colorplatform

Color Pay :

Next Paradigm for Instant Payment

Table of Contents

Abstract

Ever since the introduction of Bitcoin, thousands of cryptocurrencies each boasting its own technical edge have emerged. Unfortunately, current cryptocurrencies face the same issues that hinder wider adoption. Slow transaction speeds that make them unsuitable for everyday use and security concerns regarding cryptocurrency exchange breaches and securely storing coins for non-technical people.

We aim to resolve the above two fundamental issues found in existing cryptocurrencies with our solution Color Pay that utilizes PUF (Physical Unclonable Function) chips. By leveraging the power of PUF chips, Color Pay enables users to enjoy fast and secure transactions both online and offline.

1. What is PUF?

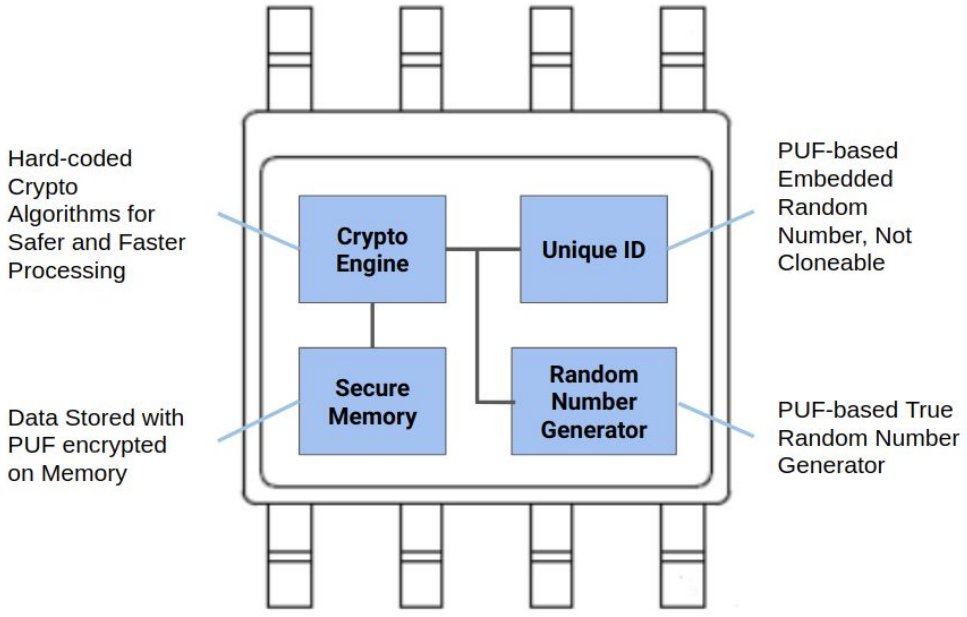
[Figure 1] PUF Chip Conceptual Diagram

1.1. Overview of PUF

PUF(Physical Unclonable Function) is a security concept formulated to develop physically unclonable semiconductors. The fundamental technology is based on the unpredictable irregularities caused by subtle differences in the physical structures of the materials used.

These natural irregularities occur under the same chip design and under the same production environment. The produced chip thus has a “fingerprint” unique to itself. In short, PUF can assign unique and unclonable fingerprints to the semiconductors, eliminating the need to devise a separate private key creation method.

1.2. Architecture of PUF Chip



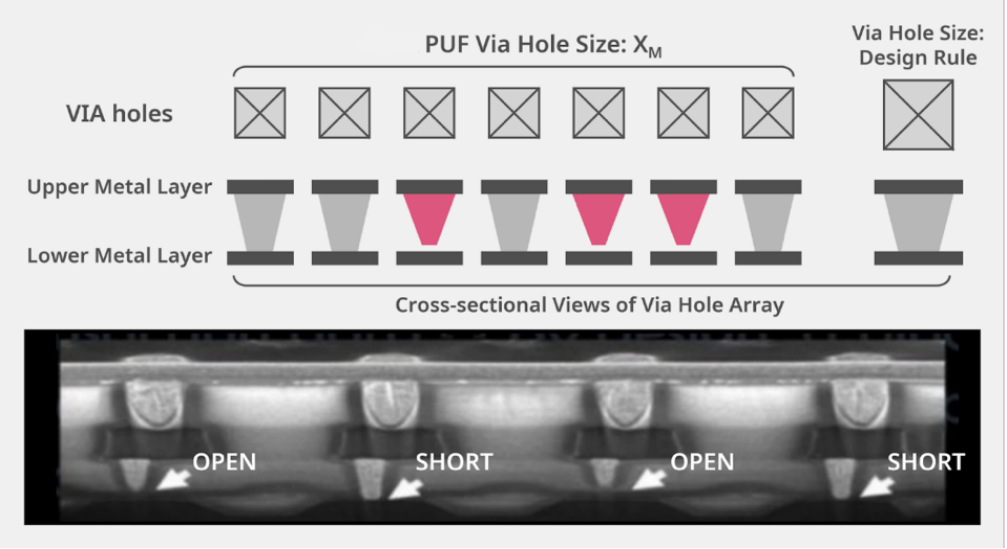
[Figure 2] PUF Chip internal structure

PUF chips are composed of the following:

1. Crypto Engine : Performs encryption tasks such as the SHA256 hash function
2. Unique ID : Creates an unclonable ID inside the PUF chip
3. Secure Memory : Capable of storing 10-20 kB of encrypted data
4. Random Number Generator : Creates random numbers required for encryption

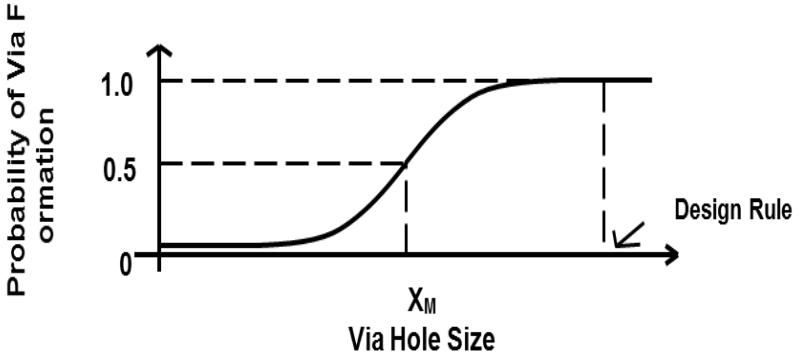
Unique ID is where the unique fingerprint, or the unclonable ID, is created. The ID is then combined with the Random Number Generator to create the private key used in the wallet.

1.3. Internals of PUF Chip



[Figure 3] PUF VLSI (Very Large Scale Integration) chip

The figure above shows the conceptual diagram as well as the actual picture of the Via[1] holes formed in PUF chips. The randomness of the Via holes created during production is what enables the implementation of PUF chips.



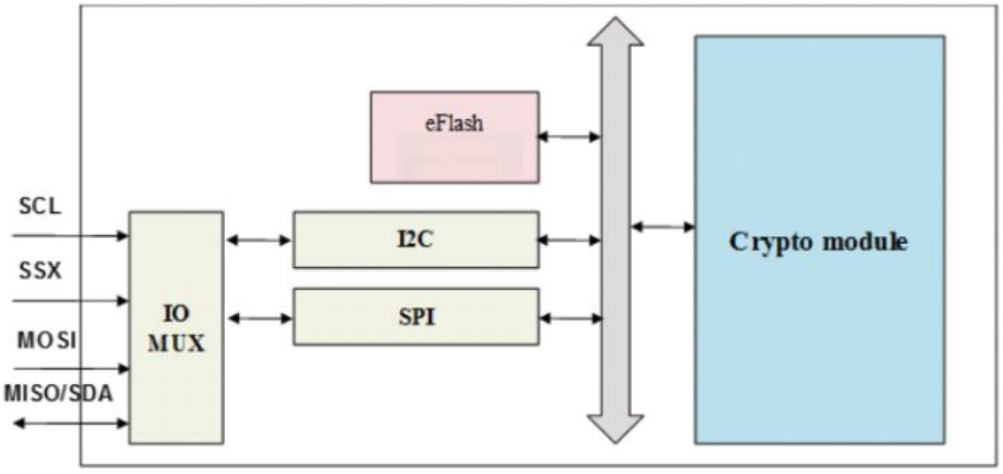
[Figure 4] The Probability of Via Formation with Via Hole Size

[1] https://en.wikipedia.org/wiki/Via_(electronics)

During the production of semiconductors, the second OPEN should be OPEN in accordance with the architecture but it can actually be either OPEN or SHORT. This is because the VIA hole size decides whether VIA will be created or not as shown in the figure above.

We can define OPEN as 0 while SHORT as 1 and there are approximately 3000 to 4000 VIA holes in a PUF chip. The encrypted key inside the PUF chip can have $2^{3000} \approx 10^{300}$ combinations. This is larger than the number of atoms in the universe, which stands at approximately 10^{80}. Thus, using PUF means holding a PUF chip that is globally unique. The uniqueness of the encrypted private key is the basis for the security of PUF chips.

