**Description:**

Proposed system would enable secure and private transaction for online or offline purchases either with your credit cards, debit cards or even a checking account without carrying any plastics or checkbook. This will also enables purchasing without giving out any personal information of any sort. Any time user wants to do any financial transaction he/she creates a new one using his/her mobile or web service application or even a tradition phone call (automated call) to a bank institution or a credit card company (aka "Providers"). Google wallet is convenient and already solves part of the problem but you need to use Google services and abide by its terms. Google and other ecosystems are convenient but they are becoming new walled gardens. This could be another tool to avoid credit card frauds especially online transaction frauds.

**Value Proposition:**

Benefit to the “Providers’:

* No need to design, manufacture and distribute millions of credit, debit cards or checks year after year, saving paper and plastic.
* They don't need to keep track of lost/stolen cards,
* May need to worry less about loss of millions of dollars to financial fraud due to lost/stolen cards.  The rapid growