

1. **Название проекта** BitFuncTor
2. **URL** [www.bitfuncutor.net](http://www.bitfuncutor.net)
3. **Краткое описание проекта**

Проект BitFuncTor ставит своей основной задачей развитие интернациональной системы пирингового обмена элементами функционального кода, их спецификациями, доказательствами и классами типов. В качестве второстепенной задачи мы видим повышение уровня профессионального программирования за счет внедрения современных стандартов специфицирования и проверки тестирования кода. Кроме того данная система может использоваться в качестве корпоративной закрытой сети для создания проприетарного или непубличного кода. Коммерциализация проекта реализуется за счет микроплатежей участников сети, продажи архитектурных решений на базе свободного кода сети, продажи готовых программных продуктов или библиотек высоконадежного кода, создания стандартов и прототипов. Кроме того, в качестве способа оценки сложности текущего состояния графа функций, планируется выпуск собственной криптовалюты, выступающей одновременно в качестве «акций» команды разработчиков и единицы экономических отношений внутри сети.

Описание концепции:

- Предоставление сервиса пирингового обмена элементами функционального программирования – кодами функций, спецификаций и доказательств соответствия функций спецификациям (базовый сервис).
- Предоставление платформы обмена элементами кода для компаний – разработчиков программного обеспечения (платный сервис).
- Создание под заказ архитектурных решений и законченных библиотек кода, не требующих тестирования, (разработка ПО).
- Разработка сверхнадежных программных решений для критических отраслей – военная, космическая, медицинская (разработка ПО).

На данный момент ведется разработка прототипа.

#### 4. Концепция / идея

Решаемая проблема:

Одна из важных проблем современного программирования – это чрезмерно большой объем непротестированного или непрофессионального кода, невозможность полноценного повторного использования стороннего кода из-за недоверия или сложности архитектуры. Единицей обмена на рынке софта сейчас являются законченные программные продукты (проприетарные или свободные) и библиотеки функций. Объективная сложность изучения стороннего кода, архитектурных решений заставляет часто принимать решения о собственной разработке с нуля, что существенно удорожает проект, откладывая его во времени. Кроме того, тестирование сторонних библиотек требует несравненно больших усилий, чем тестирование библиотек собственной разработки, а необходимость тестирования как такового является неотъемлемым требованием при создании надежного кода.

Продукт и услуги:

1. Предоставление сервиса пирингового обмена элементами функционального программирования – кодами функций, спецификаций и доказательств соответствия функций спецификациям (базовый сервис);

2. Предоставление платформы обмена элементами кода для компаний – разработчиков программного обеспечения (платный сервис);
3. Создание под заказ архитектурных решений и законченных библиотек кода, не требующих тестирования, (разработка ПО), в том числе разработка сверхнадежных программных решений для критических отраслей – военная, космическая, медицинская (разработка ПО);
4. Выпуск и поддержка криптовалюты, обеспеченной сложностью графа функций и доказательств.

Предлагаемая концепция призвана решить или во многом упростить указанные проблемы за счет:

- Прозрачного способа обмена элементами кода на основе пиринговых сетей.
- Распространяемый код не требует тестирования, его соответствие спецификации строго математически доказано.
- Тестирование архитектурных решений значительно упрощается за счет отсутствия ошибок в отдельных функциональных элементах кода.
- Создание библиотек кода упрощается за счет строгой типизации используемых функций.
- Возможность быстрого прототипирования.
- Отсутствие необходимости изучать сторонний код: достаточно прочесть спецификацию и соотнести ее с требованиями текущей задачи.

Группы клиентов (сегменты рынка):

- Частные разработчики, работающие на компании или в качестве фрилансеров.
- Компании-разработчики программных продуктов.
- Заказчики из критических отраслей экономики.
- Компании или НИИ, ведущие научные разработки.

Технологии, предполагаемые к использованию в системе:

- Технологии пирингового обмена информацией.
- Технологии удаленных вычислений.
- Технологии криптографии.
- Технологии функционального программирования в части моделирования спецификаций и доказательств тестируемых функций.
- Технологии автоматических/полуавтоматических доказательств теорем.
- Технологии встроенных микроплатежей.
- Технологии блокчейна.

## **5. Рынок, продажи и маркетинг**

Клиенты предлагаемой совокупности решений:

1. Частные разработчики, работающие на компании или в качестве фрилансеров. Выгода – быстрое прототипирование, участие в профессиональном сообществе, возможность использования свободного кода, если это не противоречит принципам работодателя, например при ведении научной деятельности.
2. Компании-разработчики программных продуктов. Могут использовать платформу в качестве внутрикорпоративной сети обмена функциональными единицами, имеют возможность быстрого прототипирования. Система сохраняет свои преимущества для больших компаний, даже в случае проприетарных решений – как внутренняя платформа, без возможности доступа извне. Возможен заказ со стороны корпораций

библиотек кода, с заданной архитектурой для ускорения разработки собственного продукта, или заказ прототипов.

3. Заказчики из критических отраслей экономики. Не секрет, что надежность космической или военной техники, или медицинского оборудования сейчас во многом зависит от заложенных программных решений. При наличии масштабного объема доказанных решений, многие задачи критических отраслей могут быть решены быстрее и существенно надежнее, чем прежде.
4. Компании или НИИ, ведущие научные разработки. Наиболее хорошо поддается доказательству код, не содержащий операций ввода-вывода, и именно научные расчеты чаще всего оперируют с таким кодом. Использование платформы для выбора подходящих функций, создание на основании их готовых решений и библиотек могут существенно сократить время для разработки кода научных вычислений, причем приобретаемый код будет абсолютно надежен.

## **6. Преимущества перед конкурентами**

Современные системы тестирования программного обеспечения построены по принципу: спецификация, основной код, план тестирования, тестирующий код, протокол тестирования, корректировка основного кода и т.д. Инновационность предлагаемого подхода в сокращении цепочки: спецификация, основной код, доказательство. В данном случае, если доказательство прошло успешно, ошибки могут быть только в спецификации, но они там могут быть и при традиционном подходе. Если код прошел доказательство соответствия спецификации, его можно не тестировать. Для кода, не содержащего операций ввода-вывода, это доказательство можно провести абсолютно строго. С точки зрения участия в профессиональных сообществах программистов-сотрудников компаний или индивидуальных разработчиков, предлагаемое решение позволит:

1. Во многих случаях автоматически получать ответ на интересующий вопрос, за счет составления спецификации (собственными силами или привлекая нашу команду), и в виду строгой типизации функционального кода находить существующие решения в системе.
2. Формализовать язык общения сообщества в возможных местах, что сократит риски непонимания или двоякого истолкования вопроса или ответа.

На настоящий момент данная задача решается посредством живого общения участников на профессиональных форумах, что, с одной стороны не плохо, но требует от участников дополнительных усилий для понимания друг друга. В качестве общественной выгоды мы получим существенное улучшение качества кода в аспектах его надежности и эффективности, а также понятности для сторонних разработчиков.

В данный момент можно выделить несколько групп конкурентов:

Конкуренты - Группа 1

Компании, предоставляющие профессиональный форум для вопросов и ответов касательно программирования определенного функционала или математических проблем.

StackExchange как технология выполняет функцию платформы для обмена профессиональными мнениями.

1. <http://stackexchange.com/>, Stack Exchange is a fast-growing network of 104 question and answer sites on diverse topics from software programming to cooking to photography and gaming. We build libraries of high-quality questions and answers, focused on the most

important topics in each area of expertise. From our core of Q&A, to community blogs and real-time chat, we provide experts with the tools they need to make The Internet a better place.

2. <http://stackoverflow.com/>, Stack Overflow is a question and answer site for professional and enthusiast programmers. It's built and run by you as part of the Stack Exchange network of Q&A sites. With your help, we're working together to build a library of detailed answers to every question about programming.
3. <http://mathoverflow.net>, MathOverflow is a question and answer site for mathematicians. It's built and run by you as part of the Stack Exchange network of Q&A sites. With your help, we're working together to build a library of detailed answers to every question about research level mathematics.
4. <http://www.codeproject.com>, CodeProject is a community of Software development and Design developers joined together with certain common goals: to learn, to teach and to have fun programming. Developers from all over the world come together to share source code, tutorials and knowledge for free to help their fellow programmers. It is our hope that you find CodeProject to be a wealth of information and a valuable resource. All we ask is that if you find CodeProject useful, then please share what source code or knowledge you can in order to give back to the community. Above and beyond articles and code snippets, CodeProject gives developers a voice. We have over 3.5 million people reading CodeProject each month, including those from companies such as Microsoft, Sun, Oracle, and more. CodeProject brings industry and the developer community together.

