

Open Co-op LLP

Project: OpenCoin

Introduction

Open Co-op LLP was founded in 2004 by Gary Alexander, Senior lecturer at the Open University ICT department, Tom Salfield, BSc in Philosophy and Economics (LSE), Josef Davies-Coates, BSc in Social Policy (LSE) and Oli Sylvester-Bradley, BSc in Sustainable Design (Centre for Alternative Technology).

The Open Co-op was set up to support other cooperatives and social enterprises and to create an international trading network. Intensive research was undertaken, and a community around the website (<http://open.coop>) formed and is maintained up to now. In 2007 Joerg Baach, freelance technologist in the social software field, joined the Open Co-op with the plan to make a new payment system for the internet.

At the moment two products are in development:

- An online collaboration system, which is targeted at cooperatives and social enterprises.
- OpenCoin, an electronic currency system, targeted at business internal use, community systems and payment providers.

The OpenCoin project is the focus of this project proposal.

Project Detail

OpenCoin is an innovative system for creating secure online cash. Maintaining the security of an online money transfer system is typically highly costly and much of the know-how is concentrated in large firms, such as PayPal, who have invested many millions in their technology. This has led to a highly concentrated market with only a few large providers. Consequently, online money transfers are currently expensive and become prohibitive when dealing with small payments. It is not worthwhile to transfer 20p because the charges would be higher than the value of the transfer. This in turn is prohibitive of various micro-payments solutions where many small transactions could create great value. An example would be charging very small amounts of money for sending an email. If there was a charge of 0.001 pence per email sent, it is unlikely this would have a significant effect on the cost of an email to an individual or even a corporate user. However for a spammer this cost would be the difference between profit and loss, thus pricing spammers out of the market. This is just one example of the potential benefits of electronic micro-payments.

Understanding the commercial value of OpenCoin begins with the realisation that computer security is never absolute. Instead, security professionals try to ensure that the cost of breaking into a system is higher than the value of what could be gained through the act. In the case of the current major online payments providers they have a set of central servers which maintain the values of all the accounts, but still have to be accessible through the internet. By compromising a system like this a criminal can gain massive amounts of money and/or valuable data. Hence criminal networks put in many millions of dollars to compromising the servers and systems of the major online payments providers.

In the OpenCoin system, since individuals hold cash, security of money holdings is distributed to those who have the money (much like cash might be kept under people beds in regimes where the banks have been historically unreliable). Since the cost of breaking into millions of systems will be much greater than breaking into just one, and the value of an individuals holdings is likely to be much less than that of a large payment provider, OpenCoin will dramatically reduce the cost of maintaining a secure money transfer system.

There are different multiple potential revenue streams from the development of the OpenCoin system.

- **'Running A Currency issuer (Mint)'** - the cost for issuing electronic coins to the user can be set by the issuer.
- **Microfinance and international money transfer** - It is now the case that 3 times as many people in the world have a mobile phone as a bank account. The ratio is higher if we consider the developing world alone. If people could hold cash on their mobile phones and pay one another at very low cost using the OpenCoin system we could potentially enter this high growth market.
- **'Marketplace for digital coins'** - if there is more than one organisation issuing electronic coins, some issuers will be trusted more than others. There will therefore be a need be for trading these coins against each other, as it is now done with currencies in a currency market. As the creator of the minting system Open Co-op LLP would be ideally placed to be the first-mover in a currency exchange marketplace.
- **Consultancy** - Assuming our proof-of-concept is successful, businesses will need consultancy for integrating the OpenCoin system in to their webshops and other online payments operators will want to adopt the same technologies to reduce the cost of their operation.
- **High quality "virtual" wallets** - there is always room for improvement, and users might be willing to pay for easier more usable wallets or wallets with extended features.

There are several ways to go forward for OpenCoin, as outlined above:

1. running a money issuer,
2. delivering consultancy around the technology or
3. using the system to sell content etc. on the internet, using micropayments.

Key to all approaches is the acceptance of the end-user, and a path to enter the market.

OpenCoin will hopefully have the first market tests within another project - disconnected.net, where it will be used for a community based software. Second, there are plans to use it within the-hub.net network, together with some communication providers, to create an internal payment system. This will give OpenCoin experience running the system as an issuer.

