Cowri White Paper

July 30, 2019

Abstract

The goal of this project is to create Internet Money by building a stable and liquid medium of exchange accessible to anyone. The building blocks of Cowri's medium of exchange are stablecoins, cryptocurrency pegged to a stable asset such as the US dollar. Individually, a stablecoin is limited. But if they work in unison, they become quite powerful. The Cowri Shell Protocol unifies an arbitrary number of stablecoins into a coherent monetary system. This is analogous to how nation states developed central banks to unify their fragmented banking system, except Cowri takes a decentralized, bottom-up approach. Cowri lets users interact with multiple stablecoins as if they were using a single currency. This is accomplished not by issuing any new tokens, nor by holding custody of user assets. Instead, the Cowri Shell Protocol is based on a set of logical procedures that ensure users always receive a stablecoin they are willing to accept. Users of the protocol need not agree on which stablecoins to hold; heterogeneous preferences are accommodated.

1 The money myth

Mastering fire was perhaps our species' foundational accomplishment. Prometheus, the mythic individual who brought flame down from Mount Olympus, was the original technologist. An equally important milestone was the invention of money. Money has been with us since the dawn of humanity; it is part of our identity as human beings. In this case, "Prometheus" was probably a tribe of skin divers living along the coast of East Africa, many thousands of years ago. And rather than bear the torch of knowledge from on high, they carried from the depths of the ocean our species' first currency: cowry shells.

When humans started to harvest these shells from the Indian Ocean and use it as a currency for trade, we took a technological leap just as profound as our mastery of fire. Our species now had a store of value and medium of exchange; the epoch of commerce had begun in earnest. Archeological evidence of cowry shell money can be found across the ancient world, from Africa, Egypt, Mesopotamia, India, China and Australia. Cowries were truly a global currency as the shell played a prominent role even amongst land-locked peoples.[21]

Cowry shells seemed to have had a particular impact on Chinese society. Over time, cowry shells were replaced by metal figurines symbolic of the original.[2][13] These physical symbols were then superseded by written symbols. On ancient oracle bones, the oldest source of Chinese writing, we see pictograms of cowry shells scratched onto the bones.[24] This early pictogram remains in modern Chinese writing as the character, 貝 ("bei"), which to this day has the kept its original meanings: "shell" and "money" (see Figure 1).

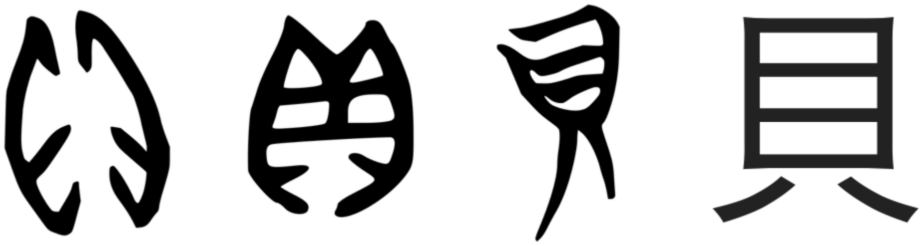

Figure 1: Over time, cowry shells changed from a pictogram on Oracle Bones (far left) to today's modern Chinese character for "money" and "shell" (far right).

Despite disappearing as a currency, cowry shells have left a lasting legacy. As the cowry shell demonstrates, money is constantly changing forms as technology progresses. We are living through one such transition, the rise of cryptocurrency and blockchain. These technologies are the substrate upon which Internet Money will be built.

2 Internet Money

Money is a social construct that experiences positive network effects. Meaning, the larger and more interconnected the network, the more valuable money becomes. It is inevitable that a monetary system will exist natively on the internet, the preeminent network of our species.

The ability to conduct global commerce as seamlessly as we send emails will radically transform civilization. However, the transition to Internet Money has not yet occurred. Currently, the global monetary system is an ad hoc confederation replete with redundant intermediaries. The internet is at best an auxiliary technology in this legacy system.

The first currency truly native to the internet was Bitcoin. However, Bitcoin is unable to serve the role of Internet Money. The currency is just too volatile for people to use. Money must be stable. A stable cryptocurrency is called a "stablecoin." To properly understand stablecoins, one must first understand how they relate to the broader history of money.

3 Money and the past

The correct historical analogy to think about stablecoins is the transition from gold specie, to paper currency, to fiat currency. In the modern version of the story, we are instead transitioning

	Original Currency	***Intermediate Currency***	***Ultimate Currency***
Old System	gold specie	paper bank notes	fiat
New System	fiat	stablecoins	Internet Money

Table 1: There are three phases of monetary transition: original currency, intermediate currency and ultimate currency.

from fiat currency, to stablecoins, to Internet Money (see Table 1). The past transition from gold to fiat will resemble the future transition from fiat to Internet Money.

3.1 Stablecoins versus paper currency

Before the advent of paper currency, gold specie was the primary form of money. In the 7th Century, merchants and bureaucrats in Tang China figured out how to imbue paper with the monetary properties of gold by storing gold in a secure vault and issuing paper notes redeemable for the gold held in reserve.[8][13] Once invented, it was inevitable that paper money would supersede physical gold. Paper money was far easier to transact with and enabled new forms of commerce such as securitized bonds and joint stock companies.[14]

Just as paper replaced gold, stablecoins will replace fiat. To create a stablecoin, all it takes is to hold fiat in a custodial account and issue cryptocurrency redeemable for the fiat held in reserve. Stablecoins are better than fiat for three reasons:

1. Faster and cheaper settlement time
2. Internet native
3. Programmable

Sending money through the legacy banking system requires one private ledger (i.e. a bank) to coordinate with at least one other private ledger (often more). On a blockchain, there is only one ledger, and anyone on the internet can make changes, which is a vastly superior design. Compared to settlement on blockchains, banks are slow and expensive. A stablecoin transaction on Ethereum can settle within one minute and cost less than $0.25. Banks charge fees just to open an account and transfers take up to two business days. Transaction settlement between banks is so onerous that VISA, a company with $20.6 billion in revenue 2018, exists to streamline payments between retailers and their customers.[23]

Because banks are private ledgers, integrating bank accounts with internet services is difficult. Multi-billion dollar companies, such as PayPal and Stripe, exist to integrate the banking system with internet applications.[20][22] In contrast, stablecoins exist natively on the internet and are trivial to integrate.

Not only are stablecoins an internet native currency with extremely efficient settlement, they are also programmable. By combining stablecoins with smart contracts, financial services and accounting operations can run autonomously, without a trusted third party's involvement.

Just as paper currency enabled new forms of commerce such as the joint stock company, smart contracts and stablecoins will transform finance. The field is still early and it is impossible to predict what will come in the future. For a foreshadowing of what will be possible, consider Uniswap. Uniswap is a smart contract protocol that provides on-demand liquidity to anyone in the world. As of July 9, 2019, the decentralized liquidity pool had $21.8 million in capital on the platform.[7] Uniswap was built with just a $100 thousand research grant.[4]

3.2 Monetary fragmentation: paper currency

Despite the success of paper currency, it created a new set of challenges. Any bank could issue their own paper notes, and so for every bank, there was a separate currency (see Figure 2). By 1907, there were over 20,000 banks in the US.[11] To facilitate payments in such a fragmented banking system, a complicated financial network between banks emerged. Banks in remote areas shared deposits with banks in the cities, who shared deposits with banks in major financial centers such as New York. And New York banks shared deposits with each other.

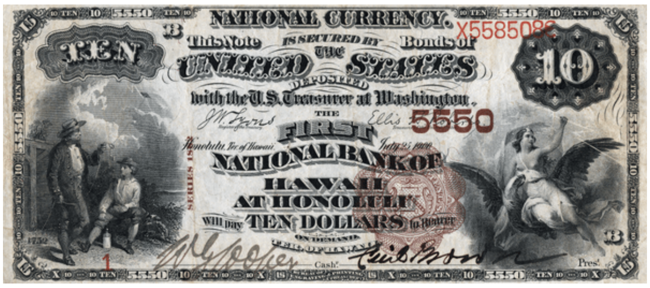
NATIONAL CURRENCY.
TEN
10
This Note is secured by Bonds of the United States deposited with the U.S. Treasurer at Washington.
X558508
5550
THE FIRST NATIONAL BANK OF HAWAII AT HONOLULU
Will pay TEN DOLLARS to Bearer
ON DEMAND

Figure 2: A $10 paper note from the First National Bank of Hawaii.

This fragmentation created two problems: high transaction costs and a fragile financial system. Sending money across the country required numerous banks to coordinate with each other, and every middleman took a healthy cut of the transaction. Fees could be as high as 50%.[9]

Tangled banking relationships exacerbated financial shocks. A minor economic shock could easily cause a number of small, local banks to collapse. Collectively, these banks may not make up a meaningful portion of the real economy. However, panics would reverberate up through the banking hierarchy, putting even major New York banks at risk. The 2008 Financial Crisis is an illustration of what can happen if institutions “too big to fail” collapse.

3.3 Monetary fragmentation: stablecoins

The same pattern of fragmentation is emerging with stablecoins. Any well connected technologist or financier can issue a stablecoin. There are already over two hundred stablecoin projects announced.[3] Over five stablecoins are widely traded at the time of writing.[17] Even powerful financial institutions and technology companies have announced plans to launch stablecoins.[10][15] There will be hundreds if not thousands of unique stablecoins.

Like banking fragmentation in the US one hundred years ago, stablecoin fragmentation will have painful consequences. Transacting will be difficult. Imagine buying coffee and having to first argue with the shop over which of the two hundred stablecoins to use? Managing even a handful of different stablecoin balances will be prohibitive for users.

As for financial fragility, stablecoin fragmentation exacerbates that too. As mentioned previously in Section 3.1, the future of commerce will be based upon smart contract protocols that perform financial and accounting processes autonomously. These smart contract services are referred to as "Decentralized Finance" (DeFi) protocols. Despite the immaturity of the technology, DeFi protocols collectively have over $500 million in assets stored on their platforms as of July 9, 2019.[6]

Stablecoins are intrinsic to the working of many DeFi protocols and will be at the heart of the ecosystem. Indeed, at the time of writing, the most popular DeFi protocol is itself a stablecoin (Maker and Dai).[5] Because these protocols rely on stablecoins, and these protocols rely on each other, the entire house of cards could collapse if only one of the stablecoins loses its peg. E.g., DeFi protocol 1 relies on DeFi protocol 2 which in turn relies on DeFi protocol 3 which relies on a Stablecoin A. If that one stablecoin loses its peg, all three protocols are at risk.

3.4 Unification

Once again, history sheds light on our current conundrum. In 1913, faced with a fragmented banking system and all its social costs, the US Congress created the Federal Reserve - not to control interest rates, inflation, unemployment, or even the aggregate money supply - to unify the banking system.[16] The mandate to pursue inflation and unemployment targets was not institutionalized until 1977.[18]

The Federal Reserve solved the fragmentation problem by creating a unified system of interbank deposits. Rather than dealing directly with each other in ad hoc connections, banks could deposit assets at regional Federal Reserve banks. In return, the Fed gave the banks Federal Reserve notes. (Although "Federal Reserve notes" are now synonymous with "cash", at the time, they were not intended to replace private bank notes as a medium of exchange). This system of pooling deposits at Federal Reserve banks and using a common currency (Federal Reserve notes) not only made inter-bank transactions more efficient, it also made the financial system more resilient to shocks (note: resilient does not mean immune, as the Great Depression would painfully demonstrate two decades later). The new model was so successful that by 1920 69% of all bank deposits were in the Federal Reserve system[12].

The early history of the US Federal Reserve shows us that unification is possible and that the benefits can be enormous. But the Fed is a centralized bureaucracy imposed top-down by a nation state. Such a solution will not do for Internet Money. Not for moral reasons, per se, but pragmatic. Blockchain and cryptocurrency is a bottom-up, decentralized system. Top-down solutions are simply incompatible with the technology and defeat the whole advantage of the new system. Ultimately, Internet Money must rely on software, not nation states.

To unify stablecoins in a framework compatible with blockchains and cryptocurrency, we need a decentralized solution. The Fed allowed banks to seamlessly interoperate with each other. What we need is an internet protocol that allows stablecoins to do the same.

4 The Cowri Shell Protocol

Collectively, stablecoins represent a powerful new monetary system. A system open to all on the internet, transparent and peer-to-peer. But, individually, a stablecoin cannot constitute Internet Money. If we can unify disparate stablecoins into a coherent monetary system, then we can create a stable and liquid medium of exchange, i.e. money.

Our key insight to solving this problem is that although stablecoins are highly fragmented, they are also highly fungible. Fungibility is an economic property where each individual unit is interchangeable with every other unit. An example of a fungible asset is gold bullion. Provided they are of equivalent mass and purity, each gold ingot is interchangeable with every other gold ingot. It does not matter where the gold was mined. Was it from a Canadian mine? A South African mine? These questions are irrelevant.

The same principle holds true for stablecoins. In practice, a super majority of stablecoins will peg themselves to the same value: the US dollar. By sharing a common peg, stablecoins become interchangeable, just like gold bullion. It should not matter which crypto-token represents your money as long as they are all worth $1.00. To be clear, stablecoins are not quite as fungible with each other as gold bullion. Stablecoins, like banks, can suddenly become insovlent and lose their peg. Gold does not spontaneously dematerialize. Thus, additional accommodations must be made for stablecoins.

In practice, inter-stablecoin fungibility means that users will be largely agnostic about which stablecoins they send and receive. The problem of unifying stablecoins into a coherent monetary system boils down to tracking which stablecoins users will accept, and making sure that when users transact with each other, the right stablecoins are sent and received. The rest of Section 4 will explain conceptually how this process works. Section 5 explains how this approach will be implemented in computer code.

4.1 Stablecoin Shells

Simply put, a stablecoin shell is a collection of stablecoins that a user is willing to treat as fungible to each other. A shell is not its own token. Rather than being an on-chain artifact, a shell is an accounting concept for keeping track of an arbitrary number of fungible assets (e.g. stablecoins). We use the term, “stablecoin shell,” because Cowri acts as a wrapper over the underlying assets. Hence, it is a “shell” for the actual stablecoins. Building on top of this concept, we can develop a set of logical procedures that will ensure users will always receive the stablecoins listed in their shell.

To see a concrete example of a stablecoin shell, consider the following: Alice starts off with a balance comprised of three popular stablecoins: 75 TrueUSD, 50 Dai and 25 USD Coin (see Table 2). She then creates a Cowri shell containing TrueUSD, Dai and USD Coin. Let’s call

Currency	Ticker	Balance
Cowri	***WRI***	***$150***
TrueUSD	TUSD	$75
Dai	DAI	$50
USD Coin	USDC	$25

Table 2: Alice's starting balance

Currency	Ticker	Balance
Cowri	***WRI***	***$100***
TrueUSD	TUSD	$75
Dai	DAI	$0
USD Coin	USDC	$25

Table 3: Alice's balance after sending 50 WRI to Bob

this shell "cowri" or "WRI". Alice's shell balance is now 150 WRI. With Cowri's shell protocol, Alice can transact in cowri as if it were a single currency. If she decides to send 50 WRI to Bob, the protocol will, on the backend, send 50 tokens of the underlying stablecoins (more details in Section 4.2). Let's assume the protocol sends 50 Dai. Alice's new balance would then be 100 WRI (75 TrueUSD and 25 USD Coin) and Bob's balance increases by 50 WRI (see Table 3).

By construct, the stablecoins in a shell are fungible with each other. In the example above, TrueUSD, Dai and USD Coin are each pegged 1:1 with USD and at any given time will have correlated exchange rates. Additionally, in the case of fiat backed stablecoins, each token will have an equivalent amount of collateral backing its value. Because of this, it shouldn't matter what balance the user has of each individual stablecoin.

If Alice prefers certain stablecoins and not others, all she needs to do is define her shell accordingly. Perhaps Alice thinks that Dai's strategy to back stablecoins with Ether is too risky for her. Instead, she prefers to hold Paxos, a stablecoin backed with reserves of USD held in a custodial bank account. All she has to do is define her cowri shell as comprising TrueUSD, Paxos and USD Coin (see Table 4). With a newly defined shell, Alice can transact in cowri and not worry about holding any Dai.

Currency	Ticker	Balance
Cowri	***WRI***	***$150***
TrueUSD	TUSD	$75
Paxos	PAX	$50
USD Coin	USDC	$25

Table 4: An alternative stablecoin shell for Alice with Paxos instead of Dai

4.2 Formal description of stablecoin shells

This section will present a more rigorous description of stablecoin shells and how users transact using the Cowri Shell Protocol. To start, we will reintroduce Alice, our canonical user. Alice chooses a set of tokens she wants to include in her stablecoin shell, defined as:

$A = \{a_1, a_2, ..., a_n\}$, i.e. a list of stablecoins

a_i = stablecoin i in Alice's set A

a_i = Alice's balance of stablecoin i, i.e. the total number of tokens held

$|A| = \sum_{i=1}^{n} |a_i|$, i.e. the total balance of Alice's stablecoin shell

For Alice, receiving tokens is fairly straight forward. If she receives a balance of tokens that are included in A, then they are simply added to her shell's balance. However, if they are not included in her shell, then the tokens are listed separately.

Sending tokens is a bit more complicated. Let's reintroduce our second canonical user, Bob, who requests X cowri from Alice. Bob's shell is defined as B. There are two scenarios to consider:

1. $A = B$, i.e. their shells are comprised of an identical list of underlying tokens
2. $A \cap B = \{\}$, i.e. their shells include completely different tokens

It is possible to have a partial overlap of users' shells; however, this case can be reduced to a combination of the two scenarios listed above and will not be covered at length. Either the partial shell overlap is sufficient to cover the value of the transaction, X, in which case it can be treated as scenario (1). Or the partial overlap is insufficient to cover X, and the case can be treated as combination of scenario (1) (for the overlapping shell) and scenario (2) (for the non overlapping shell).

4.2.1 Sending cowri when users' shells overlap

In scenario (1), sending X cowri from Alice to Bob is a matter of selecting which stablecoin tokens to send, and how much of each token to send such that the total amount sent is equivalent to the transaction request. To formalize:

For each coin $i \in A$ send x_i units of coin i such that $x_i \leq a_i$ and $\sum x_i = X$

The selection algorithm ought strike a balance between sending as few stablecoins as possible to complete the transaction while prioritizing the smallest individual balances first. It is better to send smaller balances first because that saves the larger balances for larger transactions in the future. Additionally, if the smaller sub-balances are given priority over larger balances, then it will probably favor stablecoins with a smaller circulation than large stablecoins, thus making the stablecoin ecosystem as a whole more competitive and less concentrated.