Модель монетизации данной группы:

- Реклама
- Лицензирование платформы Stack Exchange
- Поступление от работодателей за счет сервиса поиска работы

Конкуренты - Группа 2: Сервис поиска функций по их функциональной сигнатуре:

5. <http://www.haskell.org/hoogle/>, Hoogle is a Haskell API search engine, which allows you to search many standard Haskell libraries by either function name, or by approximate type signature.

Вдохновители - Группа 3: Peer-to-Peer протоколы

6. [http://en.wikipedia.org/wiki/List\\_of\\_P2P\\_protocols](http://en.wikipedia.org/wiki/List_of_P2P_protocols):
7. Ares (Ares Galaxy, Warez P2P)
8. BitTorrent (ABC [Yet Another BitTorrent Client], Azureus, BitComet, BitSpirit, BitTornado, BitTorrent.Net, G3 Torrent, mlMac, MLdonkey, QTorrent, Shareaza, µTorrent, etc.)
9. Direct Connect (BCDC++, DC++, NeoModus Direct Connect, etc.)
10. FastTrack (Grokster, iMesh, Kazaa, Morpheus, etc.)
11. eDonkey (eMule, Overnet, etc.)
12. Gnutella (BearShare, iMesh, Gnotella, Gnucleus, GTK-gnutella, LimeWire, Mactella, Shareaza, etc.)
13. MANOLITO/MP2PN (Blubster, Piolet, RocketItNet)
14. OpenNap (Napigator, WinMX)

Самый популярный P2P-протоколов для обмена файлами

15. <http://www.bittorrent.com>, BitTorrent Inc. is an Internet technology company based in San Francisco. We design distributed technologies that scale efficiently, keep intelligence at the edge, and keep creators and consumers in control of their content and data. More than 170 million people use our products every month. Our protocols move as much as 40% of the world's Internet traffic on a daily basis.

Вдохновители - Группа 4: Системы создания формализованных доказательств математических теорем и соответствия программного кода спецификации

16. [http://en.wikipedia.org/wiki/Proof\\_assistant](http://en.wikipedia.org/wiki/Proof_assistant), In computer science and mathematical logic, a proof assistant or interactive theorem prover is a software tool to assist with the development of formal proofs by human-machine collaboration. This involves some sort of interactive proof editor, or other interface, with which a human can guide the search for proofs, the details of which are stored in, and some steps provided by, a computer.
17. <http://coq.inria.fr/>, Coq is a formal proof management system. It provides a formal language to write mathematical definitions, executable algorithms and theorems together with an environment for semi-interactive development of machine-checked proofs. Typical applications include the formalization of programming languages semantics (e.g. the CompCert compiler certification project or Java Card EAL7 certification in industrial context), the formalization of mathematics (e.g. the full formalization of the 4 color theorem or constructive mathematics at Nijmegen) and teaching.
18. <http://www.cl.cam.ac.uk/research/hvg/Isabelle/>, Isabelle is a generic proof assistant. It allows mathematical formulas to be expressed in a formal language and provides tools for proving those formulas in a logical calculus. Isabelle is developed at University of Cambridge (Larry Paulson), Technische Universität München (Tobias Nipkow) and Université Paris-Sud (Makarius Wenzel). See the Isabelle overview for a brief introduction.
19. <http://frama-c.com/>, Frama-C is a suite of tools dedicated to the analysis of the source code of software written in C. Frama-C gathers several static analysis techniques in a single collaborative framework. The collaborative approach of Frama-C allows static analyzers to build upon the results already computed by other analyzers in the framework. Thanks to this approach, Frama-C provides sophisticated tools, such as a slicer and dependency analysis.

