Grig Messenger

and other SwapWire empowered applications

09/27/2019

White Paper

Date:
2/27/2020

Prepared by:

Alexander Gusev
Chicago, IL 60606

1. Project Overview

1.1. Introduction: “Obsessed with APSaS”

The first mobile platform offering the Anonymity, Privacy & Security as a Service (APSaS); merging three values together and supplying an end user with friendly and effective tools to control levels of own anonymity, privacy and security is our value proposition.

Grig™ is an ambitious project dedicated to produce a cutting-edge mobile platform with highly-secure on-the-go data-and-funds exchange environment to an end-user. Packed with bunch of redundant security and privacy tools the application is striving to meet and surpass defense-grade security requirements by employing “true end-to-end” encryption technology SwapWire™.

The application encrypts messaging data using the recipient’s public key and dissolves it inside the background picture adding yet another - far from the last - security layer. Our core technology that at the base of Grig Messenger and other products is the SwapWire™. SwapWire™ is the method of emulating hardwire connection by running channel switching protocol on top of packet switching protocol. Other SwapWire™ empowered tools are: 3-factor authentication (3FA™) and fund’s transferring (Grig Pay™) applications.

The mobile application is packed with the know-how features such as: “over-the-shoulder-look protection” mode, “chat-window pin-code-lock”, “fake-pin-code > your message erased” feature, “very private space” with parental support, and few other you can find only in Grig Messenger. Beta version of the messenger for Android devices is available for installation and free use on: https://en.grig.ai/

1.2. Abstract.

1.2.1. SwapWire™:

The backbone of our applications is the “true end-to-end”, or “on-device” encryption method – the SwapWire; in Grig Application, in order for the connection to get established the participants each must commit to the dialogue by entering their individual pin-codes - entering the fake pin-code by any participant rejects the connection request and reverses the invitation procedure. In 3FA, the SwapWire controls the transport of the random pin-code, establishing encrypted communication channel between the user, the server and the platform. GrigPay secures the transactions using SwapWire technology with the 3FA used as an additional verification tool.

1.2.2. Fake PIN: Pin-code recognition feature, allowing user to set good and fake pincodes at the time of log-on. The function performs irreversible sensitive-correspondence termination when the fake pin-code is entered – messages marked by the red checkmark are permanently erased when the user enters the fake pin-code in "Red Lock" mode (all messages are red-marked by default).

1.2.3. Chat Lock: An ability to lock particular chat with good or fake pin-code, avoiding locking the entire application.

1.2.4. Lie-Scan: User voice pattern-analyzing feature, enabling users to conduct true-false valuation of other user's voice on a base of previously conducted survey comprised of preset questions-answers. The Lie-Scan function is located on a body of a voice message as a horizontal graph (100%-red-0%-green-100%), displaying the %-probability for the received voice-message being truth or false.

1.2.5. Hold-to-Use: An innovative, supplementary revenue model. While using the Grig Application is free of charge, some features require holding a small balance of GRIG Token in their wallet for as long as they are using the selected features. Tokens can be withdrawn anytime causing the cancellation of feature. For example: in order to activate LieScan function the user would have to deposit and keep the balance of at least 1.00 GRIG in their Grig Wallet.

1.3. Other SwapWire based Applications:

1.3.1. 3-Factor Authentication: Is our ultimate response to the recently announced "quantum-attack" threat, and the next evolutional step designed to outperform conventional 2-factor authentication method. 3FA utilizes hybrid pin-code generating algorithm when computer and human logics are intertwined together in such way that the resulting verification pincode number is mathematically impossible to decrypt. We consider the 3FA to be quantum-attack proof and mathematically impossible to decrypt.

1.3.2. GrigPay: GrigPay is a cross-banking payment platform, originally designed as an internet-less phone money-transfer method "PayPhone" in 2015. The system had been developed and successfully tested with the regional Bank in Russia; it is commercially mature and is designed to be used with any phone hardware with or without an access to the internet and does not require installation. Transactions are made by accessing the bank's servers utilizing conventional DTMF analogue channels as a transport. The target product, however, is a mobile application secured by 3FA-empowered pin-code generating application combined with analogue DTMF pin-code delivery methods.