4.2.2 Sending cowri when users' shells do not over lap

At first glance, it may seem like Alice and Bob cannot transact with each other in scenario (2) because there is no overlap of their shells. However, that need not be an impediment. Let's introduce a third canonical user, Claire. Claire's shell, C, overlaps with both Alice and Bob. That is, $A \cap C \neq \{\}$; and $C \cap B \neq \{\}$. Thus, Claire can give X cowri to Bob, and Alice can give $X + \epsilon$ cowri to Claire, where ϵ is a nominal fee given to Claire by Alice in return for facilitating the transaction. The only limitation is that $|A \cap C| > X + \epsilon$ and $|C \cap B| > X$.

4.3 Transacting cowri: an example

This section presents concrete examples of how users will transact cowri under the two scenarios discussed in Section 4.2. In each example, Alice's WRI balance is the same as the example given in Table 2. Bob's transaction request is also the same as Table 3, 50 WRI.

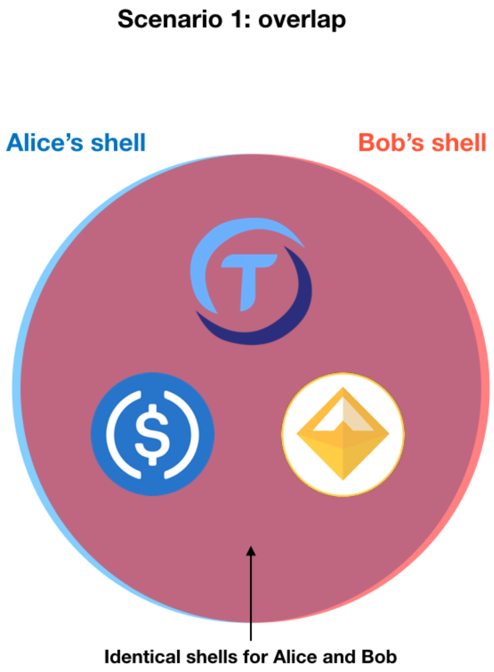

Figure 3: Alice's and Bob's Cowri shell: TrueUSD, Dai and USD Coin. Alice sends Bob 50 Dai.

In each scenario, Alice's balance will be: 75 TrueUSD, 50 Dai, 25 USD Coin. And Bob's transaction request will be: 50 WRI. For a description of the transaction flow, see Table 5. In the first scenario, Alice and Bob have overlapping Cowri shells. Alice can send any sub-balance she wants to complete the transaction. In this case, Alice sends 50 Dai (see Figure 3). In the second scenario, Alice and Bob have no overlap, but can facilitate a transaction with the help of a third party, Claire. Claire accepts TrueUSD (preferred by Alice) and Paxos (preferred by

	Alice's Balance	*Claire's Balance*	*Bob's Balance*
Scenario 1	-50 DAI	0	+50 DAI
Scenario 2	-50.5 TUSD	+50.5 TUSD, -50 PAX	+50 PAX

Table 5: In the first scenario, Alice directly pays Bob. In the second scenario, Claire acts as an intermediary and nets 0.5 stablecoins.

Bob). To complete the transaction, Alice sends Claire 50.5 TrueUSD (the extra 0.5 TrueUSD is an incentive fee for Claire) and Claire sends Bob 50 Paxos (see Figure 4).

