Past to Present Overview of Mobile Wallet Payments Architectures to Compare and Identify Overall Participants

Mansi Bosamia
Smt. Chandaben Mohanbhai Patel Institute of Computer Applications,
Charotar University of Science and Technology (CHARUSAT)
Changa, Anand, India

Dharmendra Patel, PhD
Smt. Chandaben Mohanbhai Patel Institute of Computer Applications,
Charotar University of Science and Technology (CHARUSAT)
Changa, Anand, India

ABSTRACT
In the current trends, smart phones became a continuous necessity of a person. Early era, mobile phones are only used for calls, then for few apps and now for everything by just one touch. Smart phones are exclusively personal devices; they are becoming the substitution of physical cash payment by instant payments with two-factor authentication. There are numerous architectures and security issues identified due to the fast enhancement of mobile wallet services in the markets, and the history of mobile wallet identifies tried and failed solutions. There are still alive possibilities of new promising innovative research. At this point of mobile wallet innovations, we take a literature review on available mobile wallet transaction architectures and identify the number of overall participants in these architectures. This study also gives an analysis of architectures with its use, advantages, disadvantages and comparisons.

Keywords
Mobile Wallet, E-cash, Consumer, Merchant, Agent, TTP (Trusted Third Party), IFI (Interconnected Financial Institutions)

1. INTRODUCTION
Mobile phones are the continuous necessity of people. That is the reason new era with mobiles and its apps, especially for mobile wallet apps. The mobile wallet apps concerned number of management such as mobile wallet running platforms, wallet account, consumer/business system, banking system, mobile client account, service providers, etc. The mobile wallet is widely used and its application adds two kinds of account platforms, online platform and offline platform.

1. **Online:** The online platform manages temporary account with mobile wallet cash, discounts, returned money instead of product returned or service refused. These transactions directly affect to your bank account balance.
2. **Offline:** The offline platform manages same as online, differs to transaction affect to the mobile wallet cash instead of bank directly. Its transaction amount limit based on mobile wallet software or app. It also manages offline payments balance.

For online and offline both, sends the merchant details to consumer at the time of product/service sale. As per the transaction mobile wallets sends information to the bank. A transaction detail is verified by mobile wallet account platform and manages them. After that mobile wallet platform transfer details to the bank management system to update the transaction amount to the merchant and consumer accounts. As a result, either consumer account amount decreased and merchant increased, or if the transaction failed consumer account amount and client account amount as it is and notify the client about transaction failure. Also, note that if client account amount deducted then refunded soon with proper notification. We can say that mobile wallet replaces the physical cash with electronic cash (e-cash). There are various key properties determined the e-cash. For that, step by step e-cash properties was defined and implemented such as Anonymity, Double spending prevention, Untraceability, Unforgeability, No framing, Auditability, Pseudonymity, fairness, recoverability, and transferability [5]. These all e-cash properties are important and have the strike on system distribution of mobile wallet payment architectures. Each of the properties had an impact on mobile wallet architectures cum schemes. Before understating the mobile wallet architecture we need to understand technical definition of the mobile wallet.

2. WHAT IS MOBILE WALLET?
Mobile Wallet is a virtual wallet in your Smartphone, in which your virtual money is stored to make money transactions and payments. It has the combination of software and hardware on certain devices so it can replace the use of traditional credit/debit cards with mobile phones via information added to your mobile wallet. You can pay money using Smartphone apps, text messages, social media or websites.

"A mobile wallet is an application as all in one for payments through smart phones with filled credit/debit card information in it to replace the use of physical card." [13]

Three Simple steps to use Mobile Wallet

1. Use inbuilt mobile wallet app or install it on your device.
2. Add your credit/debit card information to the mobile wallet.
3. Then start the online in-store purchase, after selecting item/service indentify the participating business merchants, and uses your mobile wallet card information to make payment. Before using a mobile wallet always prefer security measures that mobile wallet provides.

3. MOBILE WALLET PAYMENTS ARCHITECTURES WITH ITS ADVANCES AND DISADVANTAGES

Mobile wallet payment architectures may require individual players and the entities for communication or operate independently in system distribution. At that time, they may impact either positively or negatively. These players are key component or participants in discussed architectures of this paper. The payment architecture includes the consumer (user/client/payer), the merchants (payee), banking management (service providers), and security measures (like authentication, network security, two-way authentication etc). Generally, all players physically distributed so far from each other, it is compulsory to identify the number of merchants, consumers, and banking transactions in their communication for mobile wallet payments. Based on these, in general cost of mobile wallet management system is identified and possible to provide better service quality [5].