The SwapWire, thus, is the common denominator, holding the Grig, 3FA and Wallet apps together functionally, while each application individually supplements the services of another, all the apps enjoy functional integration and healthy marketability.

1.3.3. Tectum Blockchain: Tectum™ is a distributed badger protocol platform that employs the proprietary record change signature management algorithm - HashSwap™. Providing an instant event status delivery and event ownership update throughout the whole system the mechanism delivers distributed levels of access to functional system modules without cluttering the bandwidth between the nodes with big-data by employing our proprietary HashSwap™ component. Our unique method turns the impossible into routine process: we completely isolate all the transaction-related heavy data from the entire process by hashing, encrypting and signing the bundles at the end of every phase of a transaction and archiving it. This approach makes the event-related data instantly verifiable and publicly accessible, with different levels of accessibility provided to different transaction related modules. The event hashing process is ran on top of a database in order to enable items to be retrieved by far more quickly and works as an upper functional layer in order to free the main-net pipeline from heavy data processing. The mechanism of isolating the system event formalization process from big-data leading to the main-net unprecedented throughput capabilities is our value proposition.

1.4. Corporate Outlines: AML and GDPR regulations suggest to isolate data controlling operation from its processing operation in order to mitigate personal data access potential legal risks.

1.4.1. Grig Messenger: Commercial version release - Q4 2020.

1.4.2. 3-Factor Authentication: Planned release – Q2 2021.

1.4.3. Grig Wallet: Planned release – Q4 2021.

1.4.4. Data Controlling Operator: Stock Corporations – Q4 2020.

1.4.5. Data Processing Operator: Stock Corporation – Q4 2020.

2. Progress, Competencies & Infrastructure

2.1. Progress Statuses: Most technologies to be implemented in the project are commercially mature and/or available for customization with the exception of 3FA, SwapWire and Dual-consensus protocol.

2.1.1. Grig Application: Source code and logical models ready, POC complete.

2.1.2. 3FA Application: Technical maps, Source code in works, POC ready.

2.1.3. Grig Wallet Application: POC complete, Logical models developed.

2.1.4. Quantum Proof Number Generator: Logical models developed.

2.1.5. Server Base: POC complete, Beta version operational.

2.1.6. Blockchain: Base source code ready, POC complete, dual-consensus logical models being developed, Test Net operating.

2.1.7. Hardware: Logical models developed.

2.2. IPP & Know-Hows: The entire development boasts several patentable and/or patented technologies, comprised of SwapWire, hybrid-logic numbers generating components and other Know-hows.

2.3. Availability of Core Competencies.

2.3.1. Corporate Law: Chicago law department.

2.3.2. Financing: Helsinki team.

2.3.3. Intellectual Property Protection: Patent pending.

2.3.4. Cybersecurity: Proprietary software solutions.

2.3.5. Network: Owned datacenters.

2.4. Infrastructure and Facilities.

2.4.1. Datacenters:

2.4.1.1. Grig: Distributed, not outsourced.

2.4.1.2. 3FA: Centralized, licensed out.

2.4.1.3. Grig Pay: Decentralized, Blockchain based.

2.4.2. Software Development: RF and/or EU based operations.

2.4.3. Marketing: Outsourced.

3. Political, Economic & Social Influences.

3.1. Government Regulations.

3.1.1. Dilemma of Jurisdiction of Choice: While the choices of Jurisdictions for operating companies have relatively flexible requirements, their operating requires building a strong legal department to satisfy the AML and GDPR regulators.

3.1.2. Public Sale: No necessity to file local regulators in case of Crypto Exchange listed Token Offering.

3.1.3. Conditions for Different Stage Capital Entries.

3.1.3.1. Angel Phase: Unregulated entry, Stock Option, GRIG Token.

3.1.3.2. Public Token Sale: Crypto asset exchange, unregulated.

3.1.3.3. Initial Public Offering: SEC regulated.

3.2. Expected Contributions of the Project.

3.2.1. KYC: User-friendly and fully-remote user-verification and transaction authorization process.

3.2.2. Frictionless Conversion: Zero-fee funds' transferring and instant conversion payment platform.

3.2.3. Digital Governance: Will deliver the unprecedented level of freedom to a user, providing an opportunity to conduct communication and borderless payment.

3.2.4. Economy Effects: A major step towards globalization of economy through implementing remittance-free financial instruments.

3.2.5. Social & Cultural Contributions: Ability to conduct frictionless cross-border transactions will cultivate borderless, global social awareness.

3.2.6. Effect of Technologies: Advanced yet commercially mature biometric technologies provide fully-remote user authentication and contracting capabilities will produce long-term change in a way regional and cross-border business is conducted.

4. Industry Overview.

4.1. Mobile Apps Industry Problems.

4.1.1. Poorly Supported Privacy: No existing messaging platform has been able to provide privacy sufficient to protect a user's content from being viewed in case the device is unlocked by the third party. Normally, if third party receives an access to the device they are able open and freely read the content.

4.1.2. Unsupported Security: Regardless of the security promise all the messaging platforms make, they have technical capacity to decrypt and intercept user's data.

4.1.3. Unsupported Anonymity: The requirement to give away the phone number in order to complete the registration remains the major vulnerability point for a user.

4.1.4. General Data Protection Regulations (GDPR): Strict for data controller and data processor both within the boundaries of EU.

4.1.5. Anti-Money Laundering (AML) Policies Abuse: There is a polarity in a way the privacy is approached today. User anonymity is perceived as unreachable goal by data management operators, the AML policies open doors to freely collect user generated content and use in for commercial purposes.

4.1.6. Purely Regulated Behavioral Content Standards.

4.1.6.1. Wild-west on a Mobile Content Market: Today's market of behavioral content is controlled by the set of unwritten rules established between data operators and lawmakers meant to protect the interests of governments and enterprises both – with government agencies in need of access to consumer's personal data, while operators struggling to maintain their revenue streams – this balance is dynamically maintained at the cost of consumer's privacy and pocket; an end user has no control neither over own behavioral content anonymity neither over its revenue generating.

4.1.6.2. Hardware Producer's Race: Hardware producers are forced to collect and sell behavioral content, generated by their devices using it as supplementary source of revenues in never ending hardware price-reduction race.

4.1.6.3. Network Manager's Nightmare: Noone pays for using mobile networks in 20XX - Mobile messengers and Social network operators are forced to sell visitor's personal content to stay afloat.

4.1.6.4. User Phone Number as a Key Access Point: Most of social networks and messengers require registering phone number in order to complete the process of user registration. This is done to establish the easiest ID access point while managing the content.

4.1.6.5. Data Broker's Sellout: Operating under the silent agreement with Governments, data managers buy the freedom to lightly abuse AML policies and freely broker personal data at the price of full transparency of acquired data to the local Law Enforcement and Federal Agencies at request.

4.1.6.6. Loss of Privacy: Consumer is unaware and uncapable to control their personal data.

4.1.6.7. Consumer Pays Twice: An end buyer is placed in awkward position - In current Hardware Producer-Data Broker revenue cycle – user pays for hardware out of pocket and then pays second time for using social networks with their personal data - this "unwritten agreement based" revenue cycle has genetic flaws.

4.2. Proposed Solutions.

4.2.1. APS as Service: Delivering Anonymity, Privacy & Security as a single service by supplying an end user with friendly and effective tools to control levels of own anonymity, privacy and security.

4.2.1.1. Anonymity: Providing to a user an opportunity to remain anonymous by: not entering the phone number in the process of registration; conducting the communication using the Grig-ID only; issuing anonymous mobile payments in a form of digital-note;

4.2.1.2. Privacy: Implementing innovative UI features enabling user to: render the selected correspondence temporarily invisible to the surrounding people; create very safe chat rooms with advanced parental controls; selectively accept messages from desired party only.

4.2.1.3. Security: Establishing the technological impossibility to intercept and decrypt the transmitted data by pin-code protecting individual chats; keeping the messaging data in operating memory only; providing diverse instant-erase instruments; limiting the correspondence only one very important message and many other tools.