Вдохновители - Группа 5: некоммерческие ассоциации, вносящие вклад в развитие используемых технологий

20. <http://www.opentc.net/>, The Open Trusted Computing (OpenTC) consortium is an Research & Development project focusing on the development of trusted and secure computing systems based on open source software. The project targets traditional computer platforms as well as embedded systems such as mobile phones. The goal of OpenTC is to protect against system-related threats, errors and malfunctions. The lack of platform security in today's computers has given rise to waves of successful attacks, resulting in severe damages to enterprises and potential failure of critical infrastructures. [http://www.opentc.net/publications/OpenTC\\_PET\\_prototype\\_documentation\\_v1.0.pdf](http://www.opentc.net/publications/OpenTC_PET_prototype_documentation_v1.0.pdf),
21. <http://bitcoin.org>, Bitcoin is one of the first implementations of a concept called cryptocurrency, which was first described in 1998 by Wei Dai on the cypherpunks mailing list. Building upon the notion that money is any object, or any sort of record, accepted as payment for goods and services and repayment of debts in a given country or socio-economic context, Bitcoin is designed around the idea of a new form of money that uses cryptography to control its creation and transactions, rather than relying on central authorities.
22. <http://www.fsf.org>, The Free Software Foundation (FSF) is a nonprofit with a worldwide mission to promote computer user freedom and to defend the rights of all free software users. As our society grows more dependent on computers, the software we run is of critical importance to securing the future of a free society. Free software is about having control over the technology we use in our homes, schools and businesses, where computers work for our individual and communal benefit, not for proprietary software companies or governments who might seek to restrict and monitor us. The Free Software Foundation is working to secure freedom for computer users by promoting the development and use of free (as in freedom) software and documentation — particularly

the GNU operating system — and by campaigning against threats to computer user freedom like Digital Restrictions Management (DRM) and software patents.

Вдохновители - Группа 6: первый успешный продукт, созданный на базе доказательного программирования

23. <http://compcert.inria.fr/>, The CompCert project investigates the formal verification of realistic compilers usable for critical embedded software. Such verified compilers come with a mathematical, machine-checked proof that the generated executable code behaves exactly as prescribed by the semantics of the source program. By ruling out the possibility of compiler-introduced bugs, verified compilers strengthen the guarantees that can be obtained by applying formal methods to source programs. The main result of the project is the CompCert C verified compiler, a high-assurance compiler for almost all of the ISO C90 / ANSI C language, generating efficient code for the PowerPC, ARM and x86 processors.

## 7. Финансовый план (кратко)

Краткий план проекта следующий (от начала проекта):

1. 1-2 кварталы – создание прототипа, общение с инвесторами и потенциальными контрибьюторами проекта.
2. 3 квартал – нахождение финансирования
3. 4 квартал – альфа-версия.
4. 5 квартал – выход бета-версии.
5. 6-7 кварталы – бета-тестирование, общение с инвесторами, PR-акции, обсуждение проекта в блогосфере.
6. 8 квартал – первый релиз.

Объем инвестиций на альфу- \$120 000.

## 8. Команда

**Андрей Ляшин**, магистр физики, физфак СПбГУ, 6 лет работал в ЦНИИ РТК математиком, руководитель группы алгоритмов автономного движения мобильным роботом. Автор ряда публикаций по математическим методом анализа физических явлений, в области управления роботами, заканчивает диссертацию по теме применения мат. аппарата римановых пространств для моделирования траекторного управления мобильными роботами, в том числе с применением функционального программирования (Haskell). Имеет опыт работы в консалтинге, связанном со стратегиями коммерциализации и оценке интеллектуальной собственности. Доказательное программирование — на протяжении нескольких лет является увлечением, владеет несколькими языками программирования (в том числе с теоретической точки зрения). Ряд успешно завершенных проектов. Последние два года — совладелец собственной компании, ведущей, в том числе, инновационные разработки.

Роль в проекте — инициатор, бизнес-девелопмент

**Сергей Егоров**, СПБИТМО, магистр компьютерных технологий, IT-специалист с 15-летним стажем. В течение ряда лет работал программистом, с 2002 года — руководителем в области разработки ПО. Имеет многолетний опыт работы в транснациональных компаниях (Sun Microsystems, Oracle, Orc Software), руководя подразделениями размером до 70

человек из 5 стран. Имеет за плечами десятки успешно завершенных проектов. Последние два года — совладелец собственной компании, ведущей, в том числе, инновационные разработки.

Роль в проекте — Операционное руководство

В качестве вдохновителей проекта есть еще два человека, не включенных в список по причинам защиты приватности (можно встретиться лично 😊).

#### **9. Контакты для оперативной связи**

Андрей Ляшин +79213720428 [al@bitfunctor.net](mailto:al@bitfunctor.net)  
+79312703859