PAPYRUS

Decentralized Advertising Ecosystem

1 VISION

Blockchain technology is rapidly changing the way applications are built and function on the Internet. Its key advantages, decentralization and security, offer tremendous potential for reordering the Internet landscape. Advertising, the blood and fuel of the Internet economy, is on the verge of a blockchain revolution and we have a vision to disrupt the chaotic patterns and inefficiency of digital advertising by building a completely new advertising technology stack. Papyrus will be the future monetization vehicle of decentralized Internet applications and transform online advertising into a highly transparent, consistent and lucrative domain for all the participants in the advertising value chain.

We believe disruption can be both a competitive advantage and inclusive. Our vision is to provide tools that enable seamless interconnectivity between decentralized applications and traditional advertising to make this transition both attractive and smooth for existing publishers and advertisers.

We are a team of experts with strong backgrounds in building and scaling successful business processes in both advertising and blockchain technologies. We are challenging ourselves to realize the next breakthrough in AdTech space not only as entrepreneurs developing new technology and markets, but as pioneers of the new sharing economy who want to change the core relationship between advertisers and consumers from one of conflict, invasion and annoyance to an environment of partnership, transparency and profit sharing.

Today, real time bidding (RTB) protocol is a common standard for online advertising. The Papyrus ecosystem will transform this to support decentralized applications and to radically improve the function of the existing programmatic advertising stack with better privacy and transparency using blockchain architecture.

Papyrus will be an all-new global ecosystem committed to forward thinking technology and transparency in the form of a global decentralized autonomous organization (DAO) governed by token-holders and developed by the Papyrus Foundation. In this spirit, all Papyrus components and libraries will be open sourced.

Papyrus tokens (**PPR**[2]) will become the basic tokens for decentralized Internet advertising. All payments, exchanges, incentives and fees on the Papyrus decentralized market for digital advertising will require **PPR**. The total supply of **PPR** tokens will be limited to the amount of tokens created during the initial **PPR** token sales described below.

[1] https://ethereum.org/dao

[2] PPR is the name of Papyrus ERC20-compliant token, https://theethereum.wiki/w/index.php/ERC20_Token_Standard

OUR CORE OBJECTIVES:

◆ **To build the world's most efficient digital advertising ecosystem.** Blockchain technology, decentralization and scalability solutions will enable Papyrus to:

■ Preserve sensitive data that users want to keep private while still enabling precise audience targeting using appropriate data processing;

■ Compensate users directly for voluntarily sharing their personal data;

■ Build a sophisticated value-based reputation system that significantly decreases the level of non-human traffic and other types of fraud between participants;

■ Minimize the risks for advertising businesses from excessive government regulation, criminal attacks and security breaches;

■ Increase the agility of all business processes by enforcing everything in real-time via blockchain smart contracts and state channels [3] to eliminate transactional bureaucracy, corresponding offline paperwork and the need for traditional bookkeeping;

■ Create an economy that incentivizes the developer community to produce more and more efficient applications that solve practical tasks in advertising;

■ Dynamically balance the interests of users, publishers, advertisers and developers for smooth, accelerated and economically viable progress towards new and more efficient advertising products.

◆ **To incentivize the adoption of Papyrus within the global digital advertising market.** By presenting open source libraries and approaches that simplify the integration of Papyrus with traditional digital ad-tech solutions, we will ease adoption of the ecosystem into the online advertising industry. Classic digital advertising companies should be interested in integration because it provides them with much higher efficiency and access to the growing ad supply and demand within the ecosystem with low entry cost barrier. Even major advertisers will ultimately be interested in integration such a truly global, transparent and ultra-efficient digital advertising ecosystem.

◆ **To become the industry standard for digital advertising.** Our ultimate goal for Papyrus is to become the global industry standard for all digital advertising business within a decentralized economy on a single liquidity pool. The Papyrus marketplace is designed to offer fair remuneration and other benefits to all participants in transparent exchange for their product offerings, contributions and collaboration. At the same time, the marketplace will present organic penalties to those who seek to abuse the market, other participants or in any way purposely reduce the ecosystem's efficiency through intentional deception or non-transparent efforts to gain advantage.

◆ **To create a fully open and transparent ecosystem.** We will maintain market leadership and create a robust ecosystem around a basic infrastructure of open source components developed by the Papyrus team. The Papyrus design with DAO governance will be flexible enough to upgrade contracts, protocols, adjust fees and enforce other necessary structures and agreements developed and driven by the community of users and developers.

---

[3] http://www.ibtimes.co.uk/ethereums-vitalik-buterin-explains-how-state-channels-address-privacy-scalability-1566008

2.1. CHALLENGES OF TRADITIONAL DIGITAL ADVERTISING

Digital advertising is a $200+ billion industry that has transformed the way we market goods and services, but remains today a piecemeal system of incompatible components with a host of problems. While there are opportunities for improvement, the possibility of comprehensive re-engineering the current digital advertising ecosystem faces insurmountable barriers in terms of cost, regulation and cooperation. The current market for digital advertising was innovative for the needs of the early Internet, but that time has passed. Today it grows in complexity,[4] but its structures are inherently outdated and incapable of any magnitude of reform. Persistent 'incurable' issues of the current system include:

◆ **Poor user experience.** Most of digital ads on our screens are irrelevant and annoying. They are invasive, generate abusive attention and rob user time. Publishers that focus on excellence for user experience are cautious about placing too much advertising pressure on their user base and losing money. Users don't have the power to define their own rules for what and how many ads they want to see. Keeping the right balance between adequate monetization and a positive user experience has become a headache with fewer and fewer rewards for all parties involved.

◆ **Lack of data privacy.** Today we see a dangerous tendency towards the indiscriminate collection and use of user data. An amazing array of technology is being deployed to track user activities on websites and inside mobile apps. This informationis being deployedfor different business purposes such as targeted ads and other marketing even including unwanted direct phone calls, dynamic pricing at online stores, bank credit and insurance scoring — all without the consent or compensation of users from whom this data is mined. The emergence of Internet of Things (IoT) technology promises an environment where almost every move that user could be tracked. Legal regulations in the sphere of privacy are doomed to always lag far behind technological progress and thus user privacy is expected to be on a continually decreasing slope.

◆ **Net deficit of targeting information.** Not only is user data collected by multiple parties in an uncontrollable, chaotic manner without any control or input from the end user, such uncoordinated efforts are incomplete, mismatched and inefficient. Parties usually do not share information and nobody is ever able to develop a full and up to date user portrait.

◆ **User animosity.** Users have little or no incentive to share their personal data because they fear, quite legitimately, their data will be used abusively. In traditional digital advertising it is inconceivable that users themselves could be compensated for sharing data.

[4] https://martechtoday.com/infographic-marketing-technology-landscape-113956

- ❖ **Innovation against advertising.** The popularity of Adblock and other similar applications continues to grow as the only hope of diverting unwanted advertising.[5] This results in decreasing revenues for publishers and increased pressure on the remaining users without Adblock.

- ❖ **Long, inefficient chains of intermediaries between advertisers and publishers**. Many of the intermediaries in the current digital advertising structure do not necessarily bring any real value to the market. At the same time, all such intermediaries, by their very existence, increase the cost of doing business. Furthermore, because of non-transparent information flows, advertisers lack information about their actual traffic costs and publishers can't account for actual expenditure.

- ❖ **Massive levels of fraud.** Advertisers are forced to use multiple third-party measurement, analytics and verification tools to fight the rampant fraud in the traditional digital advertising system. This diverts resources and ultimately contributes greatly to costs.

- ❖ **Poor user-conversion attribution mechanisms.** Advertisers often don't understand what ads trigger desired user actions, for example purchases. Digital advertising has become increasingly less measurable and actionable over time because of changing user dynamics, fragmented information and layers upon layers of transparent and non-transparent code that reduces efficiency of ads.

- ❖ **Inefficient value exchange.** The using of fiat currencies for all transactions and settlements creates excessive accounting workloads, financial paperwork, unnecessary delays and adds cost layers.

All of these problems are endemic to the fragmented traditional digital advertising ecosystem. Furthermore, none of them can be solved by the centralized architecture used by current advertising platforms because all parties in the advertising value chain are continuously looking for new technical tricks to gain competitive advantage at the expense of other players. This is a never-ending cycle competition that by definition cannot overcome the issues that plague all participants on the market. These issues can only be solved by the introduction of a new, decentralized architecture common to all parties in the digital advertising world that will naturally balance the needs and goals of all parties involved.

In addition to spawning many varied, complicated and incompatible advertising technologies on the market and uncountable intermediary participants feeding off the resulting incompatibility, the chaos of the traditional digital advertising model leads to a digital advertising landscape of terrible inefficiency. Advertisers have to deal with long chains of intermediaries, including advertising agencies, media buyers, resellers, affiliate networks, affiliate marketers and advertising networks. A significant portion of the competition for advertising budgets is simply parasitic and brings no clear value to the table.

In most cases, advertisers don't even really know how their budgets are distributed and spent. Research suggests that more than a half of traffic that advertisers pay for is non-human bot traffic or fraudulent[6]. Another significant part of ad budget is spent on intermediaries. On average, this means that for every $1 spent, an advertiser receives less than $0.5 of value. eMarketer estimates the 2017 worldwide digital ad market volume at $223.74 billion — which means that over $110 billion[7] is wasted.

---

[5] https://www.emarketer.com/Article/US-Ad- Blocking-Jump-by-Double-Digits-This-Year/1014111

[6] http://eltoro.com/case-advertising-fraud-non-human-traffic-viewability-need-know/

[7] https://www.emarketer.com/Report/Worldwide-Ad-Spending-eMarketer-Forecast-2017/2002019

The emergence of decentralized applications, known as dApps — a new form of applications based on blockchain technology — offers a huge opportunity to establish an entirely new decentralized, trustful market for advertising. These applications operate autonomously, openly and accessible to all. What's more, dApps offer previously unimaginable imperviousness to any kind of central point of failure attacks. Carefully designed dApps fulfill exact requirements regarding user data privacy, availability and reliability that allow informational and monetary exchanges between users, creating an unprecedented level of security and trust available through open source code and consensus algorithms to perform critical functions. Projects like Ethereum[8] and Blockstack[9] have had significant success in developing the dApps ecosystem that is already rapidly evolving. In the coming years, thousands of new dApps will appear and they will require a dedicated advertising ecosystem for monetization.

The Papyrus project aims to provide just such a next generation ecosystem for a fair exchange of value between users, publishers and advertisers. We aim to deliver a post-industrial marketplace where users control which ads they want to see, who has access to their personal information and market determined compensation for their data, attention and actions. In the decentralized Papyrus digital advertising market ecosystem, all parties will be incentivized to find equilibrium between their interests and resources to obtain maximum value for themselves or the organizations they serve.

For Users:

❖ **Advertising configurability and data privacy.** A unified platform for future dApp based advertising will provide unrestricted freedom for ad formats and response behaviors as well as for the development of tools for configuring a range of targeted advertising experiences that permit users to exercise precise control over what ads they see and what data they share with advertisers. This arrangement makes adblock type software used to screen out advertising redundant.

❖ **User controlled Internet experience.** With users in control, advertisers will have to focus on enhancing the user experience instead of pestering users. Users will see only relevant, less intrusive and less distracting ads. This environment will eliminate inappropriate ads and malvertisements.

---

[8] https://www.ethereum.org/
[9] https://blockstack.org/

❖ **Compensation for interaction with ads and for sharing user data.** With the proliferation of specialized reputation, antifraud and identity management tools, the Papyrus ecosystem will ensure that users participating in the sharing economy through consensual data sharing and response to advertisements will be instantly compensated for their actions.

For dApp Developers:

❖ **Flexible infrastructure for the creation of versatile ad-based dApp economies.** Libraries, SDKs and protocols developed by the Papyrus team will enable the unlimited creation of ad monetization models for dApps. Everything from simple banner integrations to native ad distribution within user-reward-based social media platforms like SteemIt[10] will allow developers to focus on their product and easily create own value economies suited to their business goals and which benefit their application users as well.

❖ **More exciting user experience.** With the user in control of the advertising experience and appropriate antifraud mechanisms, risks for inappropriate ads or malvertisement content will be significantly minimized and the delivery of high quality user experiences will be rewarded.

❖ **Quick and affordable dApp promotion.** Developers of dApps will have seamless access to a consolidated user base of existing dApps to promote their applications and token sales. The Papyrus ecosystem will organically accelerate the distribution and adoption of dApps among end-users.

For Traditional Publishers, Ad Networks and SSPs (Supply-Side Platforms):

❖ **Access to high quality traffic from dApps.** The traditional supply side players in the current digital advertising market will have instant access to all high quality demand from the Papyrus ecosystem. Low cost barriers for participation in the Papyrus ecosystem will mean that traditional players will not need to choose between traditional and decentralized advertising ecosystems.

❖ **Higher revenues.** Existing digital advertising participants will be able to take advantage of all the benefits of the Papyrus ecosystem immediately with low transition and integrations costs using special gateways. They will leverage benefits of instant payment settlements on blockchain and transparent advertising demand within the ecosystem.

❖ **Papyrus as a strategy against adblock technology.** The ability of users to directly control their own advertising experience will lead to the redundancy of adblock solutions and their eventual extinction. This will naturally lower operational costs to reach users, increase access to the supply of users and boost revenues accordingly.

[10] https://steemit.com/

For Advertisers and Traditional DSPs (Demand-Side Platforms):

❖ **Papyrus protects advertisers from non-human traffic and ensures brand safety.** Papyrus will include decentralized reputation and antifraud solutions that will form a secure information base for advertisers to make weighted decisions on advertising bids. For example, if a publisher appears suspicious, advertisers can choose to bid with a significant discount or not to bid at all. Using smart contracts, the Papyrus ecosystem will have transparent market conditions in which honest participants will earn more revenue while dishonest will ultimately lose revenue. The structural security of the Papyrus ecosystem will be of magnitudes greater for advertisers than in traditional centralized adtech because of the openness and decentralization of the ecosystem and dynamic matching of economic incentives.

❖ **Papyrus creates transparency for advertiser stakeholders.** By tamper-proof storing of all smart contracts and event logs inside a blockchain and secured decentralized storage, it will be impossible to use corruption schemes within long intermediary chains of ad buying. In the Papyrus ecosystem, advertiser stakeholders will be able to verify directly how ad budgets are spent and to perform in-depth audits of third parties as needed.

❖ **Increased efficiency as a result of incentivizing users to take action using compensation mechanics.** This approach is not new in digital advertising, but in Papyrus it will be a basic infrastructural component allowing instant compensation for users. Advertisers will be able to offer variated compensation schemes for clicks, lead generation, mobile application installations, completed ad video views, sharing posts within social networks and other actions.

❖ **Transparent affiliate exchange.** A popular approach in digital advertising is affiliate marketing, an area with high potential but which is currently plagued by high levels of fraud. The Papyrus ecosystem will allow the creation of a decentralized affiliate exchange where advertisers publish precise offers for execution as smart contracts and affiliates exploit them to achieve their desired goals. As all relationships are subject to transparent and secure smart contracts and decentralized governance by Papyrus, all parties in such an affiliate marketing exchange will operate securely and more efficiently than in traditional affiliate networks.

❖ **Papyrus provides access to unique and valuable audiences.** When traditional DSPs and advertisers integrate with Papyrus, they will instantly have access to dApp audiences representing early blockchain technology adopters. As such, these users could be especially valuable for certain types of advertisers, including token offering marketers.

For DMPs (Data Management Platforms):

❖ **Papyrus provides an open and transparent data market with new revenue streams.** The data market in traditional digital advertising is deceptive because users often don't suspect that their information is being collected and traded. Monolithic players like Google, Apple and Facebook gather personal data and don't transparently inform their users that their data is being collected, this despite the fact that their freemium service offerings are totally dependent on it. Users are not compensated for their data except in kind through the use of free services which, in our times, have come to operate more like a public utility. At the same

time, these big players do not share this data with 3rd parties and monopolize the market. In contrast, Papyrus will provide a transparent data market by creating interfaces to collect and verify user data in exchange for compensation according to user-specified policies. In this way, DMPs will compete with each other to construct more valuable and in-demand data by collecting and processing user data. Selling data to consumers like DSPs will generate unique revenue streams. In fact, the Papyrus ecosystem will create a completely new market with revenue streams for DMPs. In this decentralized market, DMPs could even be created as dApps with artificial intelligence (AI) models trained to compile and exploit data as a commodity in the decentralized computing cloud.

For Adtech Companies and Developers:

❖ **Papyrus is an open, 360° incentivized ecosystem.** The Papyrus ecosystem incentivizes the integration of existing adtech solutions as well as the creation of new technologies capable of increasing efficiency within the ecosystem. All Papyrus libraries and protocols will be open sourced and documented. Every new project developed for Papyrus will be able to conduct its own crowdfunding within the ecosystem and may be supported by the Papyrus Foundation. Papyrus is open to include different implementations of ecosystem components, including SSPs, DSPs, DMPs, antifraud solutions, ad exchanges and many other adtech-related dApps. Developers of different components can establish flexible fees for the use of their resources under the governance of Papyrus DAO.

Common benefits:

❖ **Papyrus enforces payments in real-time without paper agreements.** With the emergence of blockchain technology, it becomes possible to make and receive payments instantly without the delays that encumber paper based accounting systems dependant on chains of contingent processes such as established accounting periods and bank transfer time frames. Smart contracts substitute paper agreements thus reducing expenses on paper work, radically reducing the time needed for transactions and greatly improving overall business efficiency.

❖ **Security and traceability of all transactions.** Every party involved in an ad interaction, from the user to publishers and advertisers, will have access to all relevant information about other parties involved in that interaction and their associated expenses. The Papyrus ecosystem will ensure that this information is available in a reliable and secure manner where everybody gets the exact information necessary.

[11] https://tether.to/

The Papyrus decentralized ecosystem for digital advertising is built on the basis of Ethereum blockchain and smart contracts with state channels and secure decentralized data storage to create a versatile and robust infrastructure that is reliable under a high ad transaction load.

1. Ethereum. Papyrus is being built on top of the Ethereum network because it has proven live implementation, a strong team and a promising roadmap. The Hyped EOS project[12] is also interesting, but it is very far from being production ready. In the upcoming Metropolis release of Ethereum, it will be possible to support anonymous transactions using zkSNARKs[13]. It is also reasonable to expect that Ethereum will successfully resolve the scalability issues. The aforementioned release will make it possible to perform private transactions using zkSNARKs to protect ad buying information from outsiders.

2. State channels. Large ad networks and publishers generate hundreds of billions of ad clicks and at least two orders of magnitude more ad impressions annually. Any attempt to execute smart contracts, even for only a fraction of these transactions, will generate exorbitant gas costs. In its present state, this would surpass the bandwidth of the Ethereum network. A technology called state channels is being developed, however, that is capable of supporting these loads. There are already projects dedicated to using state channels for high-speed payments such as the Raiden Network[14] and Lightning Network[15]. Papyrus will implement similar state channel protocols designed to accommodate real-time bidding (RTB) needs.

3. Secure decentralized data storage. The permanent storage of 10 billion ad events within a blockchain, even assuming that each event would require only a very short record of 32 bytes of data, reach costs approaching 2.2×10^{-6} ETH (store operation gas cost) x 10^{10} x $200 (ETH price at the moment of publication) = >$4 million. It would be absurd to attempt to use blockchain for the storage of all advertising data. The use of secure decentralized storage such as Swarm[16], IPFS[17] with Filecoin[18], or Storj[19] with data history tamper proofing via Merkle tree hash codes stored inside a blockchain is now a far more affordable, realistic alternative. The Papyrus team is engaged in pilot experiments with different decentralized

[12] https://eos.io/

[13] https://en.wikipedia.org/wiki/Non-interactive_zero-knowledge_proof

[14] http://raiden.network/

[15] http://lightning.network/

[16] https://github.com/ethersphere/swarm

[17] https://ipfs.io/

[18] https://filecoin.io/

[19] https://storj.io/

storage architectures to benchmark their properties and choose the most suitable one.

4. Blockchain identity and reputation management systems. By combining blockchain with identity verification, a digital ID can be created for ecosystem participants and function as digital watermark. Such an ID can be assigned to every smart contract transaction. Suitable identity verification protocols, for example the Civic[20] project, which aims to tackle the problem of consumer identity theft and reduce online identity fraud, are already available. Papyrus participants will be able to remain anonymous or to provide their identity to gain trust from other participants and in turn generate various forms of revenue for actions. Identity management is to be supplemented with decentralized reputation management protocols capable of generating dynamic trust scores between parties. The Papyrus team will complete comparative research with different approaches to reputation management with the ultimate aim of establishing DAO governance and dispute resolution that will make the ecosystem resistant to unfair ratings, collusion, Sybil and other possible attacks. Decentralized identity and reputation management in Papyrus will be a key factor in minimizing fraud in digital advertising and significantly increasing ecosystem efficiency.

[20] https://www.civic.com/

There are already several projects that aim to leverage blockchain technology in the area of digital advertising. Each of them focuses on a very specific subset of problems and does not attempt to transform the overall existing advertising landscape strategically.

1. BasicAttentionToken.[21] The BAT project is essentially an initiative to create a token that could be used for transactions within the Brave browser to pay users and publishers in exchange for user attention. Brave is an open source adblock browser developed to ensure user privacy. The main issue we see with BAT is its dependence on the Brave browser to distribution among end users. There are also doubts about whether the BAT project can find acceptable ads without sharing any user data with external parties. Finally, BAT token-holders cannot influence the development of the project since governance of the project is centralized in the hands of the project development team. At the same time, it is reasonable to assume that the BAT team will find solutions to these obvious shortcomings. The Brave browser, along with the BAT project, represents a dApp, which could potentially be integrated quite easily within the Papyrus ecosystem, improving its overall performance. Liquidity for both BAT and **PPR** mediums in this case could be provided through the use of token exchanges.

2. AdChain.[22] AdToken, the token of the AdChain project, can only be used for a single, simple task — the formation of a public registry of "good" publishers. At the moment this project and its token are incapable of solving any other digital advertising industry problems. The AdChain team believes that a simple token-based challenge and verification scheme will be enough to settle problems of fraudulent publishers. It appears, however, that without the introduction of additional mechanisms for fraud prevention the project remains open to various attacks, including dynamic publisher content substitution, which would likely significantly diminish the value of this approach. In Papyrus, the more flexible and sophisticated reputation-based approach is already fully capable of resisting such attacks and fighting ad fraud more efficiently.

3. QChain. [23] QChain is a project which aims to create a smart contract based marketplace for publishers and advertisers with a simple web interface. Publishers and advertisers will find each other on the marketplace and can negotiate advertising deals. The project proposes that some transactions can be negotiated automatically. QChain doesn't provide tools to support high load transaction throughput, however, and so any marketplace established on this framework will be forced to operate with extremely high latency due to the nature of blockchain smart contracts.

4. AdEx.[24] AdEx project is buildling a decentralized ad exchange for advertisers directly buying ad space for their campaigns from publishers. Advertisers will place their bids using advertiser portal dApp, publishers will accept bids using another portal dApp, and users may

[21] https://basicattentiontoken.org/

[22] https://www.adchain.com/

[23] https://qchain.co/

even specify their ad preferences in another portal dApp; then for actually serving ads based on accepted bids and user preferences - publishers are expected to introduce some changes on their side using AdEx SDK. This approach seems feasible while focus is solely on direct bids based on large conversion goals. It can be complementary to the real-time bidding stack supported by Papyrus as a marketplace for direct deals. We will investigate ways to integrate with AdEx with Papyrus ecosystem.

The following table summarizes key features of the projects described above in comparison to Papyrus.