4.3. Competitive Landscape and Market Entry for Grig.

4.3.1. Competitors' Advantages and Disadvantages.

4.3.1.1. Competitors' Advantages.

4.3.1.1.1. Established Momentum: 2.6 Billion established World-wide user-base.

4.3.1.1.2. Free Service: No paid features.

4.3.1.1.3. Time of Entry: Mobile Messenger's prime entry time was 2014-2016 - we are entering mature market.

4.3.1.2. Competitors' Disadvantages.

4.3.1.2.1. APS not provided as Service: Most of mobile messaging platforms do not disclose and do not guarantee the quality of methods and technologies they implement to protect their users APS.

4.3.1.2.2. Relatively Poor Behavioral Content Quality: The quality of behavioral content generated by messaging apps is poorly commoditized, unstandardized and hard to evaluate.

4.3.1.2.3. No Independent Payment Systems: Most of competitors choose not to expand their services into financial field, limiting themselves to adopting conventional crypto-exchange models and bank-card payments, lacking convertibility and limiting themselves in transaction cost control.

4.3.2. Possibility for the Market to be satisfied with Conventional Products: Implementation of APS as Service will inevitable raise the bar for the industry. Integrating Grig Messenger and other APS service - providing applications at no-cost to the consumer opens up good opportunity for the market entry.

4.3.3. Expected Barriers to Entry for Grig.

4.3.3.1. Habitual Usage: Unless we provide user-friendly interface and simplify the tunnel opening process, the majority of conventional users could be reluctant to move to using Grig Messenger.

4.3.3.2. Anti-marketing: Sabotage by competitors and reproduction of some Grig features may take place under some conditions.

5. Markets

5.1. Target Markets Overview.

5.1.1. Online Dating Services Overview: Out of all Network operators, Online Dating Services enjoy the healthiest revenue models with one of the highest proportions of paying users and highest ARPU.

5.1.1.1. Users Worldwide: 196M in 2020, expected to hit 228M by 2024.

5.1.1.2. Revenue: US$2,141M in 2020.

5.1.1.3. Revenue Annual Growth Rate: Online Dating Networks are expected to grow minimum 4.3% in 2020.

5.1.1.4. User penetration: 3.2% in 2020, expected to hit 3.6% by 2024.

5.1.1.5. Average Revenue per User (ARPU): US$8.92.

5.1.1.6. Average Revenue per Paying User (ARPPU): US$49.09 in 2020.

5.1.1.7. Revenue generated in the United States: US$973M in 2020.

5.1.2. IT Security Market Overview.

5.1.2.1. Revenue: US$114B in 2020.

5.1.2.2. Revenue: US$151.2B in 2023.

5.1.3. Private Security Service Market Overview.

5.1.3.1. Revenue: US$128B in 2018.

5.1.3.2. Revenue Annual Growth Rate: Expected 6.3%.

5.1.3.3. Revenue: US$3.6B in 2023.

5.1.4. Real Estate Security Systems Overview.

5.1.4.1. Revenue: US$19.5B in 2020, expected to hit US$35.6B by 2024.

5.1.4.2. Revenue Annual Growth Rate: 16.3%.

5.1.4.3. Household Penetration: 4.7% in 2020, expected 10.1% by 2024.

5.1.4.4. Average Revenue per Smart Home: US$221.18.

5.1.4.5. Revenue Generated in the United States: US$7.15B in 2020.

5.1.5. FinTech Services Overview.

5.1.5.1. General Adoption Rate: 75% in 2020.

5.1.5.2. Total transaction value: US$ 4,770B in 2020.

5.1.5.3. Obtained an Account: 1.2B since 2011, and 0.5B since 2014.

5.1.5.4. Mobile Service Users: 69% in 2017.

5.1.6. Mobile Messaging App User Overview.

5.1.6.1. Users Worldwide: 2.52B in 2020, expected to hit 3.6B in 2024.

5.1.6.2. Revenue: US$2.14B in 2020.

5.1.6.3. Revenue Annual Growth Rate: 4.3%.

5.1.6.4. User penetration: 3.2% in 2020, expected to hit 3.6% by 2024.

5.1.6.5. Average Revenue per User (ARPU): US$20.

5.2. Expected Market Penetrations by Grig.

5.2.1. Online Dating Apps: Target Market Penetration - 10%.

	2020	2021	2022	2023	2024	2025
Online Dating Users Worldwide	196,300,000	209,400,000	218,600,000	224,600,000	228,300,000	232,500,000
Penetration Rate	0.01%	0.10%	1.00%	5.00%	7.50%	10.00%
Grig Users	19,630	209,400	2,186,000	11,230,000	17,122,500	23,250,000