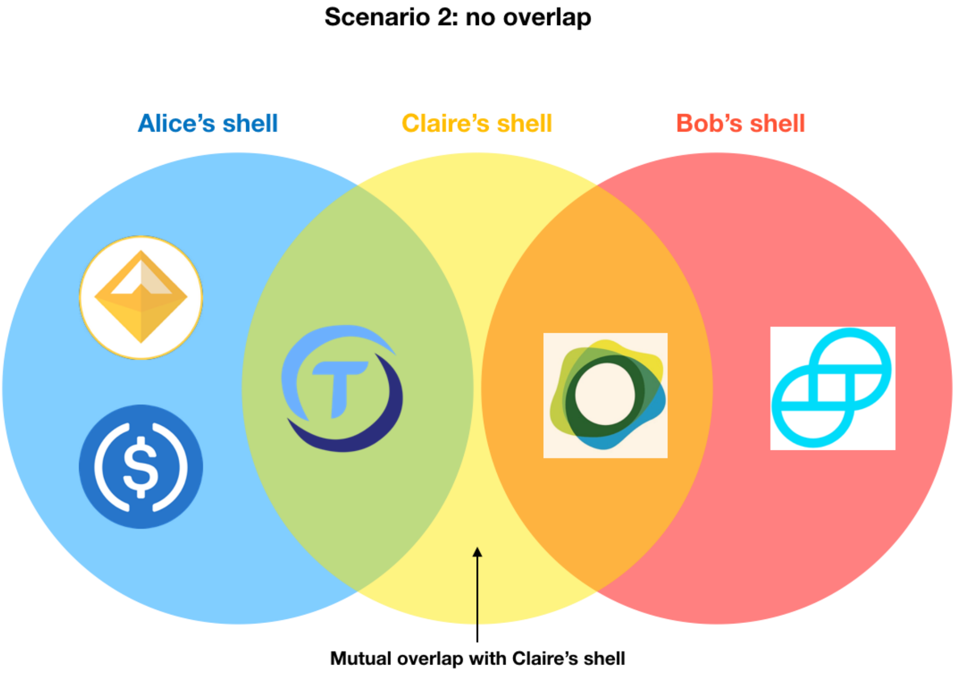

Figure 4: Alice's cowri shell: TrueUSD, Dai and USD Coin; Bob's cowri shell: Paxos and Gemini. Claire's balance: 100 Paxos, 50 TrueUSD. Alice gives 50.5 TrueUSD to Claire who sends Bob 50 Paxos.

5 Protocol Implementation

Section 4 demonstrated conceptually how we can create a unified currency by applying the concept of "shells" to stablecoins. In this section, we extend the concept even further by showing how the logic of shell transactions can be implemented as a decentralized platform. There are three components in the current iteration of the protocol:

1. Shell ledger
2. Shell manager

3. Stablecoin liquidity pool

The remainder of this section will describe the function of each component and how it works. Then, this section will explain how the three components function together in order to create the Cowri Shell Protocol.

5.1 Shell ledger

The shell ledger is the simplest yet most important of the three components. It keeps track of each users' stablecoin shell, i.e. which stablecoins are used by whom. The ledger should be stored on a decentralized, censorship-resistant computing device. Additionally, all users must agree on the state of the ledger. If Alice updates her shell but Bob refers to an old copy of the ledger, then he may send Alice incorrect stablecoins. Not only do all participants need to agree on the same ledger, only users may edit their own shell. Bob should not be able to make changes to Alice's shell and vice versa. These are fairly demanding criteria. Fortunately, this problem is a perfect use-case for blockchains. The shell ledger is straightforward to implement as a smart contract, with a data structure to record users and their stablecoin shells.

5.2 Shell manager

The shell manager has three sub-modules: the developer SDK, the core and the sequencer. The developer SDK sub-module allows third party developers to integrate the Shell Protocol into their applications. It is the link between any front-end user interfaces and the back-end of the platform. The core sub-module provides the logic for the shell manager. Primarily, it determines which stablecoins to send, which stablecoins to swap and how much of each. The sequencer sub-module handles the execution of sending and swapping stablecoins. It is the only component of the shell manager that exists on-chain. The sequencer ensures that all sends and swaps execute atomically, in a specified order.

The shell manager collectively has three main tasks: display user cowri balance, edit user shell and send cowri. Displaying user cowri balance is a simple matter of summing the sub-balances for each stablecoin in the user shell. Editing the shell is also straightforward via the shell ledger (see Section 5.1). Sending cowri is the complicated task. As in Section 4.2, there are two scenarios to consider: sender and recipient have overlapping shells, or sender and recipient do not have overlapping shells.

In scenario (1), the core sub-module will select which individual stablecoins to send and the correct amount of each. The sequencer will then execute the sends atomically. In scenario (2), the shell manager will have to swap the sender's stablecoins for a stablecoin in the recipient's shell. To complete these swaps, the shell manager will leverage the third module, the stablecoin liquidity pool (see Section 5.3). First, the shell manager will query the liquidity pool for swap rates. Then the core sub-module will decide which swaps are optimal. Finally, the sequencer will atomically execute the swaps and send the stablecoins to the recipient.

The design goal for the shell manager is to handle as much of the complexity of sending and holding stablecoins as possible. If the shell manager is doing its job, then the user experience of sending Cowri will be indistinguishable from sending a single crypto token.

5.3 Liquidity pool

In essence, this module is a decentralized market for stablecoin-to-stablecoin trades. Users tap into this market whenever they need to send Cowri to a recipient who accepts stablecoins outside the user's shell. In order for liquidity to be available on demand, there must be a pool of capital at all times ready to be the counter-party to users' trades. The source of this capital will come from third party "liquidity providers". Liquidity providers are analogous to "Claire", the third-party who has an overlapping shell with both Alice and Bob, in Section 4.2.

Liquidity providers will be incentivized to participate in the liquidity pool because they will earn a spread on every stablecoin trade they make. Just as anyone with spare computing capacity can participate as a proof of work miner, anyone with spare capital can participate in the liquidity pool to earn passive income. Thus, as the network of Cowri users grows, there will be built-in economic incentives for more liquidity to be added.