Papyrus Global - Decentralized System for Digital Advertising

	BAT	AdToken	QChain	Papyrus
Decentralized governance of the ecosystem	✗	✗	✗	✓
Incentives for developer community to build new applications for Papyrus	✗	✗	✗	✓
User attention and action compensation	✓	✗	✗	✓
User data disclosure compensation	✗	✗	✗	✓
User privacy enforcement	✓	✗	✗	✓
User advertising policy enforcement	✓	✗	✗	✓
Publisher advertising policy enforcement	✗	✗	✓	✓
Advertising brand safety enforcement	✗	✗	✓	✓
Support of dApp publishers	✗	✗	✗	✓
Support of custom dApp economies	✗	✗	✗	✓

[21] https://www.adex.network/

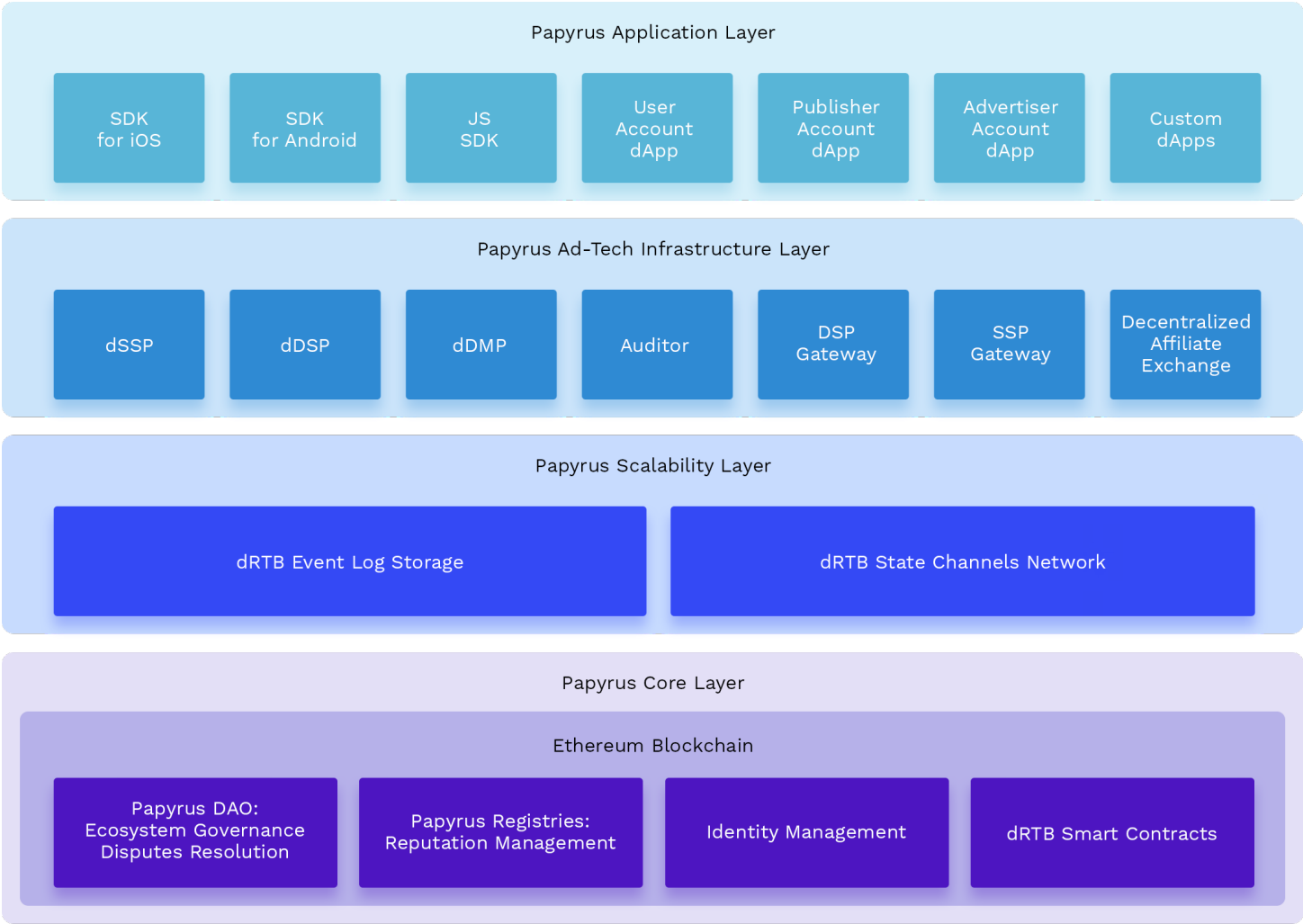|	BAT	AdToken	QChain	Papyrus
Cryptocurrency ad payments	✔	✘	✔	✔
Scalable transactions throughput (1000000+ transactions per second possible)	✘	✘	✘	✔
Decentralized programmatic buying and real-time bidding (RTB)	✘	✘	✘	✔
Up-to-date precise ad audience targeting	✘	✘	✘	✔
Integrations with data management platforms (DMP) and data marketplaces	✘	✘	✘	✔
Gateways for traditional Supply Side Platforms (SSP) and Ad Networks	✘	✘	✘	✔
Gateways for traditional Demand Side Platforms (DSP) and Ad Exchanges	✘	✘	✘	✔
Support for decentralized affiliate exchanges	✘	✘	✔	✔
End-to-end decentralized digital advertising	✘	✘	✘	✔
Full transparency of ad events for all programmatic buying counterparties	✘	✘	✘	✔
Strong reputation-based anti-fraud	✘	✘	✘	✔
Decentralized dispute resolution processes	✘	✘	✘	✔

Currently, Papyrus represents the only holistic, 360° digital advertising ecosystem project that addresses and provides real technical solutions to all major problems and inefficiencies of the traditional digital advertising industry using blockchain technologies. In short, the Papyrus ecosystem doesn't have any real competition in terms of scale or comprehensiveness. At the same time, it is expected that competition will grow. For this reason, the Papyrus team is focusing all resources on the rapid development and deployment of the Papyrus ecosystem to disrupt and conquer the market.

6.1. ARCHITECTURE

The Papyrus ecosystem can be viewed as several distinct technological layers.

Papyrus Application Layer

| SDK for iOS | SDK for Android | JS SDK | User Account dApp | Publisher Account dApp | Advertiser Account dApp | Custom dApps |

Papyrus Ad-Tech Infrastructure Layer

| dSSP | dDSP | dDMP | Auditor | DSP Gateway | SSP Gateway | Decentralized Affiliate Exchange |

Papyrus Scalability Layer

| dRTB Event Log Storage | dRTB State Channels Network |

Papyrus Core Layer

Ethereum Blockchain

| Papyrus DAO: Ecosystem Governance Disputes Resolution | Papyrus Registries: Reputation Management | Identity Management | dRTB Smart Contracts |

Layer 1 — Papyrus Core

The Core is the very basic layer of ecosystem governance which includes upgradeable Papyrus DAO, smart contracts to maintain registries of different ecosystem participants, contracts for identity management and decentralized RTB support. The Papyrus ecosystem will support a range of identity solutions when they become production-ready, including solutions such as Civic and uPort[25]. Papyrus DAO is responsible for:

- Ecosystem governance;
- Dispute resolution processes;
- Voting on upgrade proposals;
- Voting on fee limits in the ecosystem;
- Distribution of the Papyrus DAO token fund, including incentives and bounties for ecosystem participants;
- Crowdfunding escrow for ecosystem participants.

Layer 2 — Papyrus Scalability

This the Scalability layer includes technologies providing scalability and performance consistency necessary for Papyrus applications in real world programmatic advertising:

- dRTB Event Log Storage. Integration with secure, decentralized storage to store all RTB events and create transparency for all operations. Papyrus will allow integration with any suitable provider. Pilot projects with different providers to benchmark cost effectiveness, speed and reliability in real conditions will help determine which providers are most suitable. The liquidity of PPR tokens will be used to pay for necessary storage using token exchanges.

- dRTB State Channels Network. Implementation of state channel libraries in Papyrus will facilitate the opening and maintaining of a peer-to-peer state channels network. Leveraging the developments of Lightning Network and Raiden Network, the Papyrus ecosystem will introduce state channels adopted for usage in decentralized RTB protocol.

- Decentralized RTB (dRTB) protocol. The Papyrus ecosystem will introduce a dRTB protocol that will serve as an extension of the traditional OpenRTB protocol[26] with antifraud mechanisms and state channels for immediate value exchange between ecosystem participants.
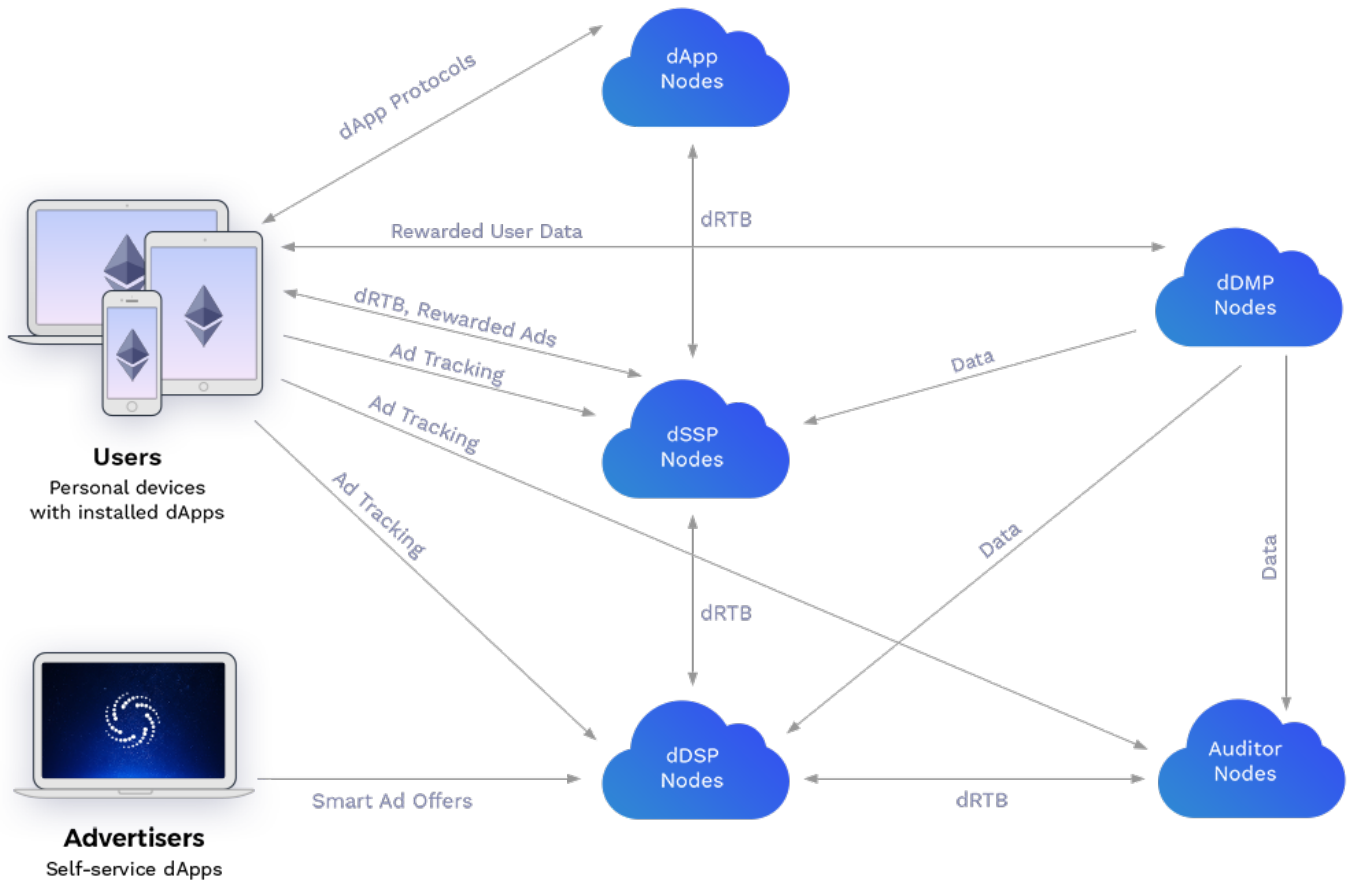
Layer 3 — Papyrus AdTech Infrastructure

The Papyrus AdTech Infrastructure layer includes all components required to establish a complete digital advertising cycle within the Papyrus ecosystem and to create gateways with traditional adtech systems.

---

[25] https://www.uport.me/
[26] https://github.com/openrtb/OpenRTB/blob/master/OpenRTB%20Protocol%20Spec%20v1.1.pdf

Papyrus will publish in open source:

❖ Papyrus iOS SDK, Android SDK and JS library that will

- encapsulate dRTB protocol logic;
- provide API for the integration of ad monetization models to dApps;
- provide API for user data sharing with DMPs;
- provide API for setting up and tuning data sharing policy,
  including balancing of data disclosure and appropriate user compensation;
- provide API for setting up and tuning advertising policy, including
  balancing of ads exposure and appropriate user compensation.

The Papyrus ecosystem will constantly provide upgraded software to support new advertising models and formats inside dApps. In the alpha release, Papyrus will support simple banner integrations and later add other formats such as video and native ads. dApp developers will be free to use their own custom implementations and work with dRTB protocol directly.

❖ **Papyrus dSSP** (decentralized SSP). Decentralized SSP is software for network nodes that will be used by dApps to conduct real-time advertising biddings for ad interactions with users. dSSP can be a part of a dApp itself and perform client-side functions or it can be launched on different network nodes. dSSP is responsible for safeguarding publisher interests by managing ad compensation split between themselves and users. dRTB protocol specifies how compensation for all parties is negotiated and executed in real-time with decentralized security. A dSSP can store all transaction data in dRTB Event Log Storage for later analysis by publishers or audit providers in the event of dispute situations.

❖ **Papyrus dDSP** (decentralized DSP). Decentralized DSP is software for advertising bidding via dRTB protocol. Papyrus will provide its own dDSP implementation with a self-service interface module that will allow advertisers to manage advertising campaigns. Papyrus dDSP will assist advertisers in the initial phase of adapting to the Papyrus ecosystem. It is expected that traditional DSPs and trading desks, with their advanced targeting and optimization algorithms, will adopt dRTB protocol and become more efficient entrance point for advertisers over time.

❖ **Papyrus dDSP Gateway.** Papyrus will create dDSP gateway software that will enable traditional DSPs to connect to the Papyrus ecosystem in a simple integration process and be able to use Papyrus resources for their ads in parallel with their traditional ad operations. To initiate bidding, a traditional DSP will need to buy **PPR** tokens for liquidity and to register as a dDSP in Papyrus registry contract.