5.2.2. Mobile Messaging Apps Users: Target Market Penetration - 5%.

	2020	2021	2022	2023	2024	2025
Mobile Messaging Apps Users	2,520,000,000	2,750,000,000	3,000,000,000	3,350,000,000	3,650,000,000	3,950,000,000
Penetration Rate	0.01%	0.10%	0.50%	1.50%	2.50%	5.00%
Grig Users	252,000	2,750,000	15,000,000	50,250,000	91,250,000	197,500,000

5.2.3. IT Security Sector: Not considerable amounts.

5.2.4. Private Security Services: Not considerable amounts.

5.2.5. Real Estate Security Systems: Not considerable amounts.

5.2.6. FinTech Sector: Not considerable amounts.

5.3. Factors that Determine Market Potential for Grig.

5.3.1. APS as Brand: Placed at the base of Grig's APS-oriented Brand (not overdone) the Anonymity, Privacy & Security could establish stable branding momentum, organically supported by the Grig-unique UI features.

5.3.2. Proprietary Features: We are proud to have developed know-how features to support Anonymity, Privacy & Security each individually.

5.3.3. Decentralized Network Structure: Form-factor follows function – every part of our network is decentralized to the exact degree it has to be. While Tectum DLP engine might not be implemented in every facet of the platform, the WireSwap and few other components are going to play major role in providing velocity and security to the network.

5.4. Expected Revenue Streams.

5.4.1. Public Token Sale: 15,000,000 GRIG is allocated for Public Sales in 2020-2021 with starting Token price at $4.95-7.95 and projected average order could be as low as $2.50 in USD equivalent. The proportion of publicly sold GRIG used to enable Hold-to-Use features is insignificant.

5.4.2. Hold-to-Use: Provided Grig App provides friendly and low step-count payment procedure, an average target consumer will likely be enabling their Hold-to-Use features right in the app with Target Paying User share growing from 1% to 5% in 2025.

5.4.3. Behavioral Content: A primary projected revenue stream, market value estimated at a minimal $5.59 per user per year in 2020 based on WhatsApp report from 2016.

5.4.4. Initial Public Offering: IPO is planned when the following value tops out: Stock Value = Lifetime User Value X # of users X 2,5 – debt / by # of shares.

6. Analyzes

6.1. PEST Analysis.

6.1.1. Political factors:

6.1.1.1. Danger to become a Demerit Service: Technical impossibility to decrypt the messaging data by any party without exception could become a stumbling stone in the process of adopting selected local AML and GDPR standards.

6.1.1.2. Vulnerability of Intellectual Property: Some technology, in particular proprietary cybersecurity software, could become the object of interest for selected governments. For that reason, the operating entities will be licensing the software from the holding company.

6.1.1.3. Government Intervention in the Ecosystem: Potential AML and GDPR related issues could lead to delays with regulatory filings.

6.1.2. Economic factors.

6.1.2.1. Economic Growth: Statistics provide wide spectrum of growth rates reaching 16%. We are using flat 9% growth rates in our 5 year market projections.

6.1.3. Social & Cultural Factors.

6.1.3.1. Cultural & Social Aspects: Our firm APSaS approach is ready to meet diverse spectre of expectations. For example: Users in developed countries and younger segment might appreciate privacy features the most, while users in developing countries could find security and anonymity features most tangible values for themselves.

6.1.3.2. Population Growth Rate: Will positively affect the user base growth since newcomers are not going to be bound by habitual use of conventional platforms.

6.1.3.3. Age Distribution: 20 to 36 years old among Online Dating network's users and to 55 years old among general users.

