

The Crypto UBI Project (TCUP) Implementation: A Kuwa-Driven Basic Income Faucet

By Jim Flynn with essential contributions from Gavin Andresen and Philip Silva
Last Update: April 12, 2018

***“Ideas are like wheelbarrows;
they go as far as you push them.”***

- Arturo (a wise old friend)

This document is a high-level description of the implementation that The Crypto UBI Project team will deploy during a 12-week project, which will start in May and end in August 2018. We will implement a [basic income faucet](#). That faucet will distribute a cryptocurrency, such as Bitcoin Cash, in periodic payments. To receive payments, users must create valid registrations. The main focus of our effort will be to create the underlying distributed identity system that will validate users. The deployment will be a version of the Kuwa (“to be” in Swahili) system. We will adhere to the *Guiding Principles* laid out in the [Kuwa white paper](#). You should review the Kuwa paper before reading this document.

Team

The project team will consist of three to five developer interns who would likely be M.S. candidates at the UMass College of Information and Computer Sciences (CICS). CICS Entrepreneurs in Residence (EIRs), and perhaps CICS faculty members, will serve as mentors for the project. Jim Flynn, CICS EIR, will be the project manager.

Output

We will release all source code that we develop during this project as open source under the most permissive license available (e.g., MIT). By the end of this project, we will also publish a white paper detailing the lessons we learned and suggesting areas for future work.

Objectives

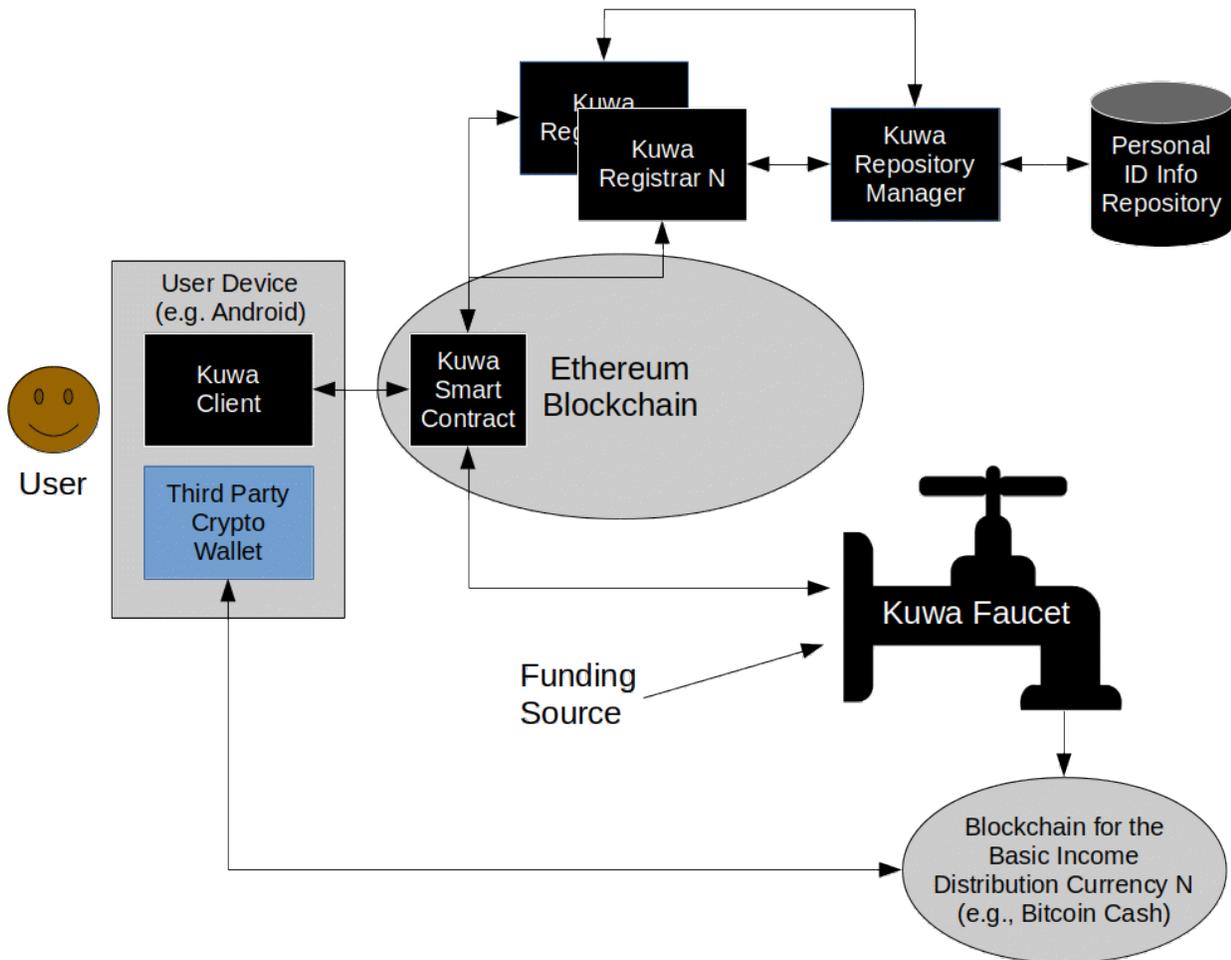
The principal objectives of this project are as follows:

1. **Test the viability of a consensus-oriented distributed ID system** – Bitcoin’s proof-of-work algorithm makes consensus easy, since it is math-based. But identifying humans is a far more organic task. Our brains do it well. Straight-up math cannot do it alone. This project will implement a consensus algorithm, including rules and incentives, to enable distributed identification of people.
2. **Add to the public knowledge base** – If this project results in something that can serve as an identity platform for distributed apps, that would be wonderful; however, even if we learn that our approach is entirely unworkable, that lesson will still help others.
3. **Help future efforts** – Since we will release all of our software as open source, others may use that software in their projects; they might also read our white paper and view our data points, which will increase the probability that those future projects will succeed.

4. **Raise awareness of basic income** - Basic income pilots have produced promising results. More people should be discussing the topic. We welcome the debate and hope that our efforts will catch the attention of an increasing number of brilliant people who will work on meaningful projects that explore or promote basic income-related concepts.
5. **Raise awareness of identity and privacy issues** – At the time of this writing, centralized servers control virtually all digital personal information. As we have learned from numerous highly-publicized breaches, when private companies hold our personal information on their centralized servers, that information is vulnerable to malevolent third parties, who may steal, seize, use or purchase it. Decentralized identity management, which has become feasible with blockchain technologies, holds the promise of giving individuals control over their personal info. That is a good idea. As part of this project, we will contribute to the effort to create *self-sovereign identity* systems.
6. **Raise awareness of decentralized computing** – In most documents that describe blockchain-based business models, you could globally replace the word “blockchain” with “database,” and it would make no substantive difference. If society is to enjoy the benefits of decentralized computing, then even seasoned developers will have to gain a better understanding of what decentralization means. By implementing a decentralized system, we will help raise awareness of the potential for, and benefits of, disintermediation.
7. **Provide a learning experience** - The intern developers who work on this project will gain invaluable insights. At a minimum, they will understand the concepts underlying decentralized systems. We are confident that we will hear more about our interns in the future as they move on to other meaningful projects.

System Components

The following diagram illustrates the components that will make up the TCUP implementation:



The following points describe the project's concepts and components:

- **Basic Income Distribution (BID)** – A periodic payment in a cryptocurrency (examples: Bitcoin Cash, Bitcoin, Ether, etc.) to validated people. For this project, we will have to pick one BID currency.
- **Funding Source** - A supply of cryptocurrency for making payments. Since the project does not require a specific currency, an inexpensive way to fund the BID is simply to create a new ERC20 token on the Ethereum blockchain. To make the BID more meaningful, and to give more users an incentive to participate, we could also use an existing, and more popular, cryptocurrency, such as Bitcoin Cash.
- **Personal Identification Information (PII)** – For this project, PII will be users' public keys, authentication videos and wallet addresses that are appropriate to receive payments in the BID currency. If implementing Sybil detection for videos will not be feasible during the project, then we can fallback to using photo images for facial recognition.
- **PII Repository (PR)** – The PR will hold all PII. This project will use Amazon's Simple Storage Service (S3) as a PR. Ultimately, the PR will likely utilize a decentralized data storage protocol, such as [FileCoin/IPFS](#).

- **Kuwa Registrar (KR)** – KRs will verify user IDs. To allow for majority KT voting, we will deploy at least three of our own KRs for this project; however, KRs will ultimately be independent entities, which can be for-profit organizations. Our goal is to define the incentives (AKA, cryptoeconomics) so that we enable multiple independent and selfish KRs to cooperate and compete with each other, resulting in a robust and reliable distributed identity system.
- **Kuwa Repository Manager (KRM)** - This process will facilitate access to the PR by KRs. Since future implementations should use more decentralized file storage (e.g., IPFS), this process will eventually be replaced. So while this process will be off-chain for this project, a longer-term goal is to move the KR and KRM on-chain as the available decentralized storage options mature.
- **Kuwa Smart Contract (KSC)** – A program that will execute on the Ethereum blockchain. This contract will issue Kuwa tokens.
- **Kuwa Token (KT)** – When a user registers, that user gets an unvalidated KT. The Kuwa Smart Contract will issue a generic KT, which will conform to the ERC 20 standard. When a Kuwa Registrar validates a KT, it becomes a validated token for the associated public key (see PII). A valid KT represents a valid unique user. Users with valid KTs will be eligible to receive basic income distributions. KTs have an expiration date, at which point the KT will no longer be valid. For this project, KTs will expire after one week.
- **Kuwa Client (KC)** – A KC will enable users to register and keep track of their KTs. We may start with the [Uport](#) client. Our priority is to implement an Android-based KC. iOS and Web-based KCs are second and third priorities, respectively.
- **Kuwa Faucet (KF)** – A KF is an off-chain process that (1) checks the validity of a KT; and (2) sends BIDs to valid KT holders’ designated wallet addresses (i.e., public keys), which must be valid for the BID currency (i.e., if the BID currency is Bitcoin Cash, the wallet address must be a valid Bitcoin Cash address). To as great an extent possible, the KF should be cryptocurrency neutral. Although the KF will be off-chain for this project, it should eventually move on-chain, which would achieve greater decentralization.
- **Third Party Crypto Wallet** – Users who receive BIDs can use any wallet software that is available for the BID currency.
- **Project White Paper** – The project team will publish a white paper at the end of this project. It will describe the lessons that we learned during this project and suggest topics for future work.
- **Kuwa Board (KB)** – The KB is a group of people. When there is an unresolvable dispute between Kuwa Registrars regarding the validity of a registration, all Registrars will vote, in which case the losing Kuwa Registrar will pay a penalty and the winning Registrar will get a reward; however, the losing Registrar can appeal to the board. If they lose their appeal, the losing KR will pay a higher penalty. Ideally, KT holders would elect the KB, but we will not likely implement such functionality during this project. Although the implementation of decentralized governance by KT holders is out-of-scope for this project, we acknowledge the desirability of on-chain governance. We will address the topic in the Project White Paper.

Cryptoeconomics: Kuwa Registrar Incentives

To become a KR, an entity will have to “stake” a certain amount of value, which could be denominated in KTs or some other currency. A principal reason for creating this project is to learn how to implement decentralized user ID registration and management. Consequently, getting the incentives right is a mandatory long-term objective. But this project is short-term and experimental. So we have to try something. Consequently, for this

project, KR's will get an arbitrary reward of 1KT for a valid registration. A KR will pay a penalty of 1.5KT for an invalid registration that it verified, but was later found to be invalid. A KR will pay a 2KT penalty for an invalid registration that it verified if they unsuccessfully appealed to the KB.

Advantages of a Kuwa-driven Basic Income Faucet

Here is a partial list of advantages of the approach outlined in this document:

- **No need to bootstrap a new currency** - We don't have to expend effort to create another cryptocurrency and convince people that it has value. Moreover, we have the option to use whatever existing currency meets a particular need.
- **Flexibility** - We can use whatever cryptocurrency that meets our requirements. If no existing currency is appropriate, we can create a new one. Our implementation can also serve as the identity component for other blockchain projects, including other basic income distribution efforts.
- **No underwriting with fiat** - If we create a new currency, we would likely have to underwrite it to convince people that it has value. We may not have to underwrite a BID currency with fiat; there is already a social consensus that major cryptocurrencies like Bitcoin Cash have value.
- **Knowledge** - We will create a large body of test data (e.g., authentication videos). By seeing how people react to the system, we will gain considerable knowledge.

Project Plan

The TCUP team will base our 12-week project plan on this document. We will adhere to the [Agile development approach](#), and use the [Jira Software](#) service to help organize and manage the project.

This Project's Raison d'Kuwa

This project might produce a useful identity system, and it might not. Either way, at its conclusion, we'll have some rather unique software, a large test data set, and we'll know more than we do now. So, let's show the world what some talented, hard-working UMass CICS grad students can accomplish during a summer break, with the help of a few experienced mentors, and a goal to make our planet a better place.

Or as Arturo would say, let's start pushing.