The architecture styles are design with achieved basic properties at the time of mobile wallet management system distribution. Each of the architecture must supports several deform with centralized model, which achieves the trust of individual player in management system. Most of architectures are e-cash architectures, which built along the bank to form a centralized architecture. However, some of the architectures are explicit as dedicated architecture with predefined necessary roles in implementation to achieve required properties. Here identified the basic two categories, first, fundamental architectures and second, latest architectures.

3.1 Fundamental Architectures

Now a day, lots of research works has been produced on mobile wallets. Here the basic architectural families concisely explained. In these families three architectures are: Online Architecture, Offline Architecture, and Transportable Architecture.

3.1.1 Online Architecture:

It is default architecture of mobile wallet, which has been used consistently for mobile wallet payments, mechanisms, and protocols. Online architectures have three participants: Consumer, Merchant, and the Bank. Refer Fig. 1 for online architecture working. In this architecture, the consumer credit/debit cards details in his/her mobile app/device and uses these details for online purchase of items/services. Merchant receives mobile wallet cash for selling items/services to consumer. Bank is responsible for managing the card issues for consumer and its transactions with few charges. Bank verifies and manages the cards money and its transactions by consumer and merchant using mobile wallets. At the time of transaction consumer money deducted and transfer/added to merchant account. This is done based on mobile wallet payment request for behalf of purchase.

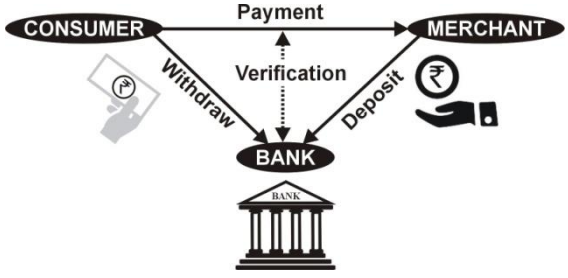

Fig 1 : Online Architecture

Uses

Online architecture mostly projected in the literatures to identify e-cash properties mandatory for transaction. In Medvinsky and Neuman's NetCash [8], focus on flexible and fair transactions with tentative consumer anonymity. While NetBill scheme of Sirbu and Tygar [9] has no consumer anonymity. Then, Chaum [10] projected the cash verify scheme with unrestricted consumer anonymity, that makes towering processing cost, thus not suited to micro payments. This limitation improved by Deng et al with blind signatures scheme. [11]. Wu, Huaigu, Louenas Hamdi, and Nolwen Mahe makes TANGO: A Flexible Mobility-enabled Architecture for Online Mobile Enterprise Applications, which uses the online architecture features by using loosely-coupled modules [31].

Advantages

- Online architecture is centralized.
- Bank plays important role for each transaction.
- Security supports by real-time double-spending prevention and detection.
- Due to centralized, trusted on bank as third party.
- Bank responsibility is more such as, transferability of amount, anonymity and transaction verification with efficiency behalf of mobile wallet.

Disadvantages

- Bank is responsible of payment transaction failure as performance bottleneck due to high load.
- Achieving payment untraceability can be very difficult.

3.1.2 Offline Architecture

This architecture is design to overcome the limitation of online architecture such as untraceability, bottleneck performance (single point failure), etc. It improves mobile wallet transactions independence and makes it more flexible. Offline architectures also have three participants: Consumer, Merchant, and the Bank. Each participant has same role as online architecture. Refer the Fig. 2 for third party payment. This architecture is unique in place of payment, it involves third party of payment instead of direct bank. In each transaction consumer and merchant involved not the bank. So there is no chance of single point failure. It uses double-spending scheme to overcome online architecture limitation but still there is few limitation in transaction results.

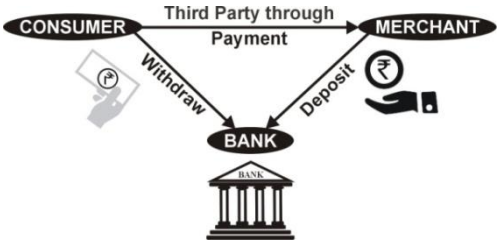

Fig 2 : Offline Architecture

Uses

Offline architectures projected in the literature include [5, 12]. This architecture related intense research is done in last decades and also going on. Chaum et al [10], proposed untraceable offline schemes. It is based on blind signature scheme, collision-free, cut-and-choose method, and one-way functions. The blind signature scheme makes sure about consumer anonymity at the time of e-cash payments [14]. Then blind signature used by the bank with few limitation which identified by Ferguson [13]. Wu, Huaigu, Louenas

Hamdi, and Nolwen Mahe makes TANGO: A Flexible Mobility-enabled Architecture for Offline Mobile Enterprise Applications, which uses the offline architecture features by using loosely-coupled modules [31].

Advantages

- Bank role is limited.
- Increased flexibility and autonomy.
- Uses double spending detection for security.
- Unrestricted client secrecy.
- Limited untraceability.
- Protection against coin forgery and framing.

Disadvantages

- Strong security is not available.
- Conceptual simplicity.
- Security limitation affects the performance and scalability.
- Increased the level of complexity.

3.1.3 Transportable Architecture

The basic architectures useful for basic mobile wallet transaction by existing card payment schemes. Transferability is mandatory for transportable architecture to achieve the high level of money transactions.

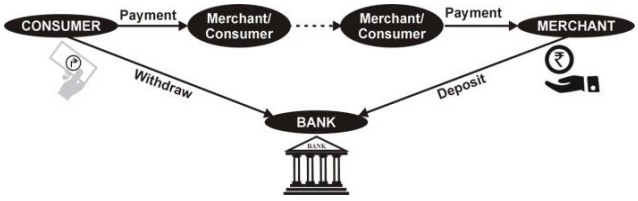

Fig 3 : Transportable Architecture

In this architecture, private details are allowed to switch between persons at the time of mobile wallet payments. Transportable architecture has four participants: Initial Consumer, Final Merchant, Agent for payment, and the Bank. Initial Consumer, Final Merchant and the Bank has same role as above architectures. Agent plays important role of Consumer/Merchant as per the payment transactions. It is also known as transferable architecture due to transferability.

Uses

Uses of this architecture projected in the literature include [5]. It mostly used for transferability property of e-cash payment at the time of system distribution. As per the design it makes transaction between consumer and merchant without bank [15]. As a result, it has ability to reuse the transaction coins for payment without bank.

Advantages

- The bank role is limited.
- Integrates more flexibility and autonomy.
- Supports autonomous and considerable scalability.
- Supports distributed processing.
- It has major performance issues.
- The split secret scheme is proposed [5].
- Reliability can be achieved, if the POS connect to the bank continuously and also update the blacklisted consumer and merchant.
- The bank maintained database size is decreasing by the validating date which bound the transaction list size.
- Transferability property is achieved.

Disadvantages

- Transfers are limited in numbers.
- Huge fake transactions cost.
- Requires some traceability mechanisms to identify fraudsters.
- Not to ensure full anonymity and security.
- Point of Sale (POS) is necessary for offline access.
- Need to maintain the size of coins to avoid all the reclaimed coins.
- State to make certain pseudonymity.

3.2 Latest Architectures

The advance latest architectures are classified into five styles as follows: Distributed Banking Architecture, P2P (Peer-to-peer) Architecture, Randomized Architecture, Agent-based Architecture and NFC-based Architecture. Advanced latest architectures discover the requirements of system distribution and security in a balance manner. It also faces main problems to optimize number of communication between participants and the bank.

3.2.1 Distributed Banking Architecture

In online architecture, the main un-trusted zone is the bank and that problem overcome by offline architecture so the trust is increased from the un-trusted zone. Another approach to overcome problems is distributed banking architecture. It has two special viewpoints. The first viewpoint is to make merge scheme of the number of banks for payment to improve scalability [16]. The second view point is distributing the bank roles between numbers of participants to decrease the load of the bank [17].

In this architecture, there are four participants are: Consumer, Merchant, the Banks group, and the Central bank/banks group manager. At the time of purchase, consumer mobile wallet app creates the coin and sends to his/her bank for blind signature. Then the bank withdraws the amount from consumer's account and transfer money to his/her wallet. To increase security avoid the blind signature or use various blind signature for different coin values. At the time of payment, merchant receives signed coin from consumer with public key verification. By the signed coin amount transfers from consumer to merchant account and account balance updated. For security avoid double spending. [5]

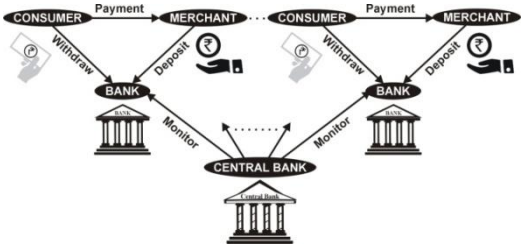

Fig 4 : Distributed Banking Architecture

Distributed banking architecture overcomes the limitation of online and offline architectures but it decrease anonymity. For that the modified distributed banking architecture introduced, in this consumers makes a bank group and it controls by central bank as trusted third party. At the time of purchase consumer sends coin to bank group for signature and given to the merchant. Merchant verifies the coin with central bank to indentify fraudulent consumer. The consumer identity was fully secret by bank of group and central bank. This concept introduced by Xu and Zhao [20] in a distributed banking environment. The bank group is fully mirrors of the banking system [16]. Bank group manages the e-cash and each

transaction monitored by the central bank. For security bank group uses blind signature scheme.

Lysyanskaya and Ramzan proposed distributed banking architecture. In this architecture, payment system works by mobile wallet apps and its wallet money or cards. Each bank have own payment and authentication mechanism. By this mechanism difficult to performed integrated transactions at various banks and its account transaction clearing activities. So the resource utilization is not optimal. To resolve this problem Lysyanskaya and Ramzan modify the third-party model and introduces the central bank (group of banks). [16] Refer the Fig. 4 for central bank concept to work in distributed banking architecture. For security, Camenisch and Stadlers' propose the group signature scheme as blind signatures group [18] to authenticate by central bank. Thus, it is also called group blind signatures. Basic group signatures concept is given by Chaum and van Heyst [19].

Uses
The distributed banking architecture implemented and testes for distributed e-payment gateway by Xu and Zhao [20]. This concept tested by Hopeman for online decentralized environment without bank groups (central bank) to resolve double spending. Each bank verifies all requests and suggests the randomization for preventing the multiple times coin spending. This architecture uses the central bank mechanism and to handle properly selected clerk sets which is responsible for coins validity at the time of payment transactions. The clerk sets mostly selected by the merchant randomly. By selecting appropriate clerk sets avoid double spending of coins. Clerk sets validate coins by its history and an assumption of static network and tiny coin operations. This is addressed by distributed banking architecture.

Advantages
- Remove the bank bottleneck issue by central bank.
- Central bank redistributed the load between banks group for performance improvement.
- Supports Blind signature and Group signature.
- Central bank distributes the e-cash to mobile wallet apps on requests without showing the identity of the issuing bank.
- Distributes e-cash are untraceable and anonymous.
- Bank roles transferred to the other players.
- At same intensity of security in online architecture gives more scalability.

Disadvantages
- When size of public key increases (scalability) the group signature does not support.
- The transferability is not addressed.

3.2.2 P2P (Peer-to-Peer) Architecture
The P2P basically design for the decentralized banks which transfer centralized entity to a solid network of banks. This architecture uses the decentralized e-cash payment in distributed system. It avoids the central bank concept so it communicates independently without the interference of the bank.

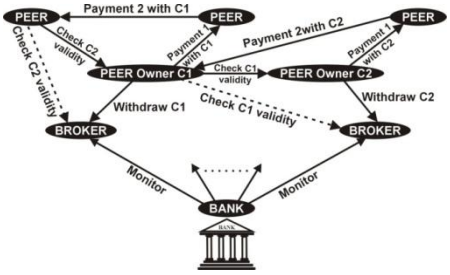

Fig 5 : P2P Architecture

As in Fig. 5, this architecture has four participants: Consumer, Merchant, Bank and the Broker. Consumer and merchant play the same role in above architectures as peers. Bank roles plays by broker. Peer-to peer purchase and the payments are done in this architecture. At that time bank involved directly or indirectly through the broker. Thus, the bank has to play a limited role. So the each participant has most suitable load. The bank distributed its role to broker or peers which improvers the overall performance of the system. In this place P2P differs from distributed banking architecture. The broker can be online or offline and plays banks role as the transaction participants. A broker works for mini-payment network. Consumer plays an active role for coin validity at the time of creation and scrutinizing. At the time of purchase, coins given to consumer by broker with assigned merchant randomly. This assigned merchant is receiver of coin payments. At the time of payment consumer transfer coins to merchant then it forwarded to broker for authentication. After authentication it's back to merchant and again transfer to broker for payment. Broker will verify the coins of transaction and accesses the secret details and informs the merchant for real/fake transaction payment.

Uses
PPay micropayment scheme use P2P architectures with scalability, security, fairness and reliability but it do not support secrecy [21]. PPay formulate distinction between transaction coin's issuer and its user. Originally, the consumer purchases the coin from broker and at the time of purchase of goods/service transfer that coin from consumer to merchant account for payment. This is the lifetime of that purchase coin. PPay does not supports secrecy, thus it allows the coin access to identified parties only and avoids double spending except the consumer. PPay extended version WhoPay proposed by Wei et al [22] with more scalability, anonymous, security, secrecy, fairness and transferability. It also added the trusted third party roles as a group manager for consumers. It uses group signatures for security. PPay and WhoPay both uses P2P architecture life cycle for distributed load access [5].

Advantages
- The distribution between the various consumers of the payment and verification done by either broker or the merchant.
- The consumer payment done by broker (as consumer temporarily) and transfers requests, and later matches the stat with corresponding consumer.
- The broker plays the role of the bank.
- By the double-spending detection and distributed verification with merchant, removes the single point of failure.
- Bank load is reduced compare to other architecture.
- Supports distributed processing and scalability.

Disadvantages

- Always online consumer's coins are accessed at the time transactions.
- Full anonymity cannot be achieved.
- Coin user is hidden, but coin issuer is shown.

3.2.3 Randomized Architecture

P2P architecture has significance of connectivity at the time of distributed banking. Connectivity defines the intensity of communication between the mobile wallet app and the bank using the coin. In digital wallet cash system has three types of connectivity: online, offline and hybrid. Online and offline previously discussed. Hybrid system has both types of connectivity and need to identify working mode is consistently either online or offline. This system does the probabilistic randomized checks/audits by middle group (either central bank or broker) at the time of transaction execution. Thus, hybrid system known as randomized architecture. At the time of online payment verified by the bank and at the time of offline payment verified by the middle group. As per randomized system distribution, this architecture is more meaningful for the scale the range of online and offline transaction with the bank [23]. Basically increase the randomized architecture use in hybrid system.

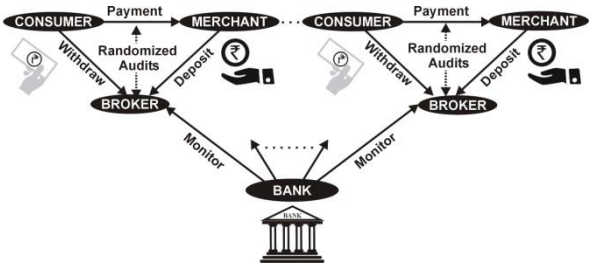

Fig 6 : Randomized Architecture

Uses

The randomized checks/audits mentioned in few literature papers re is a small number of papers [17, 24, 25, 26]. The Hopeman proposed distributed banking architecture with randomized architecture scheme at the time of double spending prevention [17]. This scheme also used for double spending prevention with probabilistic checks/audits of coins by central bank [17, 24, 25]. It is also does the randomized checking of payment through broker (banks group) [17]. Yacobi projected combined hardware and software explanation of randomized checks/audits using this architecture. Exclusively it audits the mobile wallet signed coins. Yacobi also proposed use of this architecture in connection with adversarial consumers. It does the randomized checks/audits in banks group for fully online/offline transactions. It avoids the unfair transactions by these checks. [25]

Advantages

- Large cost of online verification is optimized.
- A probabilistic payment transaction checks/audits done randomly.
- Decrease the risk and cost of double spending in offline transactions.
- It accomplishing better performance and scalability except online transactions.
- For security requires permanent connectivity and systematic checking.
- Proposed hybrid system for better security and handy implementation.

Disadvantages

- There are security issues plaguing offline environments.
- Do not formulate for business perception.
- The attacker can attack by breaking their investment in defrauding the system.
- For concerning the cost of performance, scalability and communication, this architecture is not suitable.
- There is lack of security in real-life applications.

3.2.4 Agent-based Architecture

The previous architectures are based on e-cash schemes with the basic two participants, consumer and merchant; both have each other's information for purchase/sale items and payment. For a number of mobile wallets transaction involves uncoordinated and distributed architecture services. P2P allows determining and cooperating with probable operating partners. By the number of transaction communication has the issue of performance bottleneck and resource accessibility. So to address these issues Agent-based Architecture is introduced. In this architecture, it introduces a mobile agent who works behalf of consumer. Mobile agent does the different tasks such as processing, searching, selecting and negotiating. If these agents implicated with P2P architecture for bounded number of communications, it improves the distributed processing efficiency. By the use of agents we can make a framework for real-life application which is using a distributed architecture to perform a required task. In near future, a multi-agent system for mobile wallet payment may introduce and it may have very complicated issues for more verification and authentication. [5]

Fig 7 : Agent-based Architecture

Agent based architecture have five participants, Agent butler, Merchant host, Trusted Third Party (TTP), Payment gateway and Interconnected Financial Institutions (IFI) (Bank). The agent butler plays role of consumer and work behalf of consumer. The agent accepts transaction requests from the consumer/mobile wallet owner and manages as needed by particular transaction. Consumer does not require being always online and its required tasks performed by agent butler. The IFI has banking network for manages cash issues of consumer and merchant. IFI also manages inter-bank payment transactions. IFI uses the payment gateway as front of it for communications. TTP is responsible for trusted transactions in payment or purchase.

Uses

Agent based architecture used in Secure Agent Fabrication (SAFER), which is a mobile agent community. SAFER has a framework with agent based architecture for e-commerce (e-payment) transactions to mange by its agents [27]. SAFER community have independent agent cluster for managing different entities [5]. Agents are organized as multi- layered structure known as "Agency" in SAFAR community. Each agency stands for particular group of agents with specific proficiency such as Information Agency, Management Agency, etc. Agencies communicate with each other with control of agent butler to perform various transactions.

Advantages

- It is projected to be extensible and scalable.
- There are more feasible payment options are available.

Disadvantages

- Agent has e-cash control behalf of consumer so the possibility of stealing due to weak security.

3.2.5 NFC-based Architecture

This architecture uses Near Field Communication (NFC) technology. It works for wireless short range payment system with no user interference between communication devices. There are four participants in this architecture: Consumer, Merchant, Bank and NFC technology. According to Europay MasterCard Visa (EMV) specifications, these all participants make secure payment transaction using NFC technology. Consumer stores banking data such as bank account number, PAN card detail, expiry date, card owner details, cryptology, etc in mobile device. This banking data available with NFC based either credit/debit card or mobile device. NFC records the transaction information such as accounting, offline access, and purchase/return of items/services, etc by payment network and sends details to NFC based mobile wallet device and it affects bank account of NFC based system. NFC measured security by two-way authentication. This architecture makes security checks such as, consumer/merchant identity authentication, transaction information encryption, verification of data integrity, digital signature verification for end-to-end data transmission of payment transaction. The short range of NFC gives effective use in mobile wallet application to increase security without including the third party. The security authenticate based on consumer is online or offline. Mobile wallet app creates two keys, public key and private key. A private key is within phone memory as an encrypted file. The bank also creates private and public keys. The private key is within NFC based machine and it encrypted by that machine as master key, then stores in the system database. The public key is used for certification authentication for payment by singed private key of payment. If it authenticate bank generates consumer's certification for identification of real online or offline user instead of fake user.

Fig 8 : NFC-based Architecture

Uses

NFC used for wireless payment systems such as Europay MasterCard Visa (EMV), MaterCard PayPass, VISA payWare [source info, Google search, NFC news.] NFC feature can be included many ways for communication: NFC embedded with mobile device manufacture, NFC with Sim card, NFC with SD Card (with or without NFC controller), NFC through software as SE emulation, etc. NFC based architecture used for treadmill, weighting machine, mobile wallet payment, medical, etc. In NFC based mobile wallet payment, it monitors transactions and its data, also provides a perfect source of convenience. Due to the intuitive, it takes is a simple touch when using NFC for payments. NFC can be very well used by all kinds of situations running from bank cards to transit passes, movie passes, reward systems and even keys.

Advantages

- Supports Read/Write mode (similar to QR Code).
- Supports P2P mode such as Bluetooth paring feature.
- Security provides through two-way authentication and secure element (SE).
- Offline user's information can be access power given to NFC by electromagnetic field instruction.
- Online or offline connection of two NFC devices are faster than Bluetooth connection.
- More secured NFC enabled credit cards than a credit card magnetic strip.
- It requires PIN for more security.
- The retailers no longer have physical access to your credit card information.

Disadvantages

- NFC works for very short range payment system in cm.
- Company agreement need to use NFC.
- NFC has still security issues.

4. ARCHITECTURES COMPARISONS

There are number of architectures we had discussed, according to that refer table 1 as comparison table.

Table 1 : Architectures comparisons

Parameters	**Basic Online Architecture**	**Basic Offline Architecture**	**Basic Transferable Architecture**	**Distributed Banking Architecture**	**Peer-to-Peer Architecture**	**Randomized Architecture**	**Agent-based Architecture**	**NFC based Architecture**
Participants	User, Merchants, Bank	User, Merchants, Bank	User, Merchants, Payment	User, Merchants, Banks group,	User, Merchants, Broker	User, Merchants	User, Merchants, Agent, Bank	User, Merchants, Bank,

			Agent, Bank	central bank				NFC Service
Architecture type	Centralized	Three-party	Distributed	Distributed banking	Decentralizing bank	Distributed banking	Distributed	Security architecture
Transaction type	Online	Offline	Online	Online	Online	Online, Offline, Hybrid	Online	Online, Offline
Security	Double-spending prevention and detection	Double-spending prevention and detection supports after damaging result	Not to ensure full anonymity and security	Double-spending prevention and detection, blind/group signature	Double-spending prevention and detection	Permanent connectivity and systematic checking	Security weaknesses	Two-way Authentication, Secure Element (SE),
Supports trusted third party	YES	YES	YES	YES	YES	YES	YES	YES
Performance bottleneck	YES	NO	NO	NO	NO	NO	NO	NO
Supported Properties	Anonymity, Double spending prevention, Auditability, ,	Anonymity, Flexibility, Double spending prevention, Partial untraceability	Transferability, Anonymity, Flexibility, Reliability	Scalability, Auditability, Fairness	Security, Anonymity, Fairness, Transferability, Scalability	Auditability, Scalability	Transferability, Scalability	Transferability, Fairness, Connivance, Versatility, Safety

5. POTENTIAL PARTICIPANTS IN THE MOBILE PAYMENT ARCHITECTURES

Mobile wallet payment architecture contains all the technologies that will extend the users all tasks and provides secure successful payment transaction using payment service providers. In Fig. 9, there are potential participants in the mobile payment architectures.