OpenCoin is in discussion with the Wikipedia foundation, who are interested in reducing the costs that donors pay when making donations to them. They paid 45.000 USD to PayPal for 2005 or 2006 alone, and are willing to bridge over to the Mozilla foundation (Firefox etc.), who are the big players (moneywise) in the field. There is quite some interest in using such a software in the Open Source field. So they would be very interested to fund further development as well as using our service offering. With these projects and the high exposure running a micropayment provider OpenCoin might reach the critical mass necessary to become a significant player in the payments market.

Open Co-op is also in intensive talks with a large bank in Germany who are interested in the technology. The talks are in the early stages, but given the booming market in internet sales there is a rather high demand in consulting services and expertise to be expected from this opportunity.

OpenCoin system will support electronic cash, for low cost, anonymous, money transfers. In the OpenCoin system an issuer mints electronic coins, users store them in their electronic wallets and exchange them with other wallets. Users may be end users, businesses, websites etc. The following are some of the major innovative parts of the system:

Anonymity

With real banknotes it can not be traced how people spend their money. This is one of the key properties of cash. With account based systems (e.g. credit cards, bank transfers, PayPal) all transactions are traceable. In OpenCoin the electronic coins are not traceable, therefore users have the same privacy as with banknotes. We will also experiment with variations of the system in which anonymity can be compromised if certain conditions are satisfied.

Peer to peer

Everybody is a user in the system, and is able to receive and spend coins. Business-to-business, intra-organisational, and user-to-user money transfer are all possible.

Wallets everywhere

Electronic wallets can be implemented on mobile phones, in web browsers. It could also be used on a webserver or by other means.

Micropayments

The unit of a coin can be of any size, from very large amounts to very small one. Using OpenCoin it will be possible to allow micropayment, e.g. pay 0.1 pence per page on a newspaper site.

Coins

An issuer can choose freely what to base the electronic coins on British pounds, businesses internal currency, LETS (local exchange trading schemes).

Cheap transfer

Running an OpenCoin system, acting as an issuer, can be relatively cheap, allowing for much cheaper transfers than current systems, which tend to run at 2-3% of the amount transferred.

The OpenCoin project has three different areas.

Software development

In order to run an OpenCoin system, two components are needed: server side software for issuing the electronic coins and redeeming them (issuer software) and software for the clients to handle the coins, to exchange and make payments (wallet). The project aims at getting to prototype stage for both components, which would allow for testing the system and evaluating the user experience.

There is already some existing source code from other open source projects, which we will use where appropriate, and we need to 'only' implement the components.

The core technology is very much proven to be feasible - Deutsche Bank did run a project called e-cash in the nineties, which was using the exact same underlying technology that is proposed for OpenCoin. The development risk is therefore relatively small. We will innovate by implementing variations on the core technology to suit the legal context.

Most of the components of the prototype will be on all target platforms without modification. Platform specific work would need to concentrate on user interface issues only. This is because the implementation work is going to be done in a cross-platform language called Python. Python runs basically on all existing platforms, including smartphones (Symbian as well as Windows).

Continuing cryptographic research and audit

The core of the system is cryptographic software and protocols. Even small mistakes in design or implementation of the cryptographic elements would make the system attackable by an outsider. The current existing protocols would need some extension; the possibility of the extension depends on their effects of security. Therefore an academic cryptographic researcher would be needed on an ongoing basis to help design the protocols in a secure way, feed back (in iteration) into the implementation process and research new issues arising out of the ongoing development.

Legal research

In order to commercialise this technology we will have to have a clear understanding of the legal and financial regulations around running a payment provider. In the UK this will involve research into FSA regulations relating to online payments as well as company law and banking law on a UK and European level.

There are quite a lot of different usage scenarios of the technology, which lead to different regulatory requirements. The exact setup of the technology will determine how the system is treated legally, and the legal environment will therefore have an impact on the design of the system. This is why OpenCoin takes the legal aspects of the development work quite seriously and considers it to be integral to the prototyping phase. Just as a user interface designer develops the interaction with the end user, the ongoing work steps of the legal expert and their research will design the interaction of OpenCoin with the legal system.

The purpose of the legal research is to understand the regulatory requirements that need to shape the technology development, and create a context which supplies enough information for a prototypical run. The limit of the research is the generic use of the technology as a payments system for national currencies – deployment internally in businesses should be handled by legal experts on a per case basis.

We hope that if the system is carefully researched and understood, it will provide a good starting ground and help shape a new business model, enhancing the market for micropayments in particular and payments in general.