❖ **Papyrus dSSP Gateway.** Papyrus will create dSSP gateway software that will enable traditional SSPs and Ad Networks to connect to the Papyrus ecosystem in a simple integration process and obtain additional demand for their inventory. Traditional SSPs will receive **PPR** tokens for their traffic supply and will be able to convert them to other currencies as necessary.

❖ **Papyrus Auditor.** A critical component of the Papyrus ecosystem and the dRTB protocol is fraud prevention. To succeed in achieving unprecedented levels of transparency and security, the ecosystem will provide a special, new type of market participant — the auditor. Papyrus will develop open source basic implementation of auditor. Every Papyrus participant that qualifies with a sufficient volume of network resources to evaluate large amounts of traffic for fraud and other anomalies will be eligible to become an auditor. Such participants will need to make a significant security deposit in Papyrus DAO and register in the Audit Registry. Upon entering any negotiation, contracting dSSP and dDSP parities can make use of any registered auditor or even several auditors simultaneously to review dRTB transaction streams. Such auditors will operate as third party arbiters to decide whether to adjust transactions between users, publishers, dSSPs and dDSPs or not. As part of the process of analysis, auditors may provide participant rankings on the following parameters:

- What is the probability that a user is an unbiased human?
- What is the probability that a user has forged his data?
- What is the probability that a publisher will breach an advertiser's brand security policy?
- What is the probability that an advertiser will breach a publisher's advertising policy?
- What is the probability that an advertiser will breach a user's advertising policy?

Typically, transactions will be adjusted after a brief pause that allows auditors to gather behavioral data about participants to enable more precise ranking.

Aggregated data on all transaction streams will be signed by all parties involved and filed in dRTB Event Log Storage to be used as a basis for Papyrus reputation management. Flexible reputation mechanisms will allow all ecosystem participants to make weighted decisions about bids while making transactions over dRTB. Should a participant demonstrate inappropriate behavior, such a participant will encounter scrutiny from potential partners and thus potentially receive less traffic and fewer bids. With such a setup, all participants become incentivized for appropriate behavior and will consequently enjoy greater efficiency of the marketplace.

❖ **Papyrus dDMP Gateway.** By providing API to compensate users for sharing their data, Papyrus opens up a fair and transparent market for DMPs that gather, orient and actualize user data as a commodity that is processed and presented to data consumers such as dDSPs and which is monetized and capable of generating revenue. Papyrus will implement a dDMP Gateway library that utilizes protocols for compensated user data polling for subsequent analysis and can be integrated with traditional DMPs and simplify their integration inside Papyrus ecosystem.

Layer 4 — Papyrus dApps.

On the basis of the three layers of Papyrus architecture, developers will be able to build any kind of dApps with integrated advertising monetization economies for use within the ecosystem. All dApps integrated with Papyrus will constitute this final 4th layer.

Papyrus itself will release a range of supplementary dApps for the ecosystem:

❖ **Papyrus Account Manager for users.** This will be a place where users can:

- register their identity and receive a Papyrus ID;
- bind their cookies with Papyrus ID to receive payments for ads displayed via Papyrus on traditional websites and mobile apps via SSPs connected to Papyrus using the dSSP Gateway;
- configure a personalized advertising policy — what ads a user wants to see and with what compensation;
- configure a personalized data policy — what data a user is willing to share, with whom and with what compensation;
- display statistics for ad and data interactions and receive compensation;
- withdraw compensation after identity verification to prevent Sybil attacks.

❖ **Papyrus Account Manager for publishers.** This will be a place where publishers can:

- register their identity on a publisher registry and receive a Papyrus ID;
- create advertising integrations for their dApp and receive appropriate codes to begin using them in the ecosystem;
- configure advertising policy for each integration — what ads a publisher is ready to display and with what compensation;
- configure schemes of compensation distribution with users;
- display statistics for ad interactions, received compensation and reputation;
- withdraw compensation after identity verification to prevent Sybil attacks.

❖ **Decentralized Affiliate Exchange.** A decentralized affiliate exchange is an ideal project for the Papyrus ecosystem and the Papyrus team intends to develop it. An affiliate exchange will allow advertisers to simply post offers with clearly defined goals and expenditure limits and begin realizing them utilizing the power of the multitude of affiliate marketers.

Here are some examples of other dApps that could be built on top of Papyrus project:

- **dSSP Mediator** — as Papyrus usage grows, the emergence of different dSSP solutions for Publishers is likely. It will be to the advantage of all participants to allow the mixed usage of multiple dSSPs to maximize revenue. dSSP mediation can be achieved either with a client-side approach or with the help of mediation network nodes;

- **Affiliate Network Gateway** — a dApp, which will aggregate ad offers from traditional affiliate networks and publish them on a decentralized affiliate exchange. The owners of such gateways could generate revenue ad offer fulfillment within the Papyrus ecosystem;

- **Data Tracking and Analytics Provider** — data is critical for making efficient advertising campaigns and for ensuring fairness of the network. Any solution that seeks to improve data metrics will be in high demand and could generate significant revenue.

6.2. MONETIZATION OF DAPPS AND DRTB PROTOCOL

Before diving into decentralized RTB (dRTB) protocol, it is necessary to point out the significant difference in the possible models for monetization of traditional and decentralized applications. Since dApps are usually open-source, centralized models for paying fees or disbursing advertising budgets directly to app developer accounts are not secure. Anyone can make a fork in such applications and cut off or divert compensation. Because of this, the more prevalent approach to dApp monetization is based on the use of application tokens — internal dApp currency. Users can spend them on purchasing scarce resources inside the network, for example, to access content, to use storage space, to rent computing power or bandwidth, to perform transactions and so on. As dApps become more popular, this will lead to a growing demand for tokens and to developers receiving compensation as token-holders.

The dApp token economy based on smart contracts is very flexible, but there remain some difficulties in shaping markets. For example, developers need to structure incentives for users and network supporting nodes. It is possible to incentivize users to use an application by granting them tokens for signing-up, taking desired actions and data sharing. At the same time, it is possible to incentivize network-supporting nodes by granting users tokens for their resources. A special dApp promotion liquidity pool could subsidize some portion of these tokens and other tokens would need to be purchased by dApp users on a token exchange. Network nodes could even invest in a dApp promotion pool to gradually increase demand for their resources and thus increase revenue.

It can be expected frameworks for the simplified creation of an efficient dApp economy will appear soon and Papyrus will be one of the most important building blocks for them. Papyrus will allow dApp developers to easily integrate ads into their applications with automatic distribution of ad revenue between dApp users and dApp resource providers. Such an approach will reduce dApp entry level barriers for users as they won't need to buy dApp tokens themselves and can simply use a dApp network in exchange for their attention to ads delivered by Papyrus. Papyrus achieves this by linking the automatic exchange of **PPR** tokens paid out by advertisers in their equivalent in dApp tokens and their distribution according to dApp network contracts or, alternatively, by simply distributing **PPR** tokens interchangeably with dApp internal tokens if a given dApp should support this.

It can also be expected in the future that closed source dApps and even stores of such applications will appear when some kind of decentralized developer reputation system utilizing smart contracts will be built. Papyrus will be capable of supporting any kind of smart contracts for ad revenue distribution if a dApp user agrees with them.

Let's see how all this works in the dRTB protocol. Here we provide draft protocol description, which is subject to change in the process of further development.

Phase 1. Initialization.

◆ **dSSP registration.** dSSP in the form of dApp will need to be registered in the Papyrus DAO dSSP Registry Ethereum contract to be able to operate in the Papyrus ecosystem and accumulate fees for nodes. To be registered, dSSPs will need to provide a locked deposit of **PPR** tokens the size of which corresponds proportionately to the volume of advertising traffic that the given dSSP wants to serve. Upon registration, a dDSP writes into the registry a signed list of its network nodes and their Ethereum/Papyrus account addresses for fees. The owner of a dSSP can withdraw registration at any time by requesting that its deposit be unlocked. To prevent possible attacks, any given dSSP deposit will be unlocked only after specified period of time, usually a few days. The dSSP will maintain its registration entry by updating the list of network nodes and their ad request processing fees policy if necessary.

dSSPs and other registered entities in the Papyrus ecosystem can link themselves with a variety of identity contract types to increase trust. In this way, Papyrus serves as an identity management agnostic and any Ethereum-based identity management system could be used. Furthermore, the Papyrus DAO can potentially earmark any dSSP registry entry as blacklisted in the event of abusive voting within the ecosystem.

◆ **dDSP registration.** dDSP registration is similar to that of dSSP and is accomplished using a Papyrus DAO dDSP Registry contract.

◆ **Auditor registration.** Ecosystem participants aspiring to serve as auditors will also need to register in a way similar to dSSP registration. This can be done by using a Papyrus DAO Auditor Registry contract.

◆ **Publisher registration.** To use Papyrus, dApp publishers will need to register the dApp in a Papyrus DAO Publisher Registry Ethereum contract. A dApp token reference or an Ethereum Name Service (ENS)[27] name will be used as a dApp identifier. Traditional publishers working in the Papyrus ecosystem through gateways will need to provide their web domains / mobile application IDs as identifiers

As in the case of dSSP and dDSP, publishers will need to maintain the necessary metadata about their dApp, including classification and brand-safety. They will need to provide a security deposit as well. To start displaying ads using Papyrus, a dApp publisher will need to get approval from one or more dSSPs that sign their approval and ensure that the metadata provided is appropriate within the registry. In the event that no dSSP gives approval, then a publisher will essentially be rejected and will be forced

---

[27] https://ens.domains/

to make another attempt to register after a designated period. Papyrus DAO can mark any publisher registry entry as blacklisted upon evidence of abusive voting practices within the ecosystem. Reasons for blacklisting could also include violations of stated metadata, redirects to other resources, content substitution, and other fraudulent practices.

Each publisher / dApp will need to provide a reference to its own implementation of the Papyrus token distribution contract **PapyrusDAppTokenDistribution** between a user and a publisher's infrastructure (dApp network nodes and other resource providers). This contract will be executed upon receiving ad revenue from dDSPs. The execution of such contracts is guaranteed by the Papyrus state channel contract between the dApp user and dSSP. dApp resource providers verify that the user is executing an appropriate contract when working with a given dApp and Papyrus dSSPs. This contract can either convert **PPR** tokens to internal dApp tokens and distribute them accordingly to the status of the users within the dApp or distribute **PPR** tokens without conversion if the dApp network supports this. Reference to a publisher token distribution contract is transparently presented within the publisher's registry so each dApp user can review how it works. To exchange tokens within this contract, it will be possible to use a decentralized exchange, for example **0xProject**[28], **RaidEx**[29], **OpenANX**[30] (currently in development), or Bancor-style token changer smart contract[31].

Papyrus plans to provide linking mechanisms between Papyrus and dApp state channels to support high load dApps. In order to do so, a dApp should be able to manage state channels (between a user and a dSSP and between a user and a dApp network resource providers) simultaneously and to design a dApp state channel contract so that it can work as token distribution contract by settling both state channel and ad revenue distribution on-chain. For example, depending on what a content user is trying to see inside the dApp page, the dApp can estimate how many ad slots should be displayed and with what price limits to cover all dApp network costs for the page view and to proceed simultaneously working with dRTB and dApp state channels for complete payment settlement with Papyrus.

❖ **dSSP and dDSP initialization.** Using Papyrus registries, dSSP nodes will look up and establish connections with dDSP nodes to accomplish mutual verification of identities. Upon verification they can then negotiate anti-fraud policy which can be flexibly defined, for instance:

- dSSP is trusted by dDSP in terms of antifraud and will return payment surpluses to dDSP for non-human and fraudulent traffic;
- dDSP is trusted by dSSP in terms of antifraud and has power to get back payments using dSSP state channel deposits for non-human and fraudulent traffic;
- a designated auditor is trusted in terms of antifraud parameters and has the power to revoke dDSP payments for non-human and fraudulent traffic;
- a designated set of auditors are trusted in terms of antifraud parameters and have power to revoke dDSP payments for non-human and fraudulent traffic in the event of consensus.

[28] https://0xproject.com/

[29] http://www.raidex.io/

[30] https://www.openanx.org/

[31] https://www.bancor.network/

After that, a dDSP opens a state channel **PapyrusDDSPChannel** with a correspondent dSSP using negotiated anti-fraud policy by allocating funds for bidding to multisignature transactions. The amount of funds allocated will depend on the dDSP ad spend volume and chosen antifraud policy. The sum will be obliged to cover total bidding amount for a timeframe long enough to complete traffic antifraud checks.