6.1.3.4. Emphasis on Safety: Communicational and transactional safeties are the driving socials factor of the ecosystem.

6.1.4. Technological Factors.

6.1.4.1. Power of APSaS: Anonymity, Security & Privacy is our priority and is approached as single issue our technology solves.

6.1.4.2. Longevity and Integrity of Quantum-Attack Proof Claim: No matter how sophisticated the pseudo-random number generator is, there comes a time when someone finds the way to do reverse-calculate it fast enough. Hybrid-logic true-random number generation technology affords us to make bold "no time-limit" Quantum-attack proof claim without looking back. There is only one way to hack our 3FA app – and this is by blindly guessing the number, the time spacing and who knows what other factor the user has chosen to dilute the computer logic with – an impossible task, unless you're a "quantum-computer fast magician".

6.2. SWOT Analysis

6.2.1. Our Strengths.

6.2.1.1. Firm PSA Policies: Clearly distinguished Privacy, Security and Anonymity advantages and limitations.

6.2.1.2. Relative Technological Transparency: All technologies are broken into processes and logically explained.

6.2.1.3. Anonymous Registration: No phone number is required to register.

6.2.1.4. Absolute Security: It is technologically impossible to decrypt the data transmitted between Grig devices using today technologies and within the frame of the message lifetime.

6.2.1.5. Privacy Prioritized: Unique features designed to protect user's privacy.

6.2.1.6. 3FA: Quantum-attack resistance is an easy to stand behind statement due the maturity of technologies and the low complexity of the component's logic.

6.2.2. Our Weaknesses.

6.2.2.1. Relatively Complicated Chat Initiation Procedure: A message can be sent only if the recipient consents to it by responding to push notification – this could lead to higher drop rate.

6.2.2.2. Individual Data Consolidation Issue: Registering Grig-user does not require entering the phone number in order to complete the registration, therefore

6.2.2.3. Potential Resource-consumption: True end-to-end encryption requires keeping the individual Secret key on the device of each recipient, therefore adding each additional user require one additional encryption session per session. Example: 4 user group would require encrypting the same message 4 times using 4 different public keys prior to sending it to 4 different group participants. Our proprietary encryption protocols provide the solution to this problem.

6.2.3. Our Opportunities.

6.2.3.1. Behavioral Content Market: The quality of behavioral content, generated by the ASP-conscious consumer will stimulate the development of more advanced behavioral metrics' models.

6.2.3.2. Online Dating Networks: The virgin ASP-sensitive online-dating consumer market could recognize the substantial value in the Anonymity and Privacy as new digital product.

6.2.3.3. IT Financial Services: There is a demanding but well-to-do user base - financial brokers, traders and other members of financial sector that could also appreciate the uncompromised ASPaS approach.

6.2.3.4. New Markets: An opportunity to enter markets previously untouched, some suppressed by local regulations, could expand the digital-payment user base significantly.

6.2.4. External Threats.

6.2.4.1. Market Leaders: Expected is the resistance from big guys like WhatsApp, Facebook, Signal and other players.

6.2.4.2. Habitual User Migration: An average user, being used to conventional messengers' UI and list of features, will require extraordinary stimuluses to decisively migrate to the communication platform: The bundle of unique features the Grig is already providing needs to be supplemented with conventional once to mitigate possible platform-migration discomfort.

6.2.4.3. Danger to become Demerit Service: There is always a chance to bring fire on ourselves in selected localities for not being resourceful enough to some government agencies in helping them with user data access.

6.2.4.4. Regulatory Issues: Strict GDPR policies for the EU Entities are not to be taken lightly.

7. Investments, Cost Breakdown & Returns

7.1. Funding Phases.

7.1.1. Angel Phase: Acquiring funding to cover production of commercial version of mobile application for year 2020-2021 using Stock Options and private Token sales.

7.1.2. Public Token Sale: Bridging Angel and Venture phases together; opening up additional opportunities by paying off the Angels.

7.1.3. Venture Phase: Investors will be offered to hold up to 35% of Stock for a period of 24-36 months.

7.1.4. Initial Public Offering: As the Lifetime User Value levels out by 2024, the Company may choose to go public.

7.2. Critical Factors Determining Cashflow.

7.2.1. Public Token Sale: The ICO hype was over and most of publicly offered crypto assets sold on crypto exchanges suffer significant drops within first 24 hours of sale – we are up for a challenge.

7.2.2. Behavioral Content Market Value: Though it is not reflected in Revenue projections, the value of behavioral content generated by Grig is expected to be valued higher comparing to one aggregated by conventional engines due to wider metrics, which will require extensive technological approach to data aggregation.

8. Timetable for Project Preparation and Completion

8.1. Mobile Application: 2020 year.

8.1.1. Android Beta Version: Operational, development in progress.

8.1.2. iOS Beta Version: 6 months.

8.1.3. Server Base: 6 months.

8.1.4. Traffic Load Simulation: 6 months.

8.1.5. Commercial Version: 9 months

8.1.6. Commercial Version: 9 months

8.1.7. Hold-to-Use Features: 12 months

8.1.8. Proprietary Behavioral Content Engine: 18 months.

8.2. Token Public Sale: 2020 year.

8.2.1. Regulatory Filings: 9 months.

8.2.2. Public relations: 6 months

8.2.3. DEX Applications: 9 months

8.2.4. 1st Line Exchanges Applications: 9 months.

8.2.5. Hold-to-Use features: 12 months

8.3. Venture Phase: 2022 year.

8.4. Going Public: STO or IPO process, 2023-2025 year.

8.4.1. Regulatory Filings: 2023-2024 years, up to 12 months.

8.4.2. Changes in Company Structure: 2023-2024 years, 12 months

8.4.3. Going Public: 2024 year, 12 months

9. Definitions.

9.1. 3-FA Features:

- Basic Mode: Analogue 6-digit PIN delivered by the random code generator after analogue SIP phone call authentication (user enters personal 4-digit PIN created during the application registration in order for the SIP server to initiate the code transmission to the user).
- Fake-digit Entry Mode: Same as the Basic mode, except a user enters only portion of the randomly generated code, and then enters any fake digits to make it up to full 6-digit PIN - fake digits are ignored by the system. For example: A user receives by the application the random code 1234, he enters 1, 2, 3, 4 and then 0, 7. The system recognizes 1234 and completely ignores 0 and 7.
- Pause-spaced Entry: In this mode a user spaces-out the random code with 1-2 second pauses while entering in established during the setup order. For example: 2, 3, pause, 4, 5, pause, 6, 7 – if pauses are skipped or misplaced, the system does not recognize the PIN.

- Dual-path Code Delivery Mode: When this mode is used, first part of 6-digit random code is delivered through the mobile application and the rest of the digits is dictated through the SIP component analogue delivery after the user has entered his 4-digit access PIN code.

9.2. Analytics Tools: Third party agents that analyse your platform using their proprietary behavioral content metric systems.

9.3. Behavioral Content: A digital good and commodity, a base resource to study and predict behavior of internet consumer.

9.4. Data Producer: Social networks, mobile messengers and other high-volume internet platforms that have access to visitor's data.

9.5. Metrics: See: Single (Source) and Complex (Derivative) Metrics.

9.6. Complex Metrics: Opposed to single (simple) metrics and browser metrics, complex metrics combine different types of metrics which are weighed properly, in order to quantitatively measure actions that matter. This way, you'll get access to actual insights without digging through raw data.

9.7. Derivative (Resulting) Metrics: Values, derived from Source Metrics in order to accommodate particular analytical need.

9.8. GRIG Token: Ethereum ERC20 protocol-based Token, GRIG is mGOP backed digital asset, designed to serve as Company Stock equivalent; GRIG Token is emitted in quantity of 100,000,000.00 units.

