Deloitte.

State-Sponsored Cryptocurrency: Adapting the best of Bitcoin's Innovation to the Payments Ecosystem

The "Bitcoin Buzz"

Bitcoin, the most popular virtual currency in the market today, continues to draw significant buzz. The technology behind the currency is genuinely revolutionary. It is at the forefront of a new world for payment systems around the world. However, despite the excitement and hype surrounding its introduction to the marketplace, Bitcoin suffers from some significant and legitimate drawbacks that may permanently limit its adoption in the mainstream economy. While some see potential for Bitcoin to form the foundation for a robust and secure electronic fiat currency, adjustments will need to be made for the currency to gain widespread usage.

The Marketplace Opportunity for Cryptocurrencies

Bitcoin and other cryptocurrencies face a marketplace that is ripe for disruption. The payment systems in the U.S. and the rest of the world are in dire need of overhaul. Many of today's payment systems are considered slow, error-prone and expensive relative to performance in other high-tech industries. In January, 2015, the Federal Reserve released a paper[1] outlining their goal to "improve the speed and efficiency of the U.S. payment system from end-to-end over the next decade." Desired outcomes include:

1. **Speed:** A ubiquitous, safe, faster electronic solution(s) for making a broad variety of business and personal payments, supported by a flexible and cost-effective means for payment clearing and settlement groups to settle their positions rapidly and with finality.

2. **Security:** U.S payment system security that remains very strong, with public confidence that remains high, and protections and incident response that keeps pace with the rapidly evolving and expanding threat environment.

3. **Efficiency:** Greater proportion of payments originated and received electronically to reduce the average end-to-end (societal) cost of payment transactions and enable innovative payment services that deliver improved value to consumers and businesses.

4. **International:** Better choices for U.S. consumers and businesses to send and receive convenient, cost-effective, and timely cross-border payments.

5. **Collaboration:** Needed payment system improvements are collectively identified and embraced by a broad array of payment participants, with material progress in implementing them.

Cryptocurrencies are a strong option to help deliver these outcomes while doing so cheaply and conveniently, but there are some challenges to overcome first.

Extending the Reach of Cryptocurrencies

Bitcoin suffers from some notable shortcomings inherent in its design that have constrained its expansion into the mainstream payments system. Wide-spread adoption will require Bitcoin to address governmental requirements around anti-money laundering and illicit trade, as well as other key concerns such as volatility of value, ease of use challenges, and a general lack of endorsement by "trusted" bodies.

What would happen if we combined the best attributes of the technology of cryptocurrencies with the features of an established fiat currency under the sponsorship of a central bank? The result very well may just be a new method of handling payments that would revolutionize the current system. With the potential to reduce costs, reduce errors, speed the transfer of money, balance privacy with anonymity, and do it without the day-to-day operational need for a centralized organization, whether commercial or federal, the result could truly be transformational.

Such a system would need to have important roles for banks and credit unions, support the fundamental banking functions such as lending and demand deposit accounts, and support Anti-Money Laundering (AML) / Know Your Customer (KYC) requirements. It would need to be able to start small and scale with demand. And it would need to have the full endorsement of the central bank.

Similarities and Differences between State-Sponsored Cryptocurrency and Bitcoin

Similarities	Differences
Secure transfers of value without risk of double-spend or reversal	No cap on money supply contained on the ledger. Additions to and removals from money supply stored on the distributed ledger are only made by central bank
No need for bank accounts for parties to transfer money between them.	Reduced stigma and fear of adoption due regulations, official sanction and use of national currency
Publically viewable, distributed ledger	Ledger processors (miners) could be regulated organizations. Ledger / blockchain could only be editable by regulated FI's
Anonymous transactions	Protocol supported and regulated by central bank
Borderless[2] transactions	Supports AML and KYC concerns. All transactions are traceable **with appropriate legal approvals**
Ledger processors (miners) are compensated for managing the distributed ledger (blockchain) and processing transactions	No fluctuations in exchange rate vis-à-vis base fiat currency
Instantaneously confirmed transactions are possible only with a small exposure to risk	Nullifies the risk of "51% attack" that could cripple Bitcoin
No operational involvement by a central bank or other organization	Establishment of an initial "seed" private key requires involvement of regulated FI
Virtual / electronic currency; reliance upon technology to send money	Not a new or alternative currency. Different medium of existing national fiat currency
Secure store of currency (with proper precautions)	Not a global currency – dependent on government to define value of the currency, and would still have to pay exchange rate when transacting across countries

Making It Work

The foundation of a state-sponsored cryptocurrency would be much like Bitcoin - individuals or companies would utilize computer-generated public "addresses" to send and receive payments. Payers could use an electronic wallet on a smart-phone or computer to send money to the public address of the recipients. Unlike Bitcoin's current system, however, banks and other financial institutions , previously approved by the Central Bank, would be the custodians of a shared, distributed computer-based ledger (called a blockchain in Bitcoin parlance). The currency in this distributed ledger would be existing fiat currencies (e.g., USD, CAD, Euro, GBP, etc.) rather than a new, unfamiliar digital currency like Bitcoin, and the digital currency would not necessarily have to supplant paper currency. A crypto-dollar would also need to have the same legal tender status as paper currency.

Similarities and Differences between State-Sponsored Cryptocurrency and Bitcoin

Ensuring Security and Controls

A key area of concern by those more critical of existing cryptocurrencies are their security and control mechanisms. In this scenario, existing Financial Institutions (FI) could link a private key to an identity (e.g., name, address, taxpayer ID) for AML and KYC purposes. These links would need to remain confidential to the FI and key owner except when disclosure is required by law. However, once a key-owner obtains a private key, it would be valid for life, and money could be transferred to that owner securely without any centralized party involved in the transaction. This means that the owners of private keys (individual or organizational) could transact with one another in real-time without an intermediary; there would be no requirement for banks or any central clearing house to be part of any transaction, and the transaction itself would remain essentially anonymous since only the public address would be exposed.

Banks and other financial institutions would still play a critical role. Financial institutions would serve as the processors of the distributed ledger (called "miners" in the Bitcoin environment), through which they could compete to process transactions and be rewarded with a small fee for their service. In short, banks would ensure that both the sender and receiver of the payment have a valid private key in the ledger, as well as confirm that the sender has enough funds for the transaction.

Once a transaction is confirmed, it could be posted on the public ledger, thus making the transaction transparent, auditable, and irreversible. In a key departure from the Bitcoin system, financial institutions would not be able to mine crypto-dollars, but would be solely responsible for processing and confirming transactions. This scenario would certainly mean a big change for banks, as the need for an intermediary could decrease once users have the ability to safely store their crypto-dollars on their private keys. However, although demand for traditional banking products might diminish, a constant revenue stream from processing the ledger's transactions, together with a regulatory push, might encourage banks to accept their transformed role in the new ecosystem.

Key Players in a Potential State-Sponsored Cryptocurrency Environment

Player	Role
Central Bank	• Expands or contracts the money supply of the distributed ledger • Validates, authorizes, and governs over the ledger's processors, therefore maintaining a distributed but trusted group of processors
Bank	• Acts as the custodians of a shared, distributed computer-based ledger. • Registers end-user in the blockchain by creating a private/public key pair and tying to user's identity. Banks do not have control of users' private keys. • Serves as the processor of the distributed ledger, competing to process a transaction and getting rewarded with a small fee for its service • Provides interest bearing accounts, and other current banking services, to users
End-user	• Obtains a private/public key pair from a bank by providing personal information. Information remains confidential and protected by the bank • Sends and receives money from other users securely through the blockchain, without any centralized party involved in the transaction • Has control of his/her private key. If the user wants to earn interest on his/her money, similarly to conventional investments, he/she could open an account with a bank and transfer his/her cryptocurrency to the bank, as any other two way transaction
Exchanges	• Converts users' cryptocurrency to paper currency when transacting across different currencies, and charges an exchange fee in return

Driving Lower Processing Costs

As we have seen with Bitcoin, cryptocurrency transaction fees also have the potential to be dramatically lower than current credit card fees or check processing costs. By creating a distributed, but trusted, group of processors the goals of openness, competition and security could be balanced. Individuals could transact with one another without the need for a centralized authority – financial institutions would have to reach a consensus in order to process/confirm a transaction and the Central Bank would play a key role in authorizing financial institutions as processors but exercise no authority at the transaction level.

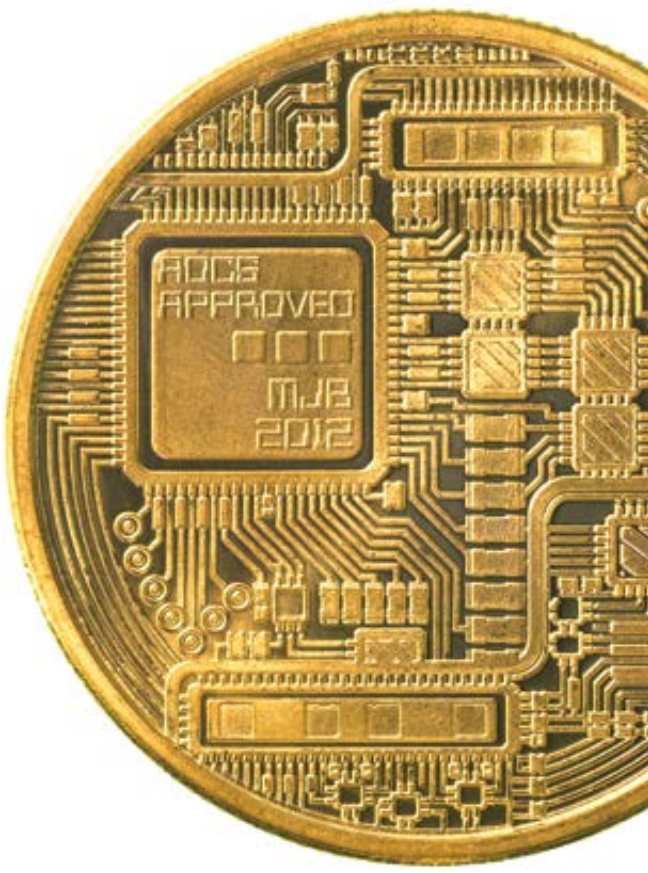
The Impact on Monetary Policy

In this hypothetical scenario, the Central Bank could expand or contract the money supply just as it does today (for example, the function and structure of the U.S. Federal Reserve banks would be unchanged), through open market operations. The increase and decrease of cryptocurrency money in circulation could be governed by the Central Bank, according to demand, policy, and protocol (just as with fiat currency). In order to increase the supply of money, a Central Bank could transfer crypto-dollars, in real-time, from its private key to different financial institutions' private keys. In order to contract the money supply, a Central Bank could increase reserve requirements and financial institutions would transfer crypto-dollars to the Central Bank's private key, in a manner that would be functionally identical to how this process works today. Interest rates would be the same as they are for fiat paper money. Reserve account balances for banks would be maintained on the distributed ledger, offering additional benefits of instantaneous and free funds transfer. Over time, as the demand for paper currency reduces, so too would the bank's costs to manage it.

Under state-sponsored cryptocurrency, supporting cross-border payments would be straight-forward and not require any additional steps than previously described. The payer and payee requirements would be the same; that is, foreign entities (banks, businesses or private citizens) would obtain a private key on the cryptocurrency's distributed ledger through the previously mentioned regulated channels. Once they have the private key, they could seamlessly transfer money in the source currency, applying the same conversion rates as fiat currencies do today.

Conclusion

Applying Bitcoin's innovation to the myriad issues in today's payment ecosystem offers an exciting opportunity. While this highlights only one hypothetical scenario, the goal is to advance the debate on the future of the payment system as there are a number of alternative routes that may be pursued. And while a state-sponsored cryptocurrency may not replace Bitcoin or any other virtual currency or paper fiat currency in its entirety, in this hypothetical world, consumers and institutions might be utilizing several digital wallets built around multiple currencies like Bitcoin, airline miles, credit card points, and the like. Consumers would be able to choose the most appropriate currency for a particular transaction with the best exchange rate.