Need for Project

The OpenCoin project represents a huge commercial opportunity for the Open Co-op LLP and if successful could be instrumental in decreasing transaction costs of online payments and increasing competition in the online payments market. The Open Co-op needs support from the SME Innovation Programme in order to facilitate the initial phases of the project. The initial phase relies to a large extent on the academic input, while later stages are much more business oriented. Even though the Open Co-op has spent some significant time on researching the topic, evaluating existing systems, running some early software tests, support from the SME Innovation Programme would enable us to complete the first steps, and reduce our time to market. Since the initial research is high-risk investment, it would be hard to raise the investment without at least a portion of grant funding.

Academic Involvement

The opencoin project is dependent on continuous academic input, especially during the phase which is the scope of this application. As outlined above the output of this project is threefold. While the main goal is a working prototype of the server and wallet software, this really is the combined effort of software development, cryptographic and legal research. The combined input and interaction of the participating parties, opencoop working closely together with academic experts during all phases of the projects is key in achieving the goals of the project and delivering the outputs. The expected publications by the academic experts are also key for the general acceptance of the system.

Cryptographer

OpenCoin will benefit from academic involvement in the theoretical design of the protocol, research into implementation issues, correct set-up. Enhancement and structuring of the protocols and components is crucial to the overall security of the system. Continuing audit of the different building blocks of the software is required, as mistakes need to be spotted and corrected as early as possible, and ongoing advice on the cryptographic elements of the system will be needed.

There is already significant scientific and academic work in the cryptographic model which Open Coop LLP intends to exploit. E-cash as invented by David Chaum in the 1970's has sparked a lot of interest in the academic world so far, and early announcements got good feedback from key players in the cryptographic field. Enhancing the system and bringing it to use requires extensive practical testing, and peer review from the scientific community.

In order to allow conditional traceability of the electronic coins (according to the needs of a payment provider) the underlying cryptographic protocols have to be enhanced. There are ideas and concepts of how to do this available within the academic community and the Open Co-op LLP but the practical feasibility of those will only become evident during the implementation phase. The academic working on this project should research the protocol enhancements, doing risk assessments, and making adjustment to the protocol as required during the development. The academic would ideally publish the protocols to the academic world for peer review.

We have an understanding to work on the cryptographic aspects with Prof. Kenny Paterson and Prof. Peter Wild, both from the Information Security Group at Royal Holloway, University of London.

Prof. Kenny Paterson B.Sc. (Hons) (Glasgow), Ph.D. (London) obtained his BSc (Hons) in 1990 from the University of Glasgow and a PhD from the University of London in 1993, both in mathematics. He was a Royal Society Fellow at the Swiss Federal Institute of Technology, Zurich, from 1993 to

1994, investigating algebraic properties of block ciphers. After that, he was Lloyd's of London Tercentenary Foundation Fellow at the University of London from 1994 to 1996, working on digital signatures. He joined the mathematics group at Hewlett-Packard Laboratories Bristol in November 1996, becoming project manager in 1999. His technical work there involved him in international standards setting, internal consultancy on a wide range of mathematical and cryptographic subjects, and intellectual property generation. He also continued with more academic activities. As project manager, he was responsible for running the group and particularly enjoyed the challenge of managing new technology development and transfer to company divisions. Kenny's research interests span a wide range of topics: cryptography and protocols, network security, finite fields and exponential sums, sequences, coding theory and information theory.

Prof. Peter Wild BSc (Adelaide) PhD(London) received his B.Sc. (Hons) degree in Pure Mathematics in 1976 from the University of Adelaide, and the Ph.D. degree in Mathematics in 1980 from the University of London. He has worked at the Ohio State University, Columbus, Ohio; the University of Adelaide; and with the CSIRO, Australia. In 1984 he joined Royal Holloway where he is currently employed as a Professor in Mathematics. His research interests are in combinatorics, design theory, cryptography and coding theory. He has acted as a data security consultant for a number of companies offering advice in algorithm analysis, key management and user identification protocols.

Legal & Regulatory

The technical, cryptographic, legal, and regulatory aspects of this project are intertwined (see above). A legal expert with a profound understanding of financial services regulation issues particularly with regards to the internet, is required to feedback continuously into the project, with specific regard to the legal setup for running an issuer, the legal situation of the clients, and the required setup to allow legal coin issuing in as many use cases as possible.