9.9. Grig Features:

- On-Device Encryption (ODE): Also known as the "true end-to-end" encryption. The unique Secret/Public Key pair is generated by the device of the recipient. While the Public Key is provided to the sender's device in order to encrypt the data, the secret key never leaves the device rendering the unauthorized decryption impossible. The ODE method is the backbone of Secure Tunnel algorithm.
- Single Time Secret Key use: The Secret key is generated only once to accommodate a single Chat (Secure Tunnel). New Secret Key is generated for every Secure-tunnel connection established.
- Phone Number Free Logon: Privacy of our users is our main priority; no phone number is required to activate and use the application.
- Dual PIN Entry Requirement: The recipient receives an encrypted message only after entering personal PIN code; the message is decoded only after the sender enters the sender's PIN (through analogue dial channel in paid version).

- Random-Board™: Custom non-system keyboard that works in 2 modes, floating and random symbol placement, designed to disorient key-logging malware by relocating symbols every time user types the button.
- Distributed Storage: Once recorded, the message is encrypted, divided into segments and distributed among random server nodes.
- Analogue PIN Transmission: PIN codes are transmitted over analogue dial channel and are not recognized and not recorded by most surveillance systems (Hold-to-Pay feature).
- Viewed and Destroyed: The message is completely erased and the Tunnel is closed after being viewed by the recipient on a single device in Security Mode.
- Single View Wipe Out: Application deauthorizes the user and deletes all the Cache after displaying a single message when used in Spy Mode.
- Street-Light Visibility: Green – chat window opens normally, Red Lock – Chat window is locked by the PIN code, and Yellow – all the symbols of the messages are changed to star symbols (*******).
- Fake PIN Code: The sensitive messages (marked by the red checkmark) are erased when a user enters the Fake pin-code in Red Lock mode.
- Ecosystem: As an Alpha user you are allowed to create, manage and control your own community (Example: Parental Control, Enterprise multilevel chat rooms).

9.10. GRIG Multiplier: Coefficient value designed to index Project GBDCs against unified GBDC stablecoin unit.

9.11. GRIG Token: Grig network Unit of Account, a driving force of Hold-to-use economy.

9.12. Hold-to-Use: Requirement to hold a balance of GRIG Token in the wallet in order to get certain application features unlocked. Tokens can be withdrawn anytime.

9.13. mGOP: The reference virtual unit of value equal to 1/1000 of GOP (Currently valued at about $1,50).

9.14. APSaS: Anonymity, Privacy & Security as a Service. Anonymity is our right to manage the level of identity exposure to others; Privacy is your right to enjoy private correspondence and Security is the confidence that no unwanted party will ever be able to read, watch or listen to you.

9.15. Single (Source) Metrics: Single metrics do not provide a full picture nor can they help you understand how your content performs. They are one-dimensional and usually describe a single action that's not necessarily tied to real human behavior. Metrics, received as a result of direct measurement of certain parameters without any additional calculations. Example: Average Usage Time.

10. References.

10.1. Analytics Tools: https://drive.google.com/file/d/1RnEw91c-wtm69qLamcrZ37Pf7onKlIyE/view?usp=sharing

10.2. Behavioral Metrics: https://drive.google.com/file/d/1tDoNcM9xCBV5g6lNKeTCOsRRJLSwg9U5/view?usp=sharing.

10.3. Comparison of Online Dating Services: https://en.m.wikipedia.org/wiki/Comparison_of_online_dating_services.

10.4. Intellectual Property Management by the Government of Israel: https://drive.google.com/file/d/1c9NiYLmwdQHHDvOhxiP2TMI99W4bmcxh/view?usp=sharing.

10.5. FinTech Users: https://globalfindex.worldbank.org/, https://www.statista.com/outlook/295/100/fintech/worldwide.

10.6. Mobile Phone Messaging App Users Statistics: https://www.statista.com/statistics/483255/number-of-mobile-messaging-users-worldwide/.

10.7. Online Dating Services Statistics: https://www.statista.com/outlook/372/100/online-dating/worldwide#market-revenue.

10.8. Revenue per User by Messaging Apps: https://www.statista.com/statistics/746028/average-revenue-per-user-among-messaging-apps/

10.9. Security Segment Services: https://www.statista.com/outlook/281/100/security/worldwide.

10.10. WeChat Revenue and Usage Statistics: https://www.businessofapps.com/data/wechat-statistics/

10.11. WhatsApp Users Worldwide: https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/.

END