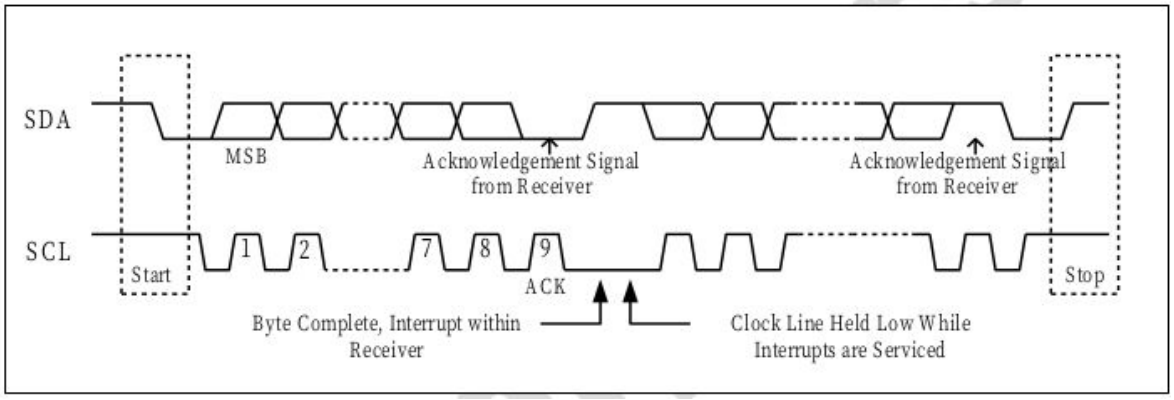
1.4. External Interfaces of PUF Chip



[Figure 5] PUF chip external interface

The figure above illustrates the crypto module, internal memory (eFlash), and external interface. Currently, I2C (Inter-Integrated Circuit developed by Philips) and SPI (Serial Peripheral Interface Bus developed by Motorola) are used to connect with other chips inside smartphones.

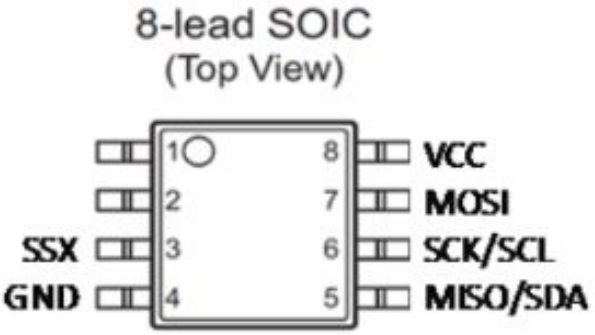
The following illustrates the I2C communication.



[Figure 6] PUF I2C (Inter-Integrated Circuit) communication

Many different semiconductors used in smartphones communicate through I2C. For example, fingerprint sensors and vibration sensors all communicate through I2C. PUF chips can also use I2C as well.

PUF chips have the following structure with 8 pins. The chips are placed inside phones or encased separately in external hardware.



[Figure 7] PUF chip package

A PUF chip has 8 pins and it is packaged in a small dimension of 5mm by 6mm.

Name	Type	Description
SSX	I	Master selection
GND	P	GROUND
MISO/SDA	O / I/O	SPI Serial data output / I²C Serial data
SCK/SCL	I	SPI/I²C Serial clock input
MOSI	I	SPI serial data input
VDD33	P	Power

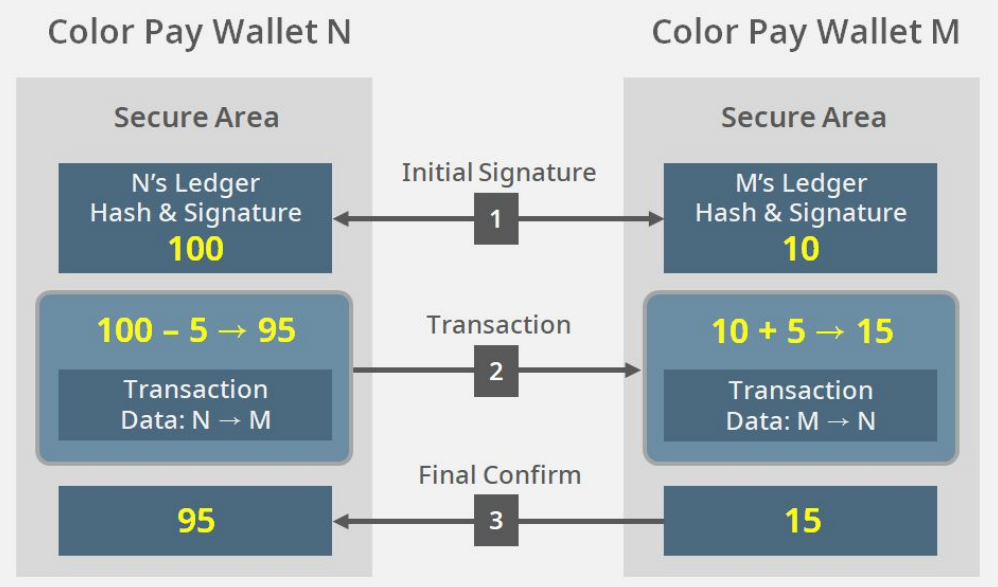
[Figure 8] PUF chip pin description

The 2 SDA/SCL pins out of the 8 pins are used for I2C communication while the 3 MISO/SCK/MOSI pins are used for SPI communication.

2. Transactions with PUF Chips

PUF chips allow anyone to easily execute offline P2P transactions of cryptocurrencies. These chips can be a solution to the sub-par TPS that existing cryptocurrencies suffer from.

The following diagram summarizes how the PUF Chips make offline P2P transactions possible.



[Figure 9] PUF Secure P2P OFFLINE Transaction

1. Check the public keys and balances of the two PUF wallets N and M through the PUF chip's secure communication channel.
2. Decrease the amount of coins to be sent from the remaining balance of wallet N and send the coins to wallet M through secure communication.
3. Increase the balance of wallet M by the amount received and confirm through secure communication.

P2P transactions using PUF chips are stored safely inside PUF chips. The saved offline P2P transactions are automatically synced with the Color Blockchain when internet connection is available.

	COLOR	BTC	ETH	EOS	VISA
Consensus	**DPoS**	PoW	PoW	DPoS	Central Server
TPS	**2k - 4k P2P: instant**	3 - 5	20	2K - 4K	1.7K (Normal) 56K (Peak)
Comments	**P2P OFFLINE Transaction**		Will be improved w/ Plasma		

[Figure 10] TPS (Transaction Per Second) comparison

Bitcoin can currently handle about 5 transactions per second while Ethereum can handle around 20 transactions per second. These sub-par TPS values makes them impossible to be used for everyday payment, unlike VISA.

Color aims to fundamentally resolve the TPS issue by leveraging PUF-based hardware. This is possible because Color coins based on PUF do not depend on block confirmation speed to execute offline P2P transactions.

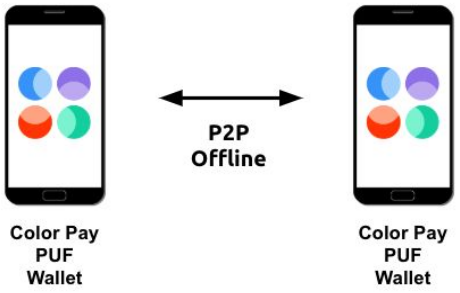
EOS, one of the fastest blockchains, can hit 1000 to 2000 TPS. This is up to par with VISA's average TPS of 1,700 but not close enough to the 56,000 TPS that VISA can handle during peak usage in holiday seasons. EOS also depends on internet connection, which makes it impossible to use in isolated areas such as in the mountains or islands.

Color coins can execute transactions offline and theoretically have no ceilings when it comes to TPS values.

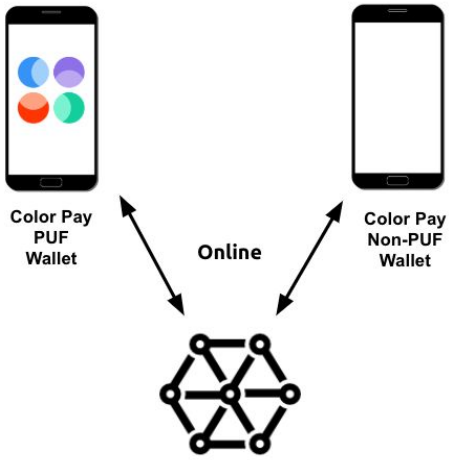
3. Example Use Cases

Let us see how users can make payments using Color Pay in real-life. Color Pay includes the PUF hardware based Color Pay Wallet and the software-only Color Pay App.