Illustrative Benefits and Challenges w/Crypto Currency

	Pros	Cons
Consumer and Merchants	• **Improved support for the un- or under-banked:** Besides a one-time, initial verification of identity processed by financial institutions, individuals would need nothing other than a smart-phone or computer to receive and transfer money. For example, paychecks could be deposited against an individual's public address with immediate access to the funds. • **Reduction in payments-related fraud:** The traceable and audit-able nature of the public ledger could drive less fraudulent activity within the ecosystem. In a utopian vision, more secure and traceable financial transactions could ultimately reduce crime, much like video surveillance has proven to do in cities. • **Increased investment:** There would likely be a large flow of new investment into technologies to further improve mass usability of the cryptocurrency.	• **Increased cyber-theft:** Consumers would have increased ownership and responsibility for their own money in this scenario, which could cause a rise in cyber-attacks/thefts on individuals' private keys and wallets.
Financial Institutions	• **Service Development:** There could be a significant number of new opportunities for products and services from financial services companies, which would not necessarily cannibalize other products and services. For example, banks could offer cryptocurrency wallet services and still offer interest bearing accounts (insured by the FDIC).	• **Product Development:** Financial institutions would likely experience a significant disruption to their traditional business models and products. Although traditional bank products (interest bearing accounts, demand deposits, loans, etc.) would still exist, banks might have to raise interest rates or develop new products to attract end-users who now have the option of securely storing their own money. • **Legacy infrastructure:** Debit cards, cash transactions, credit card networks, ACH, wire transfers, money orders and other money transfer services would be the most directly impacted. Most of the players offering these services today would have to significantly change their current operating models as adoption of the state-sponsored cryptocurrency's increases. This is due to the fact that having the ability to transact through a public ledger would either be more efficient than traditional services (e.g. a transaction is potentially faster, cheaper, and more secure than ACH) or slowly eliminate the demand for these services completely (e.g. cash). • **Infrastructure build:** Banks would need to incur the costs of establishing the proper technology infrastructure for processing and validating crypto-dollar transactions. Financial institutions would do this in order to have access to a constant revenue stream from processing the ledger's transactions (especially considering the lower demand that will exist for some of the FIs' traditional products); they would also have to follow the regulations set up by the government regarding putting this infrastructure in place. The appropriate government agencies would need to establish regulations, as well as build in the necessary alterations to the processing algorithm, in order to assure that all banks, regardless of size, could compete fairly to process transactions. • **Exchange efficiency:** Foreign currency exchanges would probably become cryptocurrency-enabled and, with lower costs to process -- and a larger consumer base -- FX spreads would be reduced.
Government	• **First-mover advantage:** Potentially, the first central bank to adopt this technology could enjoy increased attractiveness for their currency as a medium of international trade. • **Cost savings:** As cryptocurrency might gradually replace paper and coins in this scenario, the central bank and commercial banks could reap significant savings in the printing, transportation, storage and destruction of currency.	• **Governance:** New government entities would likely have to be created in order to assure proper governance, regulation, and implementation of this initiative.

So while the scenario posed by cryptocurrencies carries challenges, it could ultimately spawn a series of new opportunities that would free up capital for more productive uses, and transform the current payments system into one that is faster, more secure, and less expensive to run.

Contacts

Eric Piscini
Principal
Deloitte Consulting LLP
+1 678 477 5092
episcini@deloitte.com

Simon J. Lapscher Rosemberg
Business Consulting Analyst
Deloitte Consulting LLP
+1 404 825 5131
slapscher@deloitte.com

Contributors

Jim Eckenrode
Executive Director
Deloitte Center for Financial Services
+1 617 585 4877
jeckenrode@deloitte.com

Val Srinivas
Research Leader—Banking & Securities
Deloitte Center for Financial Services
+1 212 436 3384
vsrinivas@deloitte.com

Denise Rotatori
Manager
Deloitte Consulting LLP
+1 646 226 6028
drotatori@deloitte.com

Andrew Garfrerick
Senior Consultant
Deloitte Consulting LLP
+1 404 942 6726
agarfrerick@deloitte.com

Frances Symes
Senior Consultant
Deloitte Consulting LLP
+1 646 341 2540
fsymes@deloitte.com

Additional contributions by Chris Martin.

[1] "Strategies for Improving the U.S. Payments System", The Federal Reserve System, Jan 26, 2015.

[2] Since a receiving entity would require a Private Key and those are established through regulated FI's, it is expected that some regulation on the receiving end would be implemented.

[3] In Bitcoin, **anyone** can serve as the processor of transactions which openly creates risk of nefarious actors.