As no digital cash system has found wide use so far, so in some ways we may be entering uncharted legal territory as is the case with many Internet inventions. The legal arguments need research and publication in the academic world.

On these legal aspects we have found an understanding to work with Prof. Professor George Walker and Professor Chris Reed, both from the Centre for Commercial Law Studies, Queen Mary, University of London.

Prof. George Walker BA, LLB (Hons), DIPLP (Glasgow), DAES (Bruges), LLM (London), PhD (London), DPhil (Oxford), Professor in International Financial Law, is a member of the CCLS . He is a Solicitor in Scotland, England and Wales and a Member of the New York Bar. George is currently an examiner for the Hong Kong University and the Securities Institute and a legal consultant with Farrer & Co. and the International Monetary Fund. He is also a Senior

Fellow in Banking Law at the London Institute of International Banking, Finance and Development Law and a Professorial Fellow at the Asian Institute of International Financial Law, University of Hong Kong and the Institute for International Banking and Finance Law in Dallas, Texas. Amongst his former roles, George was an Affiliate Lecturer in Law at Cambridge University, visiting researcher at Harvard University and acted as a consultant on a number of law reform projects with the World Bank, the EBRD, the Asia Development Bank and with various national governments, and served as Executive Editor of the Financial Times 'Financial Regulator Report' and now Informa 'Financial Regulation International'.

Prof. Chris Reed BA (Keele), LLM (London), Professor of Electronic Commerce Law, is a member of the [CCLS](#). He joined the Centre in 1987 and is responsible for the University of London LLM courses in Information Technology Law, Internet Law, Electronic Banking Law and Telecommunications Law. Chris has published widely on many aspects of computer law and research in which he was involved led to the EU directives on electronic signatures and on electronic commerce. From 1997-2000, Chris was Joint Chairman of the Society for Computers and Law, and in 1997-8 he acted as Specialist Adviser to the House of Lords Select Committee on Science and Technology. Chris participated as an Expert at the European Commission/Danish Government Copenhagen Hearing on Digital Signatures, represented the UK Government at the Hague Conference on Private International Law and has been an invited speaker at OECD and G8 international conferences.

Project Outputs

- Prototypical implementation of the OpenCoin system - issuer and wallet.
- Cryptographic understanding and documentation of the system and publication in the academic world, therefore increasing trust in the system.
- Understanding of the legal and regulatory implications of various payment solutions.

Through achieving these goals, the Open Co-op would gain:

- The chance to deploy an OpenCoin system for real world testing.
- Better understanding and quantification of emerging business opportunities.
- A system to use directly for business growth as well as to incorporate into other projects through a licensing or franchise type exploitation model.
- Move the Open Co-op business towards an investment-ready state.