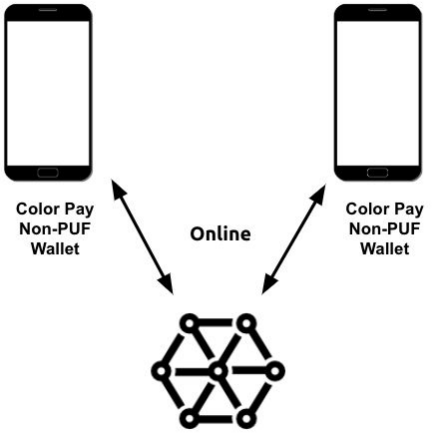
1) Color Pay (PUF chip) ↔ Color Pay (PUF chip) : **P2P OFFLINE Transaction**



2) Color Pay (PUF chip) ↔ Color Pay (Software) : **Online Transaction**



3) Color Pay (Software) ↔ Color Pay (Software) : **Online Transaction**



Using the Color Pay Wallet enables a safe offline P2P transaction. Those without Color Pay Wallets are not left out as active development is ongoing for the color pay software app. However, the TPS for the color pay app may be as slow as the existing blockchain solutions.

Color Pay Wallet users can enjoy fast and easy payments through the Color Blockchain with anyone around the world, whether or not a stable or existant internet connection is present.

PUF wallets are currently being integrated into Smart Card and USB devices, but can be expanded to other form factors in the future.

4. CBDC with PUF Technology

Central Bank Digital Currency (CBDC, also called “Digital Fiat Currency” or “Digital Base Money”) is the digital form of fiat money regulated by the government. CBDC is different from virtual currencies or cryptocurrencies as these are not issued by the government and thus lack the legal status.Various states are initiating discussions on the prospects for the introduction of CBDC.

However, there has not been any detailed discussion on the technical requirements for such instruments to appear. CBDC can be possible only through a reliable platform that offers both offline and online transactions in a secure manner. CBDC will require the same properties of fiat money while adding the convenience of online transactions possible with cryptocurrencies. As such, CBDC will require PUF based Color Pay to enable reliable monetary transactions and ultimately replace old fiat money.

The table below compares the properties of each form of money.

	Fiat	Blockchain	CBDC	Color Pay with PUF
24/7 availability	O	O	O	O
Anonymity	O	O	X	X
P2P transfer	O	X	O	O
Limits or caps	X	O	X	O

[Figure 11] Comparison of various forms of money

5. Conclusion

PUF-based Color Pay aims to be the first truly usable and viable blockchain killer app. PUF technology solves the two most fundamental issues in blockchain, slow transactions and security concerns. Leveraging the uniqueness of each semiconductor chip produced, Color Pay provides users with secure private keys that are not hackable or cloneable.

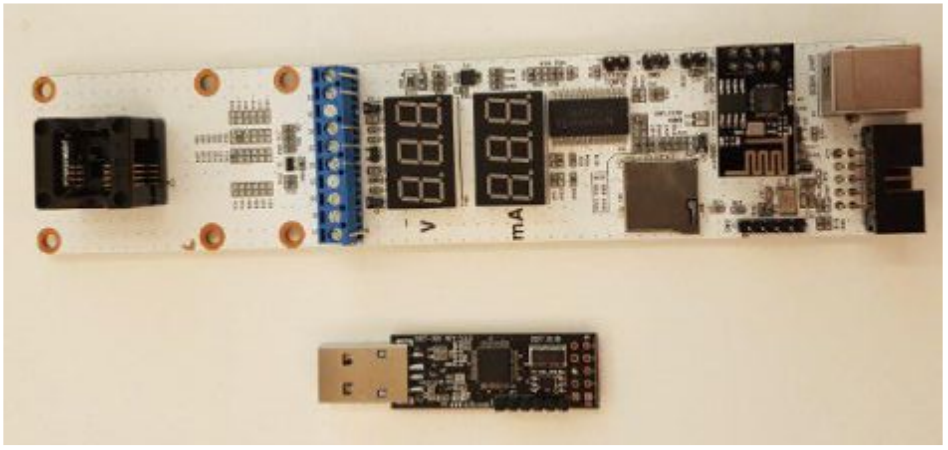
Color Pay is not just for the blockchain geeks but for the general public to use in everyday life. Furthermore, Color Pay allows those who live in disconnected areas to make secure transactions. We are confident that Color Pay will be next paradigm in cryptocurrency innovation.

Reference

1. Color Coin : https://www.colors.org/
2. PUF Chip : http://m.blog.daum.net/serapeum/7594748
3. Bitcoin Hardware Wallet : https://en.bitcoin.it/wiki/Hardware_wallet
4. Sirin Coin : https://sirinlabs.com/
5. CBDC(Central Bank Digital Currency) : https://www.bis.org/cpmi/publ/d174.pdf

Appendix

[Figure A] USB type Color Pay



[Figure B] Color Pay prototype in development