

Payment Layer for Unattended Merchandising (PLUM) Smart Contract Technology & Applications

C. M. Smolen <chris@gedco.io>, S.W. Card <stu@gedco.io>
Quotidian Engineering & Development Corp. (QED)

Abstract

The PLUM ERC-20 Token was created to facilitate and reduce friction in un-/semi-attended transactions and their price discovery mechanisms in a hierarchical payment system with commission layering.

1. Background

Since the dawn of virtual (electronic, digital, crypto-) currencies [1], their security and scalability have been fundamental concerns, motivating invention of Bitcoin, sparking development of blockchain [2] and distributed ledger technology, enabling modern network software based smart contracts on platforms such as Ethereum. Since ancient times, smart contracts have existed in the form of vending machines [3]. PLUM® unites these ancient and modern forms of smart contract using an ERC-20 Token. Potential applications, and the security and scalability of the technology in their context, are briefly introduced here.

The payment network Visa achieved 47,000 peak transactions per second (tps) on its network during the 2013 holidays, and currently averages hundreds of millions per day. Currently, Bitcoin supports less than 7 transactions per second with a 1 megabyte block limit. If we use an average of 300 bytes per bitcoin transaction and assumed unlimited block sizes, an equivalent capacity to peak Visa transaction volume of 47,000/tps would be nearly 8 gigabytes per Bitcoin block, every ten minutes on average.[4]

One approach to accelerating blockchain based payments is localizing transactions, as in Lightning [5], which enforces security using on-chain smart contracts without creating an on-chain transaction for each payment. This has some of the same goals as legacy payment networks, but a very different architecture. In Figure 1 we see the VISA centralized model (A), a hierarchical decentralized model (B) typical both of current blockchains and of conventional vending operations, and a fully distributed mesh model (C). PLUM targets a hybrid architecture to minimize latency and to maximize scalability and resilience.

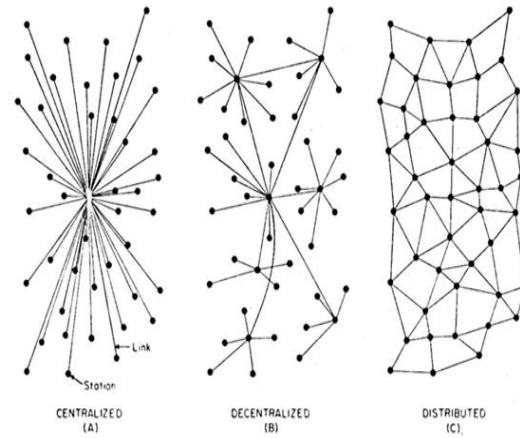


Figure 1: Architectural Alternatives

Decentralized Applications (DApps) can run atop distributed ledgers on such architectures, and can implement smart contracts, which ideally obviate the need for enforcement by external agencies. A smart contract can codify the decision making apparatus and rules of a Decentralized Autonomous Organization (DAO), today minimizing, and ultimately with the aid of Artificial Intelligence (AI) eliminating, the need for paper documents and human staff. A DAO offers transparent governance according to rules embedded by its developers, subsequently modifiable by its stakeholders if and as its code permits. “The DAO”, an infamous early example, was aborted soon after launch due to exploitation of security flaws in its code, but some other DAOs persist and more will emerge. Merchant dissatisfaction with legacy payment networks (e.g., Visa) is endemic and perennial; a payment network with DAO based governance could adapt to changing participant desires and expectations. Given their potential to transform the payment landscape, DAO, AI and other advanced technologies are being actively pursued for integration into PLUM.

2. Implementation

Initially, we developed a simpler (no DAO, AI, etc.) prototype that accepted conventional pliant currency (“paper money”) for conversion to on-chain currencies and product purchases: smart contract, ERC-20 token, hardware, firmware, server and Android client

software. Subsequently, the hardware and firmware were productized and the token listed on exchanges. Figure 2 shows the hardware used in proof-of-concept experiments and demonstrations.