Work Breakdown

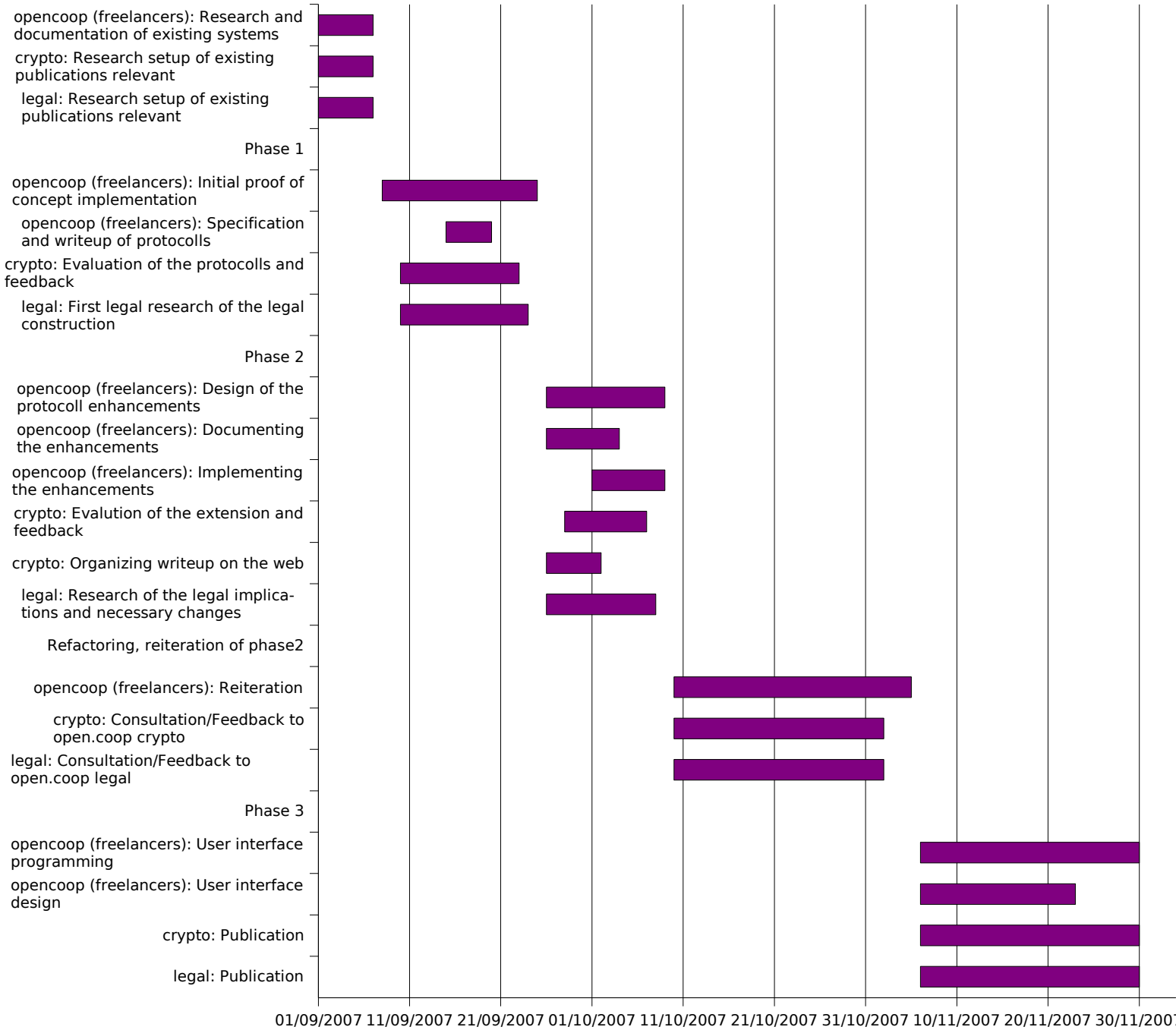
A project/cost plan is attached to the project description.

The project is planned to begin on 1st September 2007 and to be completed by 1st December 2007.

The main activities/outputs are highlighted in this table:

	SME Activity & Outputs	Academic Activity & Outputs
Phase 0	Research and detailed documentation of existing systems	Research set-up of existing technical and legal publications relevant to proposed system
Phase 1	Initial proof of concept implementation, without the enhancements of the cryptographic set-ups. Output: running issuer software and command line driven wallet	Evaluation of the protocols (crypto) First legal research of the system from the perspective of the different business models (legal) - feeding back to phase 2 of the SME activity
Phase 2	Enhancing the system with regards to protocols, implementation on a proof of concept level	Research of the extensions (crypto) Peer review of the extensions (crypto) Research on legal issues around the proposed enhancements (legal)
Phase 2.1, 2.2.	Iteration of the work in phase2, until a satisfactory designed is reached	Iteration of the work in phase2, until a satisfactory designed is reached
Phase 3	Creating the necessary graphical interfaces and components that allow 'end users' to use the system	Publication of the extensions to the scientific community (crypto) Publication of the legal learnings to the community (legal)

Time estimation on project progress



What are the key risks associated with the project?

On the technology side the greatest risk is to not get to a usable implementation of the OpenCoin system, therefore not allowing proper field testing. We aim to mitigate this risk by building upon proven technology, and only augment in iterative steps, employing test driven development strategies. This will lead to a running system in the early stages of the project, which will be improved and extended, but kept in a working stage pretty much all of the time.

On the conceptual level the greatest risk would be to have severe errors in the cryptographic extensions of the protocols. We aim to mitigate this risk by working with academic cryptographic experts during the initial design processes and on an ongoing basis. We will also release all work on open source licences from the very beginning, allowing continual peer review of ideas, concepts and implementation.

On the legal level the main risk is that we may struggle to find a legal setup that allows feasible commercial use of the system. We aim to mitigate this risk by designing OpenCoin in a way that it can be used for multiple purposes, effectively distributing the risk, and using the legal research through the whole development process to shape the system in the most suitable way. This risk does not affect the prototyping stage.