❖ User initialization. In the Papyrus ecosystem, users are in control of their own exposure to advertising and thus become responsible and enabled to create their own advertising "policy". This includes what ad topics will be allowed and the desired balance between ad load and compensation. Users can change these parameters either in a publisher's dApp itself or in their Papyrus Account Manager dApp. In either case, these parameters are written as a reference to a user's own Papyrus / Ethereum account. Information about which SSPs, DSPs and auditors from Papyrus registries are acceptable will also be stored in user account.

Client-side dApp code reads Papyrus registries from a Ethereum blockchain and checks which dSSPs are available to serve ads to the user within this specific dApp. Using registries, the dApp locates dSSPs nodes ready to process dRTB requests and establish connectivity with them. Upon connection, a client-side SDK/library verifies the identity of nodes by their signatures. dSSP verifies incoming user connections and user attributes for DoS-protection. If all verifications result in positive identification, a client-side SDK/library will initiate a state channel PapyrusUserChannel with dSSP with a special Papyrus contract for its settlement. At this stage, the client-side SDK/library is required to spend some Ethereum gas to open the state channel, but this is a normal function in decentralized architecture and represents an anti-Sybil security measure that can lead to more significant compensation at a later time. To the total amount of gas spent on the usage of state channels by millions of users, dRTB includes a peer-to-peer state channels network similar to Lightning Network, which allows users and dApps to use a path of already open state channels to transact with dSSP.

The Papyrus User Channel is accepted by both parties as a link to a specific Papyrus DApp Token Distribution contract and this link cannot be changed without closing and reopening Papyrus User Channel. If a single Papyrus user is using several dApps at the same time, the user will be required to open several PapyrusUserChannel state channels with dSSPs for each dApp.

When opening a PapyrusUserChannel, a client side SDK/library and dSSP negotiate within the channel contract anti-fraud policy, which also specifies a time-lock period before transfers can be settled and PapyrusDAppTokenDistribution can be executed and how this settlement can be partially or completely cancelled by the parties involved. The duration of the time-lock can depend on user behavior history and identity verification. Various rules can be incorporated to stipulate that payments can be revoked if a dSSP considers traffic to be non-human or fraudulent or if at least two designated Papyrus auditors disagree with it and so on.

This PapyrusUserChannel anti-fraud policy can be renegotiated by a client side SDK/library and dSSP in real time. In this way automated policy adjustments depending on traffic conditions will be possible, and will create a flexible mechanism that prevents payments for fraudulent and non-human traffic and making the overall ecosystem resistant to cartel attacks. Should registered dApps, dSSPs, dDSPs or auditors start abusing other participants, for example revoking all their payments, other parties can contest these actions via Papyrus DAO and provide tracked interactions signed by participants from dRTB Event Log Storage as evidence of fraud. As most token-holders have

an interest in Papyrus efficiency and token value growth, dispute voting will essentially lead to economic punishment for parties who abuse the system and this will stimulate self-regulation and transparency.

Phase 2. Ad bidding.

Bearing in mind that in dApps ad integration may take forms different from simple ad banners and their variations, dRTB will extend traditional RTB from basic impression bidding to bidding for any type of ad event. Possible events could include: a banner impression, a banner click, a message or notification to the user, a compensated video view, compensated lead generation, and other user actions.

With a dRTB, Papyrus uses traditional OpenRTB **BidRequest** over HTTPS signed by the user with a series of innovative modifications:

❖ An extended Imp object to describe possible ad events within any given dApp and to provide information about user motivation concerning the event. For example, whether the event will be explicitly announced as compensated or not will greatly affect the quality of user attention to the event;

❖ First-party user data in a User object is encrypted with a session key. Access will be granted only for DSPs and auditors explicitly accredited by a user's advertising policy;

❖ An additional PapyrusStateChannel object that includes references to:

- User Ethereum/Papyrus account;
- dApp Publisher Papyrus account;
- dSSP Papyrus account;
- PapyrusUserChannel.

When a dSSP node receives a **dRTB BidRequest**, it verifies and redirects this request to connected dDSP nodes to elicit a **dRTB BidResponse** from each of them. Should the dDSP decide to participate in the bidding, it considers factors such as the established PapyrusDDSPChannel anti-fraud policy, PapyrusUserChannel state, publisher brand-safety and other parameters. The **dRTB BidResponse** represents a signed OpenRTB BidResponse with certain amendments:

- A bid is made in **PPR** tokens;
- Additional tracking mechanisms for ad events from dDSP and information about auditors (signed pixel calls, etc);
- An optional requirement for anti-fraud policy adjustment for PapyrusUserChannel;
- Additional PapyrusStateChannel object with a PapyrusDDSPChannel update that includes payment of bid amount to dSSP.

A response already gives a dSSP the ability to settle a bid payment from a dDSP. The dSSP is not motivated to get a bid, however, without evidence of an actual ad event. In the event of encountering irregularities or fraud attempts, a dSSP can stop using a dSSP and even win a possible dispute with such a dSSP. Such a dSSP risks losing revenue, tokens from its security deposit and can be even blacklisted in the Papyrus registry in case of severe violations. If the dDSP requests an anti-fraud policy adjustment,

then the dSSP can either reject the bid or try to adjust the policy and only after that accept the bid for the auction.

The dDSP decides itself which auditors to involve in ad event bidding and adds their tracking to **dRTB BidResponse** if necessary. In simple cases, if the PapyrusDDSPChannel anti-fraud policy implies revocation of payments by dSSP or dDSP, it can function without the involvement of external auditors. The dDSP can adjust its own bid according to PapyrusDDSPChannel anti-fraud policy and fees for auditors for their ad event processing. To pay auditors, the dDSP uses special Papyrus state channels established for this purpose and forwards the dRTB **BidRequest** and **dRTB BidResponse** upon participation in bidding.

Every **BidResponse** undergoes a screening process by the dSSP before it can enter a live auction for a requested ad event. The dSSP checks user and publisher advertising policies / restrictions stored on blockchain to identify whether a bid from the dDSP fits the given parameters. After successful validation, the dSSP node performs the auction between approved responses from dDSPs, calculates **the second price** auction price for the winning bid, signs it and then translates the winning **BidResponse** to the dApp. For the winning bid, the difference between final calculated auction bid and the original bid amount is then returned via the PapyrusDDSPChannel to the winning dDSP, extracting the dSSP bid processing fee according to the dSSP registry. All losing bids are also returned via their appropriate PapyrusDDSPChannels back to the dDSPs, extracting a bid-processing fee. After debiting fees, the dSSP transfers the calculated auction bid via the PapyrusUserChannel to the dApp user for later settlement. As stated above, a user cannot just settle PapyrusUserChannel bid payments in his favor but rather they must be settled with a PapyrusDAppTokenDistribution contract. Settlement succeeds only for amount of payments, which were not revoked within the designated time-lock period by the enforcement of the negotiated PapyrusUserChannel anti-fraud policy.

Since a dSSP is responsible for honest setting a second price auction in the design of dRTB, there emerge potential dSSP cheating scenarios to earn more profit by tweaking the auction.

We propose that a dSSP takes a small bid processing fee as a percent of every dDSP bid. This commission is non-refundable. Thus to maximize profit, a dSSP should accept all valid bids. Invalid bids not conforming to publisher or user advertising policies should not be accepted as they could provoke disputes and losses for a dSSP. The processing fee protects against idle dDSPs that only collect data without making any real bids. The formula for a dSSP fee could be defined simply:

fee = a*sum(b)

where b = bids, a = dSSP-specific constant.

According to this formula, a dDSP will be discouraged from making false bids as they will still incur extra fees paid to dSSP. A dSSP could try to make additional profit, however, by colluding with other parties.

Hiding a second-price bid attack

In case of collusion between a dDSP and dSSP, the latter can pretend that higher bids from other dDSPs never happened or were too late. This could technically lower the dSSP bid processing fee, but

it would also greatly lower payment resulting from winning dDSP that can share part of the profit with a dSSP at the expense of a publisher.

Fake second price attack

A dSSP could also wait until all bids have been made and thencreate a fake bid with the help of a colluding dDSP with a price close to the maximum one offered. This case would theoretically allow colluding dSSP, dApp publishers and dDSPs to get more revenue from winning dDSP.

To prevent these types of fraud, dRTB will support two modes of auction:

- Fast but less secure auctions with a single network round-trip between the dSSP node and dDSP nodes. In this mode, after a dSSP accepts a bid, it signs proof of acceptance and sends it back to dDSPs. After the auction is completed, the dSSP sends results back to dDSPs for their bids along with the winning bid information signed by both dSSP and winning dDSP;
- Completely secure auctions with two-phase commit-reveal scheme[32] where all bids from dDSPs are accepted in encrypted form and only after receiving proof of acceptance do dDSPs reveal their bids to a dSSP. In this case, there are two network communication round-trips between a dSSP and dDSPs to complete the auction, but dDSPs obtain a strong cryptographic guarantee that the second-price auction is resistant to the above mentioned type of attacks.

The first mode is supported for its simplicity and lower bidding latency. Even in this mode, colluding parties trying to perform an attack on a dRTB auction incur significant risks of being caught, penalized and blacklisted. Auditors or dDSPs can catch them by analyzing unexpected anomalies in dRTB event logs.

It is to be expected that the second auction mode will predominate when sufficient number of geographically distributed nodes of dSSPs and dDSPs is live. In a traditional RTB auction there is a 100ms latency limit on receiving a BidResponse from DSPs after a BidRequest is sent. In an environment with high node connectivity, it will be easy to achieve even lower latency for two dSSP-dDSP network round-trips.

When a dApp receives a winning **BidResponse**, it initiates verification according to advertising policies of the user and the dApp and then executes appropriate ad events within the application, activating tracking mechanisms such as auditor-, dDSP- and dSSP-provided pixels specified in the **BidResponse.** The dDSP, dSSP and auditors use the received tracking information for decision-making on whether to try to revoke a bid payment according to PapyrusUserChannel and PapyrusDDSPChannel anti-fraud policies.

To be able to make weighted decisions on bidding and anti-fraud matters, auditors, dSSPs and dDSPs in the Papyrus ecosystem will store and maintain raw dRTB event logs signed by interacting parties for each known user, publisher, dSSP, dDSP with Papyrus accounts in secured decentralized storage — the dRTB Event Log Storage. To provide tamper proofing for historical sequences of

---

[32] https://en.wikipedia.org/wiki/Commitment_scheme

events, event hashes can be used to form Merkle trees and hashes of event blocks can be written into Ethereum blockchain as tamper-proof evidence. In the case where raw event logs need to be presented for dispute resolution, each party can create public evidence to demonstrate that a particular sequence of events actually took place in the past and were signed by participants. Another case for the usage of raw data is to build self-learning AI models for anti-fraud detection. For example, auditors can collect their own raw data and buy data from other participants to train AI models and use them for dRTB payment verification decision making.

Phase 3. Payments settlement.

After a predefined period, any given dApp can initiate a PapyrusUserChannel settlement. Similarly the dSSP initiates a PapyrusDDSPChannel settlement to enforce real payments within the Ethereum blockchain. A PapyrusUserChannel settlement initiates the execution of a PapyrusDAppTokenDistribution to distribute tokens between a user and a publisher's dApp network resource providers. Adjusting the time periods for the initiation of these settlements reduces the load on the core Ethereum network while maintaining the dRTB ability to process thousands of ad events per second.

If there are no disputes on a state channel settlement — on transfers or their revocation — then all parties continue bidding according to market conditions. In the event of a dispute, any party can claim in Papyrus DAO that another party has misbehaved and will be required to provide evidence of this misbehavior. The Papyrus DAO dispute resolution process will enforce actions most suitable for the given case, punishing either the party proven to have abused the system or the party who issued a false or inappropriate claim should the evidence of these motivations be deemed credible.

The anti-fraud policy principles described above ensure that most fraud is virtually filtered out in real-time by negotiated consensus between dRTB protocol parties. In time, a best practice of reviewing transaction behavior of different parties retrospectively after longer periods will likely emerge organically. This will enable auditors and other parties to identify anomalies and to either suggest modification of bidding policies or to initiate disputes should inappropriate behavior or fraud be uncovered.

Papyrus incentivizes this behavior among all ecosystem participants by granting compensation to participants who can identify and provide evidence for misbehaving parties and settle disputes in Papyrus DAO. It is expected that the major arms of the law in Papyrus will be auditors who generate a significant amount of traffic for verification requests and thus begin to build up large knowledge bases useful in detecting and possibly even predicting fraud in the bidding process. It is also expected that anti-fraud processes inside Papyrus will be further self-organized by incentives pledged by Papyrus DAO. For example, it will be naturally rational for ecosystem participants to gather aggregated and verified data about other Papyrus participant's behavior and statistical metrics, to sign and publish them in addition to Papyrus registries so that other ecosystem participants can determine different community ratings for potential counterparties and make decisions regarding the choice of partners for each bidding transaction. Auditors acknowledged by the community will earn more traffic for their verification efforts, earn better reputational ratings and thus earn more total fees and so on. A framework for such reputation management are being researched by Papyrus and will present opportunities for the Papyrus decentralized digital advertising ecosystem community in the near future. A framework for such reputation management is being researched by Papyrus, and will present opportunities for the Papyrus decentralized digital advertising ecosystem community

in the near future. Overall direction and envisioned approaches to reputation management are outlined in the subsequent section.