The Cowri stablecoin liquidity pool takes many design cues from Uniswap.[1] Liquidity providers stake their stablecoins to the pool. Swaps are handled by the smart contract and require no human or off-chain input. Swap rates are calculated based on the quantity of stablecoins staked as liquidity. Consider an example where Alice swaps X of Stablecoin A for Stablecoin B. The larger the value of Stablecoin A relative to Stablecoin B, the higher the swap rate. The higher the value of X relative to the value of Stablecoin B, the higher the swap rate.

The main point of divergence between the Cowri stablecoin liquidity pool and Uniswap is that whereas Uniswap uses ether as an intermediate currency, Cowri trades are direct stablecoin-to-stablecoin. Removing ether as an intermediate currency bestows two benefits to our liquidity pool. First, liquidity providers for Cowri do not need to expose themselves to ether price volatility, thus reducing their risk. Second, the liquidity pool will be more capital efficient for direct stablecoin swaps because all the capital can be allocated for stablecoins, instead of diverting a large portion to ether.

5.4 Sending transactions with the Cowri shell protocol

With the three main components described, the shell ledger, the shell manager and the liquidity pool, we can now explain how the system functions as a whole. Consider the two following scenarios (see Section 4.2):

Scenario (1): Alice pays Bob $50 in Cowri without needing to swap stablecoins

Scenario (2): Alice pays Bob $50 in Cowri while needing to swap stablecoins

To send a transaction in scenario (1), there are two steps in the protocol. First, Alice's Shell Manager queries the Shell Ledger for Bob's shell. Second, Alice sends $50 worth of stablecoin A based on the logic in the core sub-module (see Figure 5).

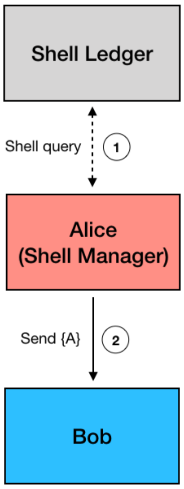

Figure 5: Alice sends a $50 transaction to Bob. Both parties have overlapping stablecoin shells.

To send a transaction in scenario (2), where swapping tokens is necessary, there are a total of four steps (see Figure 6):

1. Alice's shell manager queries the Shell Ledger for Bob's shell
2. The shell manager queries the liquidity pool for swap rates
3. The shell manager swaps stablecoin A for stablecoin B
4. In the same transaction, the shell manager sends $50 worth of stablecoin B to Bob

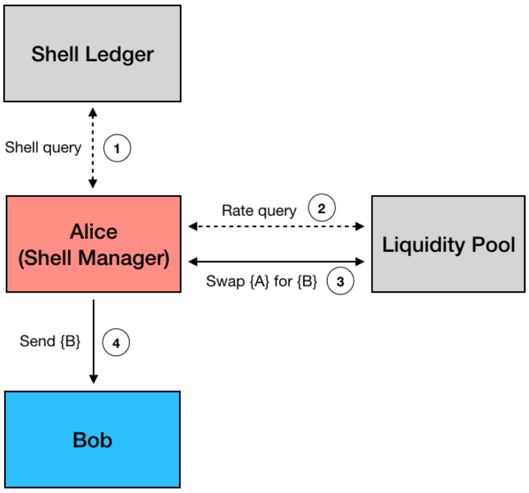

Figure 6: Alice sends a $50 transaction to Bob. Neither party has an overlapping shell so Alice executes a swap.

6 Conclusion

Built upon the concept of stablecoin shells, the Cowri Shell Protocol is an extremely flexible monetary system that can accommodate users even if they want to use different stablecoins than their peers. In effect, this system creates Internet Money without issuing or holding any assets.

By solving the stablecoin fragmentation problem, Cowri reduces transaction costs for users and makes the decentralized financial system more resilient. The protocol, if successful, will also have profound impacts upon the underlying stablecoins. By making stablecoins easier to use, Cowri will encourage faster adoption and thus faster growth. New, smaller stablecoins will compete more easily against established rivals. A more competitive stablecoin ecosystem is a more decentralized stablecoin ecosystem. Lastly, Cowri increases diversification among stablecoins. The easier it is for users to transact with multiple stablecoins, the more stablecoins they will use. Stablecoin diversification will increase financial resiliency.

The final transition to fiat (backed by nothing) came in 1971.[19] US President Richard Nixon, with the backing of the Federal Reserve, announced to the world that the US would no longer peg its dollar to gold. Instead, the US dollar would float freely on the open market. Whether this event was ultimately in the rest of the world's interest is a matter of debate. But it was nonetheless a significant milestone for our species: no longer did we require physical scarcity to create money, but abstract scarcity. Money as an abstract technology came into its own. And once an abstract concept, money became programmable. Cryptocurrency, a natural implementation of programmable money, is the logical next step.