Fig 9 : Potential Participants in the mobile payment architectures

Potential participants in the mobile payment architectures are:

- **Consumer/Users/Card holders:** User is the main participant who makes actual payment through credit/debit card or mobile wallet cash.
- **Mobile Device or Handset Manufacturer:** It contains mobile wallet app and communication technology (like NFC, QR code), and user digital cash. Some mobile device manufacturers traditionally produce mobile phones with payment functions.
- **Mobile Payment Application:** It contains credit/debit cards details, mobile balance, bank account details for payment transaction. It provides mobile wallet & account profile services.
- **Security & Authentication Provider:** Security can be supported by double-spending prevention and detection, Two-way Authentication, Secure Element (SE), user details authentication by pin, NFC, QR code, etc.
- **Mobile Payment Providers:** It provides services for make purchases, transfer money, pay bills, etc. Other common services include third party payments, online services access, etc.
- **Card Issuers:** It is bank or financial institutions for mange card holder identity, card validation and authorization service.
- **Payment Network Providers:** It provides token services, payment clearing & fund settlement facilities.
- **Acquires:** It is bank or financial institutions for

payment processing and authorization service to/from issuers.

- **Payment Service Providers:** It provides payment services for merchants. It provides cash-in and cash-out facility but not allows other banking transactions such as an account open/close, loan, check, etc.
- **Merchants:** It provides to hosting Point of Sale (POS) contactless terminals & POS servers with financial management system

A mobile wallet payment contains typical payment component such as mobile wallet money, credit card, debit card, service provider, payment gateway and specific architecture. Payments are categories for either for purchases or invoices. If mobile payments are for purchases, it uses mobile wallet money, digital checks, credit cards, debit cards. If mobile payments for invoices, it allows money transfers account to account, direct payment through debit card, internet banking. [1]

6. CONCLUSION

By the emerging era of mobile wallet payments, there are numerous architectures are in the market and new coming day by day with the distributed environment. This paper gives the literature reviews on available mobile wallet transaction architectures and gives the comparison and identifies the supported participants. These architecture literature reviews may helpful for new innovative research. Discussed architectures are partially helpful to mobile wallet application developer to make a more convenient, efficient and flexible mobile wallets application. Most of the architectures are developed by experts in early phases. They suggest that mobile wallet architectures have a general control and security environment, specific control and security measures, and customer awareness, education, and communication. In future, it may possible to develop new architectures which overcomes the limitations of previously defined architectures and enhances the current available architectures with required participants.

7. ACKNOWLEDGMENT

I thank my co-author Dr. Dharmendra Patel, Associate Professor, CMPICA, CHARUSAT, Changa for guidance, support and valuable comments to greatly improve the paper manuscript. Last but not the list, we offer our true regards to all of those who supported us in any respect during the completion of the paper.

8. REFERENCES

[1] Dahlberg, Tomi, Niina Mallat, Jan Ondrus, and Agnieszka Zmijewska. "Mobile payment market and research–past, present and future." Presentation at Helsinki Mobility Roundtable, Helsinki, Finland (2006).

[2] Hoofnagle, Chris Jay, Jennifer M. Urban, and Su Li. "Mobile payments: Consumer benefits & new privacy concerns." (2012).

[3] Kasiyanto, Safari. "Security Issues of New Innovative Payments and Their Regulatory Challenges." In Bitcoin and Mobile Payments, pp. 145-179. Palgrave Macmillan UK, 2016.

[4] Khiaonarong, Tanai. "Oversight issues in mobile payments." (2014).

[5] Simplot-Ryl, Isabelle, Issa Traoré, and Patricia Everaere. "Distributed architectures for electronic cash schemes: a survey 1." International Journal of Parallel, Emergent and Distributed Systems 24, no. 3 (2009): 243-271.

[6] Ala-Peijari, Ossi. "Bitcoin The Virtual Currency: Energy Efficient Mining of Bitcoins." (2014).

[7] Security of Mobile Payments and Digital Wallets, ENISA December 2016, https://www.enisa.europa.eu/publications/mobile-payments-security/at_download/fullReport.

[8] Medvinsky, Gennady, and Clifford Neuman. "NetCash: A design for practical electronic currency on the Internet." In Proceedings of the 1st ACM conference on Computer and communications security, pp. 102-106. ACM, 1993.

[9] Sirbu, M., and Tygar, D. Netbill: An internet commerce system optimized for network delivered services. In Proc. Technologies for the Information Superhighway (COMPCON'95) (San Francisco, California, USA, 1995), IEEE-CS, pp. 22–27.