6.3 REPUTATION MANAGEMENT

One of the cornerstones of the Papyrus ecosystem is reputation management. It is envisioned that all registered participants will have reputation associated to their identity – essentially a complex metric based on their previous behavior and establishing estimation on what behavior to expect from them in the future. For any interaction between the participants, either of the parties can (and should) take into account the other party's reputation when choosing how to interact (e.g. dDSP proposing a higher bid price based on outstanding publisher's reputation) and whether to interact at all (e.g. dDSP deciding not to bid for an impression from a publisher with low reputation) – and as interactions ultimately deliver value to the participants, all the parties are incentivized to behave in way that improves (or, at least does not damage) their reputation. Thus, a reliable, transparent and tamper-resistant reputation management mechanism contributes greatly to eliminating fraudulent behavior and building trust across the ecosystem.

Representing various aspects of complex behavior, reputation is in general multidimensional – it can be viewed as a vector with components depending on the nature and context of interactions participant of a particular type are involved in. Different consumers of this data can interpret reputation components differently, their expectations and trust level can be derived from whole complex patterns identified across several reputation dimensions.

Depending on the source of the data used for calculation, reputation components can be split into two major groups:

❖ Those dynamically derived from the trace of transactions occurring in the ecosystem as part of the main business flows (real-time bidding, auditing and payment, associated disputesresolution, user data exchange). For example,

- large total volumes/amounts of confirmed and payed transactions are positive characteristics of virtually any type of participant;

- large amounts of transactions deemed fraudulent are negative characteristics, mostly for the publisher, but also for the other parties (though to a lesser extent);

- large value lost in the disputes on wrong payment channel settlements significantly reduces credibility of the party.

From a technical standpoint, such metrics can be calculated based on various reputation events – dRTB transaction confirmations/rejections by auditors, payment channel settlement, dispute voting decisions. The Papyrus team will evaluate various metrics of this type for practical feasibility and utility for the ecosystem.

❖ Reputation components derived from the ratings explicitly submitted by some other parties. This approach takes roots in the traditional reputation management which suffers from biased scoring and direct manipulation by colluding parties – and merely tracking such metrics / input scores using blockchain does not solve the problem. As one of the possible approaches Papyrus team will consider building an additional mechanism on top which will promote fair ratings based on verifiable facts reviewed by other randomly selected parties or challenged by arbitrary parties.

In a decentralized ecosystem reputation needs to be calculated and tracked in a decentralized and tamper-resistant manner. Since the amount of reputation events is overwhelming (especially if we consider transactions for individual impressions) reputation cannot be calculated directly on the blockchain – which can only be used as a registry to store reputation calculated by some off-chain mechanisms, and to provide some basis to ensure correctness of such calculations. The Papyrus team will evaluate two possible approaches:

❖ To make parties directly involved in generating reputation events perform calculation using agreed algorithms (and most likely the reference implementations provided by Papyrus), and publish reputation updates. Such parties can be incentivized by a small fee deducted from the 'reputee', and can be discouraged from submitting a wrong update by allowing another party who spotted an error to raise a dispute resulting in penalties against the wrong-doer.

❖ To allow any party to calculate reputation update for another party based on the logged data and trace in the blockchain, and submit it to the registry. Similarly to the above, calculation will be verifiable and any third party could submit a dispute in case of erroneous calculation.

6.4 DATA MANAGEMENT

The heart of programmatic ad buying is data. To satisfy data requirements, Papyrus proposes several means of collecting and using additional information about users.

6.4.1 DDMP CONCEPT

As described above, one of the core concepts of the Papyrus ecosystem is to provide users with the opportunity to control their own data and to earn compensation for by sharing their interests and other relevant ad targeting information with advertisers. Such discrete and user approved data sharing would significantly enhance the user advertising experience.
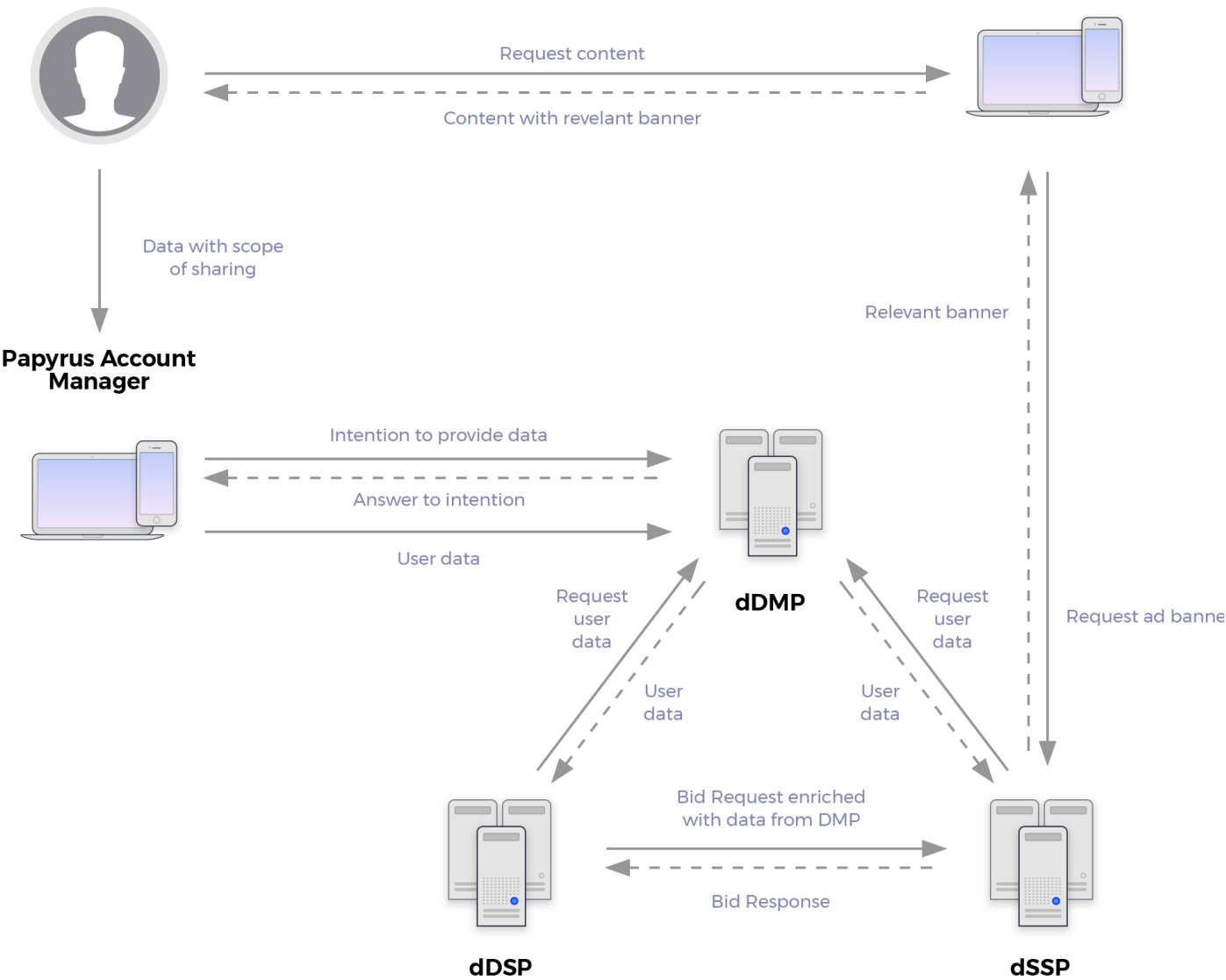
Each user can register an account in the Papyrus ecosystem. This will be possible with the Papyrus Account Manager (PAM) dApp. Users can provide details such as age, gender, general interests, geo-location, device models and so on.

To simplify data collection, the PAM application will connect external user accounts (Facebook, Google, LinkedIn, etc.) via OAuth. This feature will allow account holders to populate their Papyrus user profile in just a few clicks. Also, Papyrus will specify API for other applications that can collect and provide user data automatically. For example, users can connect installed applications on their wearables and other IoT devices. Such applications can aggregate various data, classify it and send to the PAM. Sometimes applications can send raw data (browsing history, viewed banners, etc.) to be aggregated in dDMP later.

The PAM application doesn't store information in any centralized database. Data is stored locally or encrypted and placed in decentralized storage (we will experiment with Swarm and IPFS) or blockchain. The important point is that the PAM application disables sharing of new sets of user data until a user enables this manually. This default step prevents the unintentional sharing of sensitive or incomplete user data.

The PAM is the application where a user can manage any desired advertising and data sharing policies. A user can select user-preferred advertisement topics and set a user-defined blacklist for certain advertisers and ad creatives. This list can be appended through banner interface implementation where a user can simply click on any displayed ad and designate it as inappropriate. Policy settings are shared with advertisers by the same mechanisms as other user data.

The PAM application doesn't connect with dSSP or dDSP directly. Instead, the application provides user data to dDMP instances. The Papyrus ecosystem provides a blockchain registry of dDMPs with their rating. Each dDMP can append itself to the registry and indicate which types of data it can accept. Users can manually choose what data to share, with which dDMPs and at under what conditions.

Although the Papyrus infrastructure offers an unprecedented safeguard protecting users from ads, users are motivated to share their data with dDMPs for several reasons that previously didn't exist:

1. dDMPs will compensate users for their data update;
2. Users will receive more relevant and interesting advertisements in return for providing more complete information about themselves;
3. Users will earn more compensation from advertisers as a result of better ad targeting.

After users adjust their settings in the PAM application, data provision becomes automated. The application connects to the chosen dDMPs, periodically polls them and sends them user data in the event a dDMP is interested in the data update.
In dRTB, requests to dSSP/dDSP can contain a global user ID. If the global ID is provided, it can be used to request additional user data from a dDMP. The dDMP can enrich data not only with basic data provided directly by the user but also with other derivative information about a user, including interest vectors, look-alike segmentations and other augmented forms of data.
This approach satisfies the demand for transparent data access that can evolve with rapid developments in machine learning and AI. Many independent researchers will be able to collect training data sets and develop their own algorithms to improve performance and relevance forecasting in advertising.

6.4.2 DDMP GATEWAY

The other way for advertisers to receive user data while bidding over dRTB is by using traditional DMPs via the Papyrus dDMP Gateway. The dDMP Gateway adds a separate state channel between a DMP and dSSP or between a DMP and dDSP for instant payments (PapyrusDMPChannel). The figure below shows the interaction process in the case where a dSSP uses traditional DMP data.
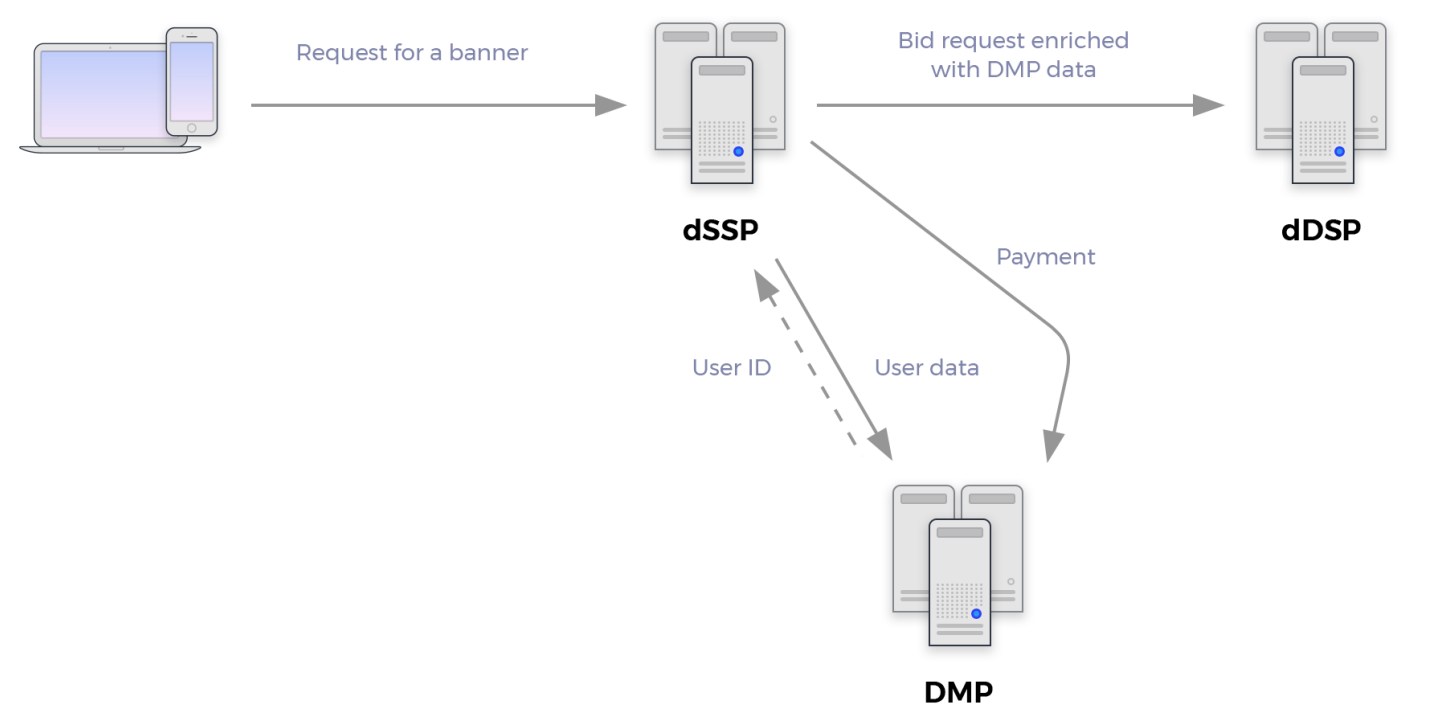
The most obvious external difference with the traditional DMP usage is online payments for user data via PapyrusDMPChannel. As in a traditional RTB, this stage can be preceded by ID/Cookie matching.

Papyrus is planning to use a milestone-based approach and schedule several token generation ("TGE") rounds:

- **TGE Round 1:** Launch on **12th of October 2017** after the deployment of the initial scope of the Papyrus ecosystem prototype in Ethereum network.
- **TGE Round 2:** The **TGE Round 2** will be launched after Papyrus deploys permanent version of the ecosystem smart contracts and successfully launches pilot integrations with target external advertising platforms and partners providing benefits in real use cases. Papyrus expect this will take place in the next few months.
- **TGE Round 3:** Tokens allocated for this event will be locked until 2019. TGE Round 3 will be launched no earlier than in 2019 after Papyrus achieves significant market traction, grows its user base and ad traffic volume within the ecosystem.

Smart contracts for all token sales will undergo independent third party audits from credible companies before launch to ensure the security and integrity of the code.

During **TGE Round 1,** Papyrus will be building out the the Papyrus prototype ecosystem and start pilot integrations with Papyrus partners, including antifraud vendors, publishers, SSPs and DSPs, as well as to attract early supporters of the project and accelerate the establishment and development of a Papyrus expert community.

Papyrus will be introducing two different tokens:

- **PRP – Papyrus Prototype Tokens** that will be used in the ecosystem prototype.
- **PPR – Papyrus Permanent Tokens** that will be used in the permanent version of the ecosystem. These tokens will be generated during **TGE Round 2** and will serve as the permanent tokens of the Papyrus economy during its long-term development and adoption on the digital advertising market.

All **100%** of prototype tokens emission will be exchanged to **15%** of overall permanent tokens emission after **TGE Round 2**. Papyrus plan to suspend support of the prototype ecosystem and continue with development of permanent ecosystem after **TGE Round 2** is complete and the exchange of prototype tokens to permanent ones is opened.

Token Utility

Both **PRP** and **PPR** are a ERC20-compliant utility tokens usable within the Papyrus for:

- Making advertiser payments for ad campaigns;
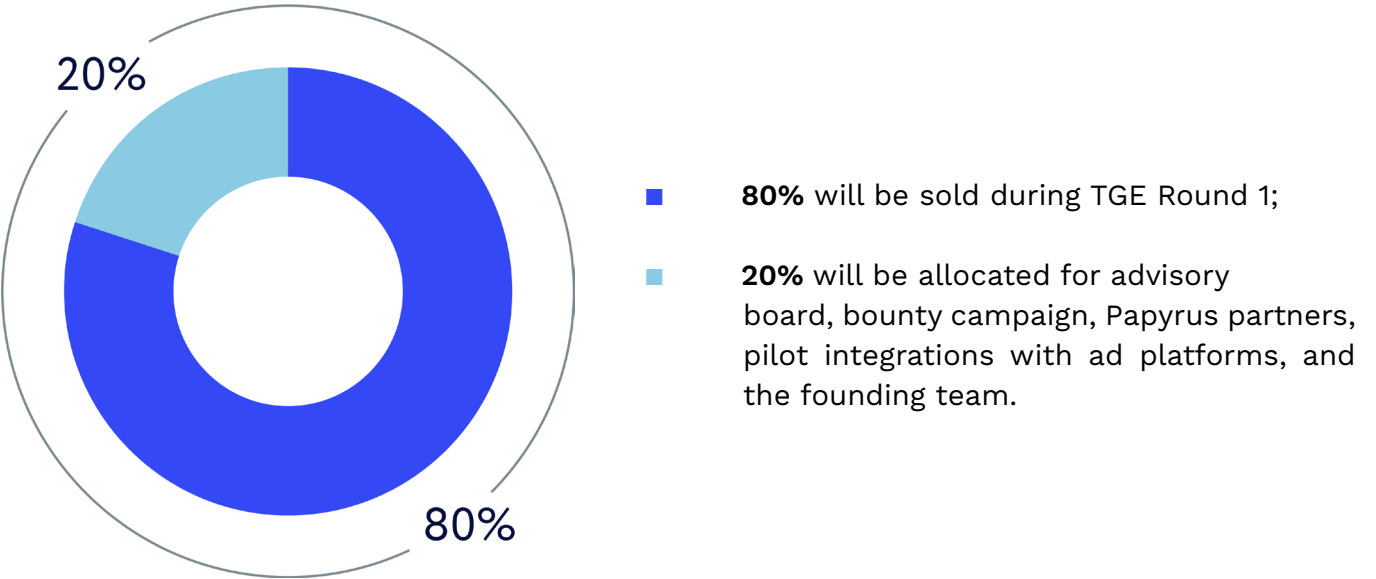- Compensation for publishers and users;

- Proof-of-Stake deposits for connected participants (Publishers, dDSPs, dSSPs, Auditors,Ad Agencies, Advertisers) to ensure fair play and secure Papyrus against fraud;
- Paying service fees to ecosystem participants, including dDSPs, dSSPs, Auditors, and others providers of specific services within the ecosystem;
- Governance of the Papyrus ecosystem, including votes for dispute resolutions, and votes for Papyrus protocol upgrade proposals, changes in basic fee limits and thresholds.

Each ecosystem infrastructure participant (Publishers, dDSPs, dSSPs, Auditors, Ad Agencies, Advertisers) needs to lock a specified minimum amount of Papyrus tokens as a Proof-of-Stake deposit in Papyrus registry. This minimum amount depends on the volume of payments flowing through the participant. There is a default minimum for new registrants of each type. To ensure more trust, improve reputation and get higher ratings registrants are incentivized to make higher deposits. This ensures that demand for Papyrus tokens will grow with the growth of the amount of connected participants and volume of the traffic going through Papyrus-enabled components.

Papyrus Prototype Tokens (PRP) Allocation

PRP tokens will be issued during **TGE Round 1** and will be immediately fungible in the initial prototype of the Papyrus ecosystem. Should the target hard cap be reached, the number of **PRP** tokens will be fixed at the end of **TGE Round 1** and no additional token-generation will be allowed. If the target hard cap is not reached, an additional TGE round for **PRP** tokens may be scheduled. After Papyrus reach hard cap goal as a cumulative result of these TGEs, the amount of **PRP** tokens will be fixed and no additional **PRP** token-generation will be allowed.

The **PRP** token allocation will have the following configuration:

- **80%** will be sold during TGE Round 1;

- **20%** will be allocated for advisory board, bounty campaign, Papyrus partners, pilot integrations with ad platforms, and the founding team.

Token Generation Event Round 1

The **TGE Round 1** includes sale of Papyrus Prototype Tokens **PRP** with hard cap of **$5M.** Any funds raised beyond this will be transmitted back at the cost of the contributor. The Papyrus reserves the right to choose a lower hard cap should it deem this reasonable.

Starting **15th of September 2017** Papyrus opens private pre-order on Papyrus **PRP** tokens. Parties interested in buying **PRP** tokens for amounts of **>=$50k** are invited to participate in a pre-order program of **PRP** tokens with a special discounted token price. All interested parties can submit requests for participation in the pre-order via the official Papyrus website.

Public phase of TGE Round 1 will start on 12th of October 2017 14:00 UTC and will end when any one of the following criterion are met:

- When the hard cap goal is reached;
- When the designated TGE Round 1 public sale period of **21** days ends.

During public phase of **TGE Round 1** any eligible customer can buy **PRP** tokens. Sale will be compliant with international regulations and could be restricted for some jurisdictions. Participants may require undergoing KYC (know your customer) checks for international anti-money laundering (AML) requirements compliance.

PRP price is denominated in **USD** and is specified as follows:

- During first 3 days of the TGE Round 1 period, the PRP price will be **$0.8;**
- From the 4th to the 7th day (both including) of the TGE Round 1 period, the PRP price will be **$0.85;**
- From 8th to 14th day (both including) of the **TGE Round 1** period, the **PRP** price will be **$0.9**;
- After 14th day and until the end of the TGE Round 1 period, the PRP price will be **$1.00.**

Payments for the tokens will be accepted in ETH and BTC using established conversion ratio to USD.

In the event that **TGE Round 1** hard cap is not reached before TGE Round 1 ends, then an additional TGE round for **PRP** tokens may be scheduled to reach the hard cap.

All TGE Round 1 proceedings will be under the management of the Papyrus Foundation Pte. Ltd. (Limited company incorporated in Singapore with UEN: 201726387E) that has a mission to develop Papyrus ecosystem and promote it on the digital advertising market.

Approximate **TGE Round 1** budget allocation:
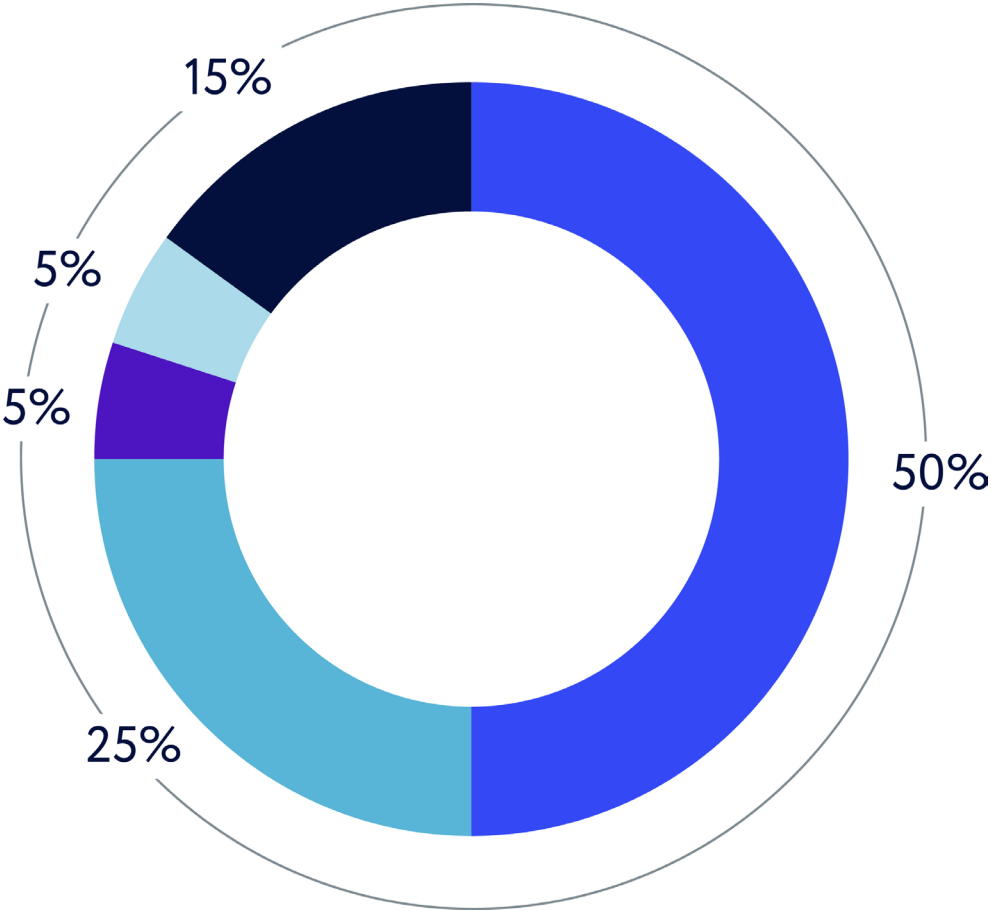
- **50%** will be used for Papyrus ecosystem marketing and promotion, hiring business developers and community managers in different regions around the globe, as well as in building relationships with expert advisors and companies from the advertising and blockchain industries, including making pilot integrations with ad networks, DSPs, SSPs, antifraud vendors and other ad market players.
- **25%** will be used for research and development, including the hiring of development team employees.
- **5%** will be reserved to cover infrastructure costs, such as hardware and office expenses.
- **5%** is reserved for legal costs and counsel.
- **15%** is reserved for motivation schemes for early project supporters and the project founding team.