What does the past tell us about the long-term future of cryptocurrency? For the time being, stablecoins will be a necessity. But what will happen after cryptocurrency consolidates and entirely supersedes the legacy system, just as the banking system superseded gold in 1971? We cannot know for certain. Perhaps, one day we will detach from the fiat peg and let our money float freely through the internet.

References

[1] Adams, Hayden (2019, July 5). "Uniswap white paper". https://hackmd.io/C-DvwDSfSxuh-Gd4WKE_ig#DEX-inside-a-Whitepaper

[2] Ashkenazy, Gary. *Bei - Cowrie shells used as coins and various imitations*. Retrieved 2019, July 21: http://chinesecoins.lyq.dk/Bei/BeiNetpakke/index.htm

[3] Cement (2019, Apr 7). "How Many Stablecoins Are There?" *CementDAO Blog*. Retrieved 2019, July 21: https://www.cementdao.com/post/how-many-stablecoins-are-there

[4] Dale, Brady. "A David vs. Goliath Battle Is Brewing in Ethereum Decentralized Exchange Race." *CoinDesk*, 20 Feb. 2019, https://www.coindesk.com/bancor-uniswap-dex-competition.

[5] DeFi Pulse (2019, July 21). "DeFi Pulse: Maker". Retrieved 2019, July 21: https://defipulse.com/maker

[6] DeFi Pulse (2019, July 21). "DeFi Pulse: Total Value Locked (USD) in DeFi". Retrieved 2019, July 21: https://defipulse.com/

[7] DeFi Pulse (2019, July 21). "DeFi Pulse: Uniswap". Retrieved 2019, July 21: https://defipulse.com/uniswap

[8] Extra Credits (2016, Oct 8). "The History of Paper Money - Extra History - #2." YouTube. Retrieved 2019, July 21: www.youtube.com/watch?v=rPHTmGjoe2k.

[9] Extra Credits (2016, Oct 29). "The History of Paper Money - Extra History - #5." YouTube. Retrieved 2016, 29 Oct: www.youtube.com/watch?v=LrB9bS2VOLE.

[10] Facebook (2019, Jun 18). "Libra white paper". https://libra.org/en-US/white-paper/

[11] Friedman, M., & Schwartz, A. J. (1963). *A monetary history of the United States, 1867-1960.* Chapter 4: Gold Inflation and Banking Reform (page 169). Princeton University Press.

[12] Friedman, M., & Schwartz, A. J. (1963). *A monetary history of the United States, 1867-1960.* Chapter 5: Early Years of the Federal Reserve System (page 190). Princeton University Press.

[13] Goetzmann, W. N. (2016). *Money changes everything: How finance made civilization possible.* Part 2, Chapter 8: China's Financial World. Princeton University Press.

[14] Goetzmann, W. N. (2016). *Money changes everything: How finance made civilization possible.* Part 3: The European Crucible. Princeton University Press.

[15] JP Morgan (2019, Feb 14). "J.P. Morgan creates digital coin for payments". https://www.jpmorgan.com/global/news/digital-coin-payments

[16] Sprague, O. M. W. (1914). The federal reserve act of 1913. *The Quarterly Journal of Economics*, 28(2), 213-254.

[17] Stable Report (2019, July 21). “Stable Report: dashboard”. Retrieved 2019, July 21: http://dashboard.stable.report/

[18] The Federal Reserve Bank of Chicago (2019, July 12). “The Federal Reserve’s dual mandate”. Retrieved 2019, July 21: https://www.chicagofed.org/research/dual-mandate/dual-mandate

[19] The US Department of State: Office of the Historian (2018). “Nixon and the End of the Bretton Woods System, 1971–1973”. Retrieved 2019, July 21: https://history.state.gov/milestones/1969-1976/nixon-shock

[20] Wikipedia contributors. (2019, July 21). PayPal. *Wikipedia, The Free Encyclopedia*. Retrieved 2019, July 22: https://en.wikipedia.org/w/index.php?title=PayPal&oldid=907237484

[21] Wikipedia contributors. (2019, July 3). Shell money. *Wikipedia, The Free Encyclopedia*. Retrieved 2019, July 21: https://en.wikipedia.org/w/index.php?title=Shell_money&oldid=904661921

[22] Wikipedia contributors. (2019, July 16). Stripe (company). *Wikipedia, The Free Encyclopedia*. Retrieved 2019, July 22: https://en.wikipedia.org/w/index.php?title=Stripe_(company)&oldid=906544237

[23] Wikipedia contributors. (2019, July 18). Visa Inc.. *Wikipedia, The Free Encyclopedia*. Retrieved 2019, July 22: https://en.wikipedia.org/w/index.php?title=Visa_Inc.&oldid=906844433

[24] 貝. (2019, July 15). Wiktionary, The Free Dictionary. Retrieved 2019, July 22: https://en.wiktionary.org/w/index.php?title=%E8%B2%9D&oldid=53661334