[10] Chaum, D. Online cash checks. In Proc. Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT'89) (Houthalen, Belgium, 1989), vol. 434 of Lecture Notes in Computer Science, Springer, pp. 288–293.

[11] Deng, R. H., Han, Y., Jeng, A. B., and Ngair, T.-H. A new on-line cash check scheme. In Proc. 4th ACM Conference on Computer and Communications Security (CCS'97) (Zurich, Switzerland, 1997), pp. 111–116

[12] Buttyan, Levente, and N. Ben Salem. "A payment scheme for broadcast multimedia streams." In Computers and Communications, 2001. Proceedings. Sixth IEEE Symposium on, pp. 668-673. IEEE, 2001.

[13] Ferguson, Niels. "Extensions of single-term coins." In Annual International Cryptology Conference, pp. 292-301. Springer, Berlin, Heidelberg, 1993.

[14] Chaum, David. "Blind signatures for untraceable payments." In Advances in cryptology, pp. 199-203. Springer US, 1983.

[15] Pagnia, Henning, and Ralph Jansen. "Towards multiple-payment schemes for digital money." In International Conference on Financial Cryptography, pp. 203-215. Springer Berlin Heidelberg, 1997.

[16] Lysyanskaya, Anna, and Zulfikar Ramzan. "Group blind digital signatures: A scalable solution to electronic cash." In Financial cryptography, pp. 184-197. Springer Berlin/Heidelberg, 1998.

[17] Hoepman, J.-H., and Jacobs, B. Increased security through open source. CoRR: Computing Research Repository abs/0801.3924 (2008).

[18] Camenisch, Jan, and Markus Stadler. "Efficient group signature schemes for large groups." Advances in Cryptology—CRYPTO'97 (1997): 410-424.

[19] Chaum, David, and Eugène Van Heyst. "Group signatures." In Advances in Cryptology—EUROCRYPT'91, pp. 257-265. Springer Berlin/Heidelberg, 1991.

[20] Xu, Qiang, and Hong Zhao. "Distributed electronic payment system based on bank union." In High Performance Computing in the Asia-Pacific Region, 2000. Proceedings. The Fourth International

Conference/Exhibition on, vol. 1, pp. 548-551. IEEE, 2000.

[21] Yang, Beverly, and Hector Garcia-Molina. "PPay: micropayments for peer-to-peer systems." In Proceedings of the 10th ACM conference on Computer and communications security, pp. 300-310. ACM, 2003.

[22] Wei, Kai, Alan J. Smith, Y-FR Chen, and Bin Vo. "Whopay: A scalable and anonymous payment system for peer-to-peer environments." In Distributed Computing Systems, 2006. ICDCS 2006. 26th IEEE International Conference on, pp. 13-13. IEEE, 2006.

[23] Lipton, Richard J., and Rafail Ostrovsky. "Micro-payments via efficient coin-flipping." In International Conference on Financial Cryptography, pp. 1-15. Springer, Berlin, Heidelberg, 1998.

[24] Gabber, Eran, and Abraham Silberschatz. "Agora: A minimal distributed protocol for electronic commerce." In The Second USENIX Workshop on Electronic Commerce Proceedings, pp. 223-232. 1996.

[25] Xu, Qiang, and Hong Zhao. "Distributed electronic payment system based on bank union." In High Performance Computing in the Asia-Pacific Region, 2000. Proceedings. The Fourth International Conference/Exhibition on, vol. 1, pp. 548-551. IEEE, 2000.

[26] Yacobi, Yacov. "Risk management for e-cash systems with partial real-time audit." Netnomics 3, no. 2 (2001): 119-127.

[27] Zhu, F. M., Sheng-Uei Guan, and Yang Yang. "SAFER e-commerce: Secure agent fabrication, evolution & roaming for e-commerce." Internet commerce and software agents: Cases, technologies and opportunities (2000): 190-206.

[28] Falk, Eric, and Jérémy Charlier. "Your Moves, Your Device: Establishing Behavior Profiles Using Tensors." In International Conference on Advanced Data Mining and Applications, pp. 460-474. Springer, Cham, 2017.

[29] Dahlberg, Tomi, Niina Mallat, Jan Ondrus, and Agnieszka Zmijewska. "Past, present and future of mobile payments research: A literature review." Electronic Commerce Research and Applications 7, no. 2 (2008): 165-181.

[30] Ma, Xiaohua, and Wenxue Wei. "The architecture of mobile wallet system based on NFC (near field communication)." Research Journal of Applied Sciences 7, no. 12 (2014): 2589-2595.

[31] Wu, Huaigu, Louenas Hamdi, and Nolwen Mahe. "Tango: a flexible mobility-enabled architecture for online and offline mobile enterprise applications." In Mobile Data Management (MDM), 2010 Eleventh International Conference on, pp. 230-239. IEEE, 2010.