Papyrus Permanent Tokens (PPR) Allocation

Papyrus - Decentralized Advertising Ecosystem

Overall emission of **PPR** tokens will be limited to **1 000 000 000 (one billion)** tokens. No additional **PPR** tokens creation will be allowed.

PPR tokens will be issued during **TGE Round 2** with the following allocation structure:
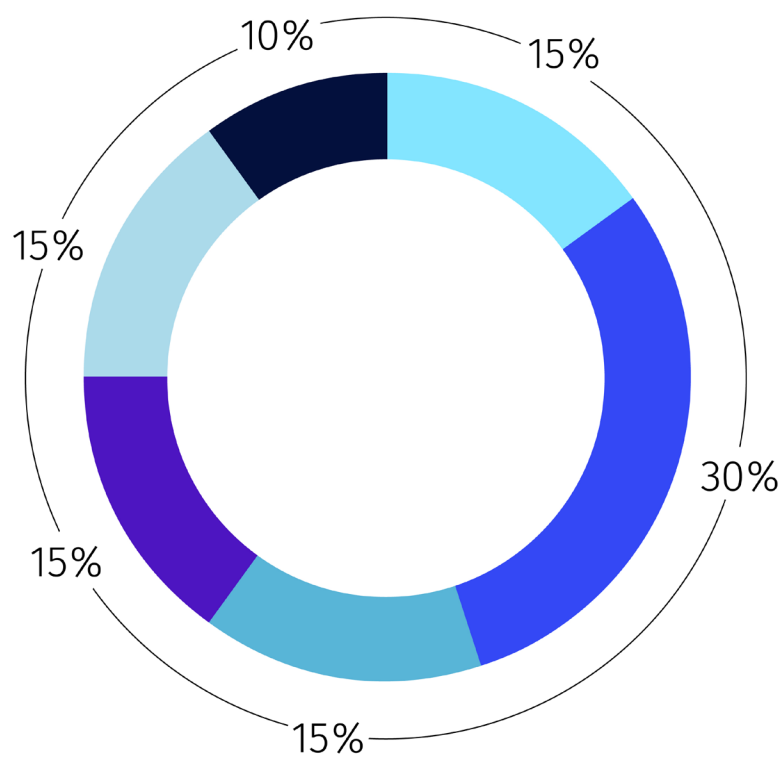
- ■ **15%** will cover **TGE Round 1** and will be distributed to all prototype **PRP** token holders proportionally to their **PRP** holdings in exchange for their **PRP** tokens after the completion of **TGE Round 2.**
- ■ **30%** will be sold during **TGE Round 2.**
- ■ **15%** will be locked until 2019 for TGE Round 3.
- ■ **15%** will be reserved for the Papyrus Foundation Pte. Ltd. (Limited company incorporated in Singapore with UEN: 201726387E) company as a treasury fund. These tokens will be locked for 24 months after the completion of TGE Round 2 with a 6-month cliff. They will act as a surety for the long-term incentive of the company to support ecosystem development. They may be used for different purposes, including employee motivation programs, research and development activities as well as promotional packages for business partnerships.
- ■ **15%** will be used for network growth, including automated incentivization for early ecosystem adopters, bounty campaigns, marketing activities, community building, advisory board compensations, and Papyrus partners' motivation. They will be used to boost adoption of the Papyrus ecosystem worldwide.
- ■ **10%** will be reserved for the Papyrus founding team. These tokens will be locked for 24 months after TGE Round 2 with a 6-month cliff. They are intended to function as an incentive for the original team to continuously drive Papyrus development and adoption.

Purchaser Eligibility + KYC / AML Compliance

Papyrus is restricting the sale of its tokens to citizens and residents of the United States (unless they are certified "accredited investors" within the meaning of the Securities Act of 1933), Singapore and the People's Republic of China.

Papyrus has consulted with legal advisors and shall conduct its token sale in full compliance know your customer ("KYC") rules and regulations across jurisdictions of its sale. Papyrus collects and stores personal information of its purchasers as well as verifies the identity of purchasers.

In addition, Papyrus complies with anti-money laundering ("AML") rules and regulations worldwide and screens token purchasers in accordance with a formal AML policy (the "Papyrus AML Policy") that has been approved by the Board of Directors of Papyrus Foundation Pte Limited. You may view the Papyrus AML Policy at https://papyrus.global/static/AMLPolicy.pdf

Token Ownership

Purchase, ownership, receipt, or possession of PRP or PPR Tokens (the "Tokens") carries no rights, express or implied, other than the right to use such Tokens as a means to participate, interact or transact in the Papyrus ecosystem, if successfully completed and deployed. In particular, Tokens do not represent or confer any ownership right or stake, share, security, or equivalent rights, or any right to receive future revenue shares, intellectual property rights or any other form of participation in or relating to the and its corporate affiliates, other than any rights relating to the provision and receipt of services from Papyrus, subject to limitations and conditions in the Token Sale Terms + Conditions. The Tokens are not intended to be a digital currency, security, commodity, or any kind of financial instrument.

8 DEVELOPMENT ROADMAP

2017 Q1-Q2

- Team assembled
- Project development launched
- White paper published

2017 Q3

- Launch of Papyrus initial prototype in Ethereum mainnet
- Token Generation Event Round 1

2017 Q4

- Pilot projects with Publishers, SSPs, DSPs, Auditors and Advertisers
- First ads served using Papyrus ecosystem
- Scalability stress-testing
- Deployment of permanent ecosystem
- Decentralized RTB documentation v1.0

2018 H1

- Token Generation Event Round 2
- Launch of business development offices in US and UK
- Integration with first dApps, extending their economies
- Papyrus Protostar Release - development and testing
    - Libraries for dRTB Event Log Storage
    - Libraries for dRTB State Channels Network
    - Libraries for Auditor integrations
    - Libraries/Gateway for SSP
    - Libraries/Gateway for DSP
    - JS for Publishers
    - Papyrus Publisher Account
    - Papyrus User Account
    - Papyrus Advertiser Account
- 20 Connected Partners

2018H2:

- **Papyrus Protostar** Realease — first comprehensive release of all basic Papyrus components

- **Papyrus Uprise Release** — development and testing
- Mobile SDKs for Publishers
- Libraries for dApps
- Libraries for DMP
- 50 Connected Partners

2019H1:

- **Papyrus Uprise** Official Release.
- **Papyrus Equilibrium** Release Development and Testing:

2019H2:

- **Papyrus Equilibrium** Official Release.

The following releases schedule will be announced at a later date.

This roadmap is subject to amendments conditioned upon progress in a very dynamic and unpredictable environment. Technology developments and competition from other projects must be taken into account as they arise to ensure that the roadmap is robust and responds appropriately to circumstances in order to achieve Papyrus objectives.

The Papyrus team will make project development results open to the public and will use all available resources to spread information about the project. This includes the creation of a Papyrus knowledgebase with comprehensive documentation and tutorials.

Along with the development of Papyrus ecosystem components, the Papyrus team will pay special attention to ecosystem marketing, business development and community building to achieve adoption of Papyrus worldwide as a standard ecosystem for digital advertising.

Alexander Shvets
Product Director

Alexander has more than 7 years of experience in ad tech and more than 12 years in software development He is a Papyrus Product Director responsible for product vision, coordination between the business, marketing and developer units. He is also a Papyrus evangelist representing the project at conferences all over the world. He has in-depth knowledge of advertiser demand, publisher pain points and agency kitchen environments. Alexander has experience as an entrepreneur and is a co-founder of Marilyn, a leading advertising automation system in Europe. He developed vision of this platform from the ground up and popularized it by his public activities. Before Marilyn, he was immersed in Aori, an advertising aggregator for SME since 2010. Alexander founded Famous meetups MoscowDigital in 2015, connecting advertising professionals from all sides of Digital.

Leo Eletskikh
Technology Evangelist

Leo is a visiting lecturer on Master's programme 'System and Software Engineering' at the National Research University — Higher School of Economics. He has considerable experience in the mobile sphere, including mobile traffic quality analysis and fraud prevention activities at Adjust, application analytics at App Annie, and as a driver of both user acquisition and sales with Alibaba Group. Leo also has a background in investment and banking. He is the founder of @Tabee and @Softlation and continues to advise at these projects.

Elena Obukhova
Comunications Director

Elena has more than 16 years of experience in marketing communications and PR in the spheres of Media and IT. She has diverse professional experience in the development and implementation of communication and promotional strategies. Elena graduated with honors in 2001 from the Institute of International Business Education founded in partnership between the National Research University of Electronic Technology in Russia and the University of Tulsa, US. Her background in leading Media and IT companies includes international television and film production and right holder StarMediaGroup, Sheremetyevo International Airport, CTC Media Group, television channels holding NMG Group and social media network OK.ru.

Tanya has over than 6 year of experience in web and mobile traffic acquisition. She is strong at traffic quality analysis and fraud prevention. She shared her considerable experience with such multinational companies as Banka Intesa, online travel agency anywayanyday.com, largest Russian search engine Yandex. Her knowledge includes Infrastructure development for traffic acquisition and adtech processes automation.

Tanya Krishtopa
Product Manager

Alexander is a Lead Software Engineer at Papyrus responsible for backend development and ad-related technologies. He has a solid background in advertising platform development from his 5 year tenure at Mail.ru and Yandex, two of the largest digital ad-systems in Europe. He has more than 10 years of experience in highload services development with firms such as my.com, Yandex and badoo.

Alexander Kholodov
Lead Software Engineer

Andrey has a degree in Computational Mathematics and Cybernetics from Moscow State University and has a strong technical background and hands-on experience in software engineering. Andrey participated in the infrastructure development for "connected cars" products at tech innovator WayRay as Backend Architect & Team Lead. Andrey has also been a Senior Software Engineer at Sberbank Technology where he has gained significant experience with instant payment technology and financial markets risk management automation in the financial sector.

Andrey Vlasenko
Lead Software Engineer

Igor Sokolov
Block-chain Engineer

Before joining the Papyrus team as a Software Engineer, Igor had an extensive career at Computer Vision working on performance issues in the sphere of computer video and graphics. He has more that 5 years of C/C++ programming experience developing and optimizing critical performance for video decoders/encoders, video editors and rendering using OpenGL. In addition, Igor has years of freelance experience in a range of software development directions. At Papyrus, Igor is responsible for smart contracts and back-end systems of the project development.

Trofimov Vyacheslav
Web developer

Vyacheslav has 6 years of experience in front-end development. He has been a Lead Front-End Developer at rbc.ru, Mnogo.ru and Wildberries.ru. He has been a Lead Engineer / Front-End Developer at Sberbank Technologies

Alexander Telegin
Mobile Software Engineer

Alexander has a degree in Marketing from Saint Petersburg State University and in Information Systems Management from the London School of Economics. Previously he helped drive emerging markets growth in the CEE region at Google working closely with SME advertisers and ad agencies. Since his time with Google, Alexander has turned to iOS mobile development, working on a range of projects, including open source p2p communications framework Thali. Alexander lead iOS development at mobile VR startup FullDive.

Aleksei Pupyshev
Mobile Software Engineer

Aleksei has a degree in Neuroscience from Saint Petersburg State University. Previously he worked as a Data Scientist and Software Developer at QuantumBrains where he contributed to the development of quantitative trading and investment management. After QuantumBrains, Aleksei turned to client-side software development for both Web and iOS at Wrike Inc where he worked on a various projects, including features development for Wrike Workspace and iOS app analytics modules. In recent years Aleksei moved back to Data Science and Engineering. Aleksei lead the R&D team at Wrike Inc. working with marketing/sales/ engineering teams using AI / DL technologies for business and product improvements..

Thomas Hulbert
Ecosystem Evangelist

Thomas has degrees in the Humanities, Communication and Philosophy from California State University, Chico, in the US. He has worked in the US, the Netherlands and Russia and over the past 25 years has developed expertise in corporate communications as a writer, editor and spokesman in the sphere of PR, GR, shareholder communications, and client-side marketing. He is a freelance educational consultant and motivational speaker on the subjects of education, career development and futurology.

Andrey Lyubimov
Research & Analytics

Andrey has a degree in Probability Theory from Moscow State University and has a strong mathematical and financial background. He worked as a Market Risk Analyst at Renaissance Capital and Promsvyazbank. Also he has held the position of Quantitative Analyst at Sberbank CIB. He has exceptional knowledge of critical finance-related IT systems such as Murex and Numerix.