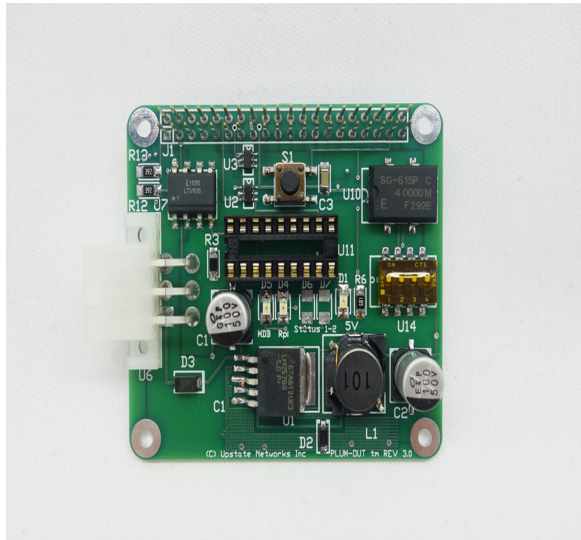


Figure 2: Initial Prototype Hardware

3. Intellectual Property

Prior to this development, cryptocurrency based vending was considered desirable but it was not clear that it was feasible. High speed double spend attacks seemed to preclude the convenient, low-latency experience that vending machine customers demand. There was no intersection between practitioners skilled in the arts of Vending Machine Controller (VMC) interfaces and cryptocurrencies. Upstate Networks Inc. (UNI) and Critical Technologies Inc. (CTI) jointly addressed the prior vulnerabilities by devising distributed ledger network architectural innovations and reduced the invention to practice. The first ever purchase anywhere using Bitcoin to pay for a product from a vending machine was executed in UNI's lab in 2012 [6], return of change in US dollar bills was shown in 2013 [7], and this work was independently recognized as having “pioneered the concept” in a 2014 article [8]. After an extended experience with the United States Patent and Trademark Office, the authors were granted a fundamental patent on cryptocurrency based vending in 2020 [9]. The patent was assigned to Quotidian Engineering and Development Corp. (QED). UNI, CTI and QED continue to advance the state of the art and assist licensees of their intellectual property with products and services integrating blockchain, cryptocurrency, and smart contract technologies for

vending and other un-/semi-attended transactions. UNI counts several *Fortune 100* firms among its customers, manufactures PLUM hardware, and develops both standard and custom software based on their deep experience in vending bus protocols. CTI develops trustworthy networked autonomous system products for commercial and military clients, often involving marketplace methods and transparent immutable logs.

4. Ongoing & Future Work

PLUM enables, *inter alia*, customer loyalty programs that do not require the vendor to collect and store personal information about or from the customer. This avoids a potential liability and may attract customers averse to providing such information. How to use PLUM to incentivize not only direct customers but also influencers is an open question; cryptocurrencies bear an obvious relationship with reputation based currencies, such as the fictional Whuffie (whose author has since opined they are a terrible idea) [10]. Perhaps a greater reach is how to gamify PLUM: loyal customers could be given credits usable in-game; players who do well in the game and/or influence other players to become customers could also gain credits, usable not only in-game but also to make purchases from vending machines etc. in the physical world. Such interplay between worlds is highlighted by the increasing recognition of Cyber-Physical Systems (CPS), such as networked Unmanned Aircraft Systems (UAS, “drones”), which with increasing autonomy might be paid in cryptocurrency for a product delivery, then pay with cryptocurrency for a battery charge, hydrogen fuel or a human-authored firmware upgrade.

All this discussion of first-world issues may seem to miss the point that much of the globe's population has basic needs unmet. Un-/semi-attended transactions offer scalability to meet such needs. Many people are “unbanked”. There are approximately 4 times as many vending machines as Automated Teller Machines (ATMs) globally; the former, equipped with PLUM, can provide both essential products (e.g., medications, bottled water) and the most basic of financial services (precious metal coins and fiat currencies, in and out of money storage and transfer networks). A surprising fraction of the world's population that struggles with basic needs has smartphones: one of the authors witnessed, in one of the world's 5 poorest countries, in Africa, human-drawn wooden cart delivery of water to customers who ordered it from the cart puller by using their cellular phones to call his; a smartphone and a free app is all a person needs to use PLUM. One could

even imagine a water vending machine that not only accepts both tangible currency and PLUM, but also pays humans in either form of currency to restock it.

5. References

- [1] Chaum, David (1982). *Blind signatures for untraceable payments*. Department of Computer Science, University of California, Santa Barbara, CA.
<http://blog.koehntopp.de/uploads/Chaum.BlindSigForPayment.1982.PDF>
- [2] <https://en.wikipedia.org/wiki/Blockchain>
- [3] Savelyev, Alexander (14 December 2016). *Contract Law 2.0: "Smart" Contracts As the Beginning of the End of Classic Contract Law*. Social Science Research Network.
<https://ssrn.com/abstract=2885241>

[4] <http://www.visa.com/blogarchives/us/2013/10/10/stress-test-prepares-visanet-for-the-most-wonderful-time-of-the-year/index.html>

[5] <https://lightning.network/lightning-network-paper.pdf>

[6] <https://www.youtube.com/watch?v=pDOcLros-w0>

[7] <https://www.youtube.com/watch?v=CAU81Dz9SZU>

[8] <https://www.coindesk.com/6-cool-machines-accept-bitcoin>

[9] US Patents 8417376 and 10621809B2

[10] Doctorow, Cory (4 March 2016). *Whuffie Would be a Terrible Currency*.

<https://craphound.com/down/2016/03/04/whuffie-would-be-a-terrible-currency/>