in tokens.

There will be two types of tokens: VeCap tokens for paying monthly subscription and the purchase of hardware devices and IoT tokens that will be burnt each time when a transaction between IoT devices takes place.

Thus, VeCap will earn money not only on software, devices and commissions in online store, but also on massive number of transactions that will happen among numerous IoT devices.

VeCap tokens



Paying for VeCap software monthly subscription (price fixed in tokens for 6 years)



Online store purchases:

VeCap Smart Home devices VeCap Smart Office devices

Tokens are sold with discount to motivate growth of device prices after the ICO and press releases.

Prices are fixed in tokens for 6 years and will not be differ from fiat price by more than 5-10%

IoT tokens

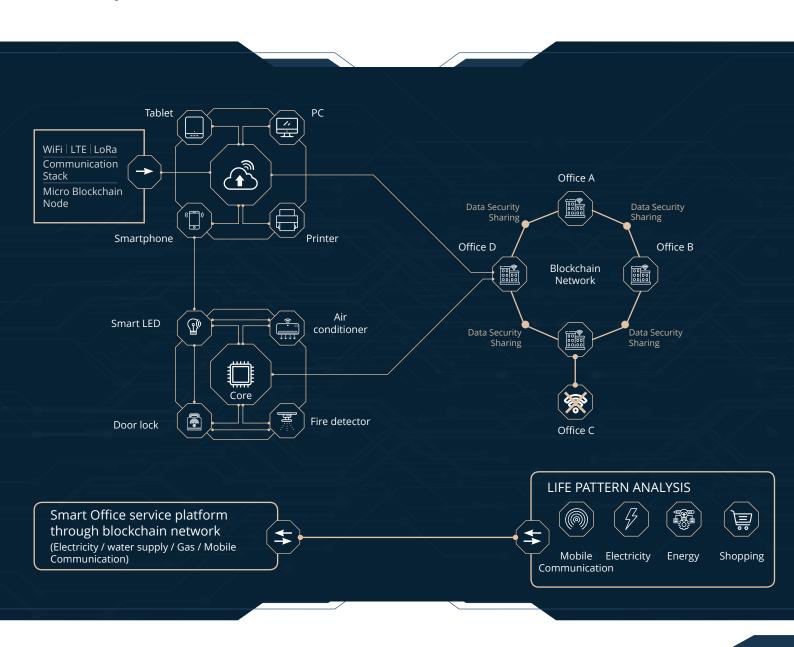
Tokens for transactions between smart devices



Transactions between smart devices

VeCap Technology

VeCap will create the public Blockchain Platform on Etherium that will support smart contracts in order to guarantee the security of smart home and smart office devices.



Public Blockchain Platform

Since the problem of Security is one of the biggest in smart home and smart office IoT, clients of VeCap would benefit from a public blockchain platform uniting devices from all of the users. Since hackers need to take control of over 51% of devices in the system to hack it, the more devices connected to the platform, the better.

However, VeCap might negotiate the creation of private blockchain platforms for Enterprise B2B clients who would want to separate themselves from the public platform. Additionally to that, the platform will be able to analyze patterns in energy consumption, shopping, mobile communications, productivity of workers, etc.

Smart Contracts

The information about the transactions among devices will be saved as smart contracts on Ethereum-based Blockchain. The use of smart contracts will increase the speed of operation and on top of that they will help VeCap to conveniently track the number of IoT tokens burnt.

Decentralized, hacker-resistant system of VeCap's smart contracts will create the standard for smart home and smart office markets.

Data Encryption

Blockchain technologies will provide the security of the devices, but they won't be able to secure the data of users. To solve this problem, VeCap will add end-to-end encryption.

Vecap will raise \$72m

to develop and market its product if hard cap is reached

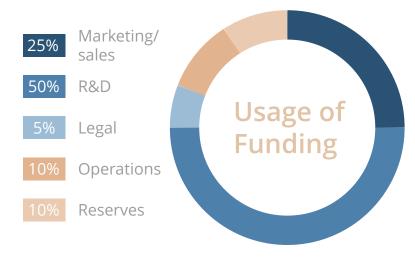
VeCap will issue 1 billion tokens for ICO. They will be divided between tokens used for seed round, pre-ICO, ICO, team investments, marketing incentives and reserves for further selling.

VeCap will spend half of attracted investment on R&D to create the best products for clients. This will include the creation of Blockchain platform, software for vendors and hardware for consumers.

There will be both B2C and B2B marketing and sales to attract consumers and vendors to VeCap's platform and guarantee sustainable growth. Marketing and Sales will account for 25% of use of investments.

15% of investments will be spent on operations and legal.

VeCap will reserve 10% of investment for unexpected expenditures.



Fundraising caps for ICO:

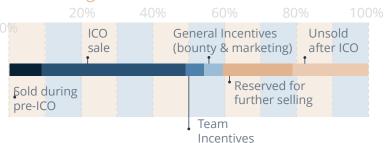
\$24M \$48M \$72M

Soft cap Medium cap Hard cap

ICO parameters:

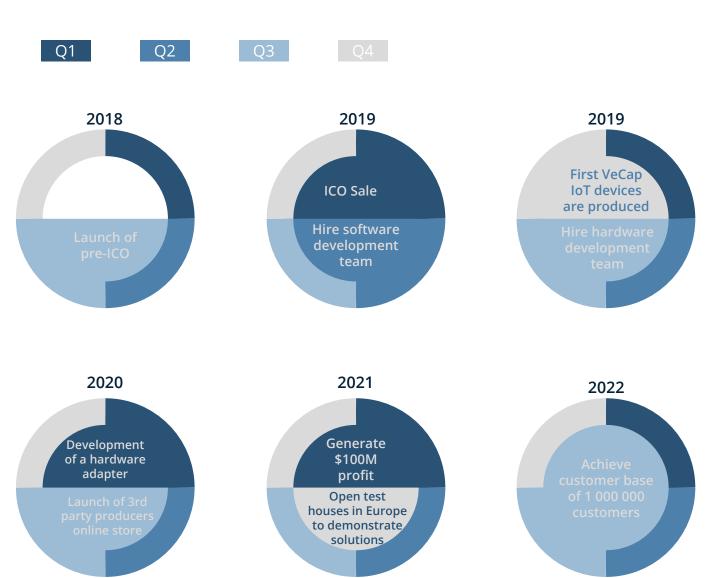
1B \$0,12
Total issue 1 Token price

Sold during seed round



In case of hardcap scenario VeCap will purchase or rent several demo-houses in large European cities.

Vecap team outlined following plan for product development



Team



Imad Labbadi

Founder & CFO

Entrepreneur with experience in strategic conception and business development.

8 years of Experience in start up - tech Industry.

Blockchain enthusiasts with deep understanding of their technology

With the passion for Sales & Mindset Coaching.



Sebastian Frank Wobig

Co-Founder & COO

Communication specialist in techbased business models.

Leading our Press relations & internal communication with a deep understanding in Blockchain and cryptocurrency.



Sems Samars

Token & Crowdsale develope<u>r</u>

Passionate Developer and technical team leader.

With expertise for Ethereum-Blockchain development.

Current working as software developer & IT consultant.



Boris Bosnar

Web developer

Entrepreneur with experience in developing websites, web application,

content management systems, front and backend system and other web technologies.

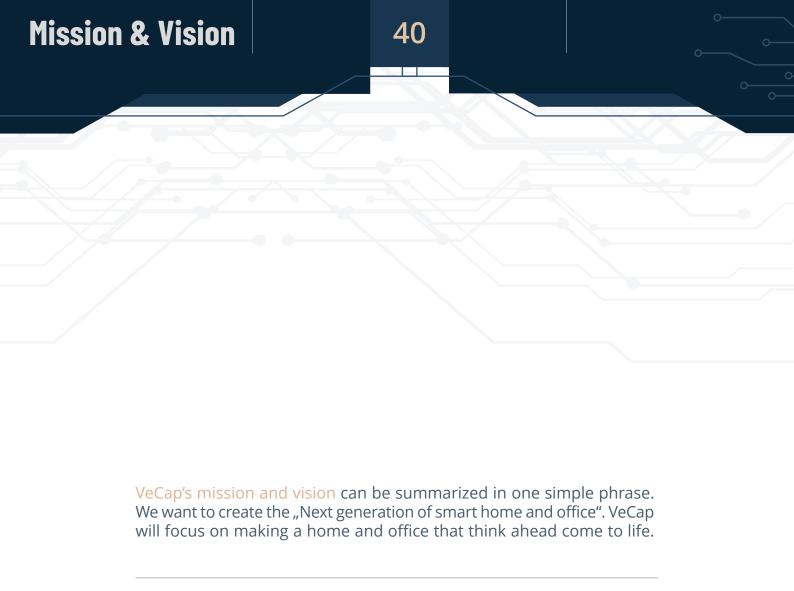


Claas Gnerlich

Web developer

Entrepreneur with experience in Web Development and technical products.

Specialized in iOS and android platform development.



41

The given White Paper document has been formulated to present the VeCap project to potential participants of the platform and those interested in contributing to its development. The information set out below may not be exhaustive and does not imply any contractual relationship. Its sole purpose is to provide information to potential Token holders, so they may determine whether they are willing to analyze the company with the intent of acquiring VeCap Tokens.

No part of the given White Paper shall be deemed to constitute a prospectus or a solicitation forcontribution, nor does it in any way pertain to an offering or a solicitation of an offer to buy anysecurities in any jurisdiction.

The given document is not composed in accordance with, nor subject to, any laws or regulations of any jurisdiction aimed at protecting contributors.

Certain statements, estimates, and financial information contained in the given White Paperconstitutes forward-looking statements. Such forward-looking statements or information deem risks and uncertainties, which may cause actual events or results to differ materially from the estimates or results implied or expressed in such forward-looking statements.

The given English language White Paper is the primary and sole official source of information about the VeCap project and its Token launch. The information contained herein may be translated into other languages or used for establishing written or verbal communication channels with potential partners or contributors of the project. As a result of translation, some information contained herein may be omitted, corrupted, or misrepresented. In the event of inconsistencies between any translations or communications and the given official English language White Paper, the provisions of the given English language original document shall hold primary status and prevail.

VeCap reserves the right to introduce changes to the given White Paper. In the case of a difference or differences between the versions of the document, the latest version of the White Paper published on the VeCap.com website shall prevail, and all previously published versions are considered to be invalid in all their iterations and representations.

VeCap prohibits users of the platform to avoid capital controls of any kind and does not allow them to conduct contributions in foreign assets of any manner.

The information contained in this Whitepaper and on https://www.VeCap.com are of descriptive nature only, are not binding and do not form part of the terms and conditions of the Token generation event (hereinafter known as the "Terms"). In particular, you should be advised that the purchase of VeCap Tokens may involve high risks. Please refer to the risks section in the Terms for more information.

Before purchasing any VeCap Tokens, please ensure you are capable of offering official representation and warranties, specified in the respective sections of the Terms.

Any distribution, public or otherwise, of the given document and the offer and/or sale of VeCap Tokens may be restricted by law in some jurisdictions. Failure to comply with any restrictions could result in a violation of the law. At the moment, VeCap Tokens have not been registered under the U.S. Securities Act of 1933 (hereinafter the "Securities Act"), or with any regulatory authority of securities of any state or other jurisdiction in the territory of the United States. VeCap Tokens shall not and cannot be offered to, purchased by or sold to, on the account of or for the benefit of, any green card holder of the United States or any US citizen or permanent resident of the United States (tax or otherwise), or to an individual having a primary residence or domicile in the United States (tax or otherwise), including Puerto Rico, the U.S. Virgin Islands or any other territory or possession of the United States.

VeCap Tokens shall not and cannot be offered to citizens or permanent residents of the Republic of Singapore (tax or otherwise), or anyone having a primary residence or domicile in Singapore.

VeCap Tokens shall not and cannot be offered to citizens or permanent residents of Canada (tax or otherwise), or to anyone having a primary residence or domicile in Canada.

We do not and cannot provide guarantees and disclaim any liability that the above-mentioned conditions shall be fulfilled. It is the sole responsibility of the reader and potential participant or contributor to ensure that participation in the Token Sale is not prohibited under the applicable laws of said participant's or contributor's country of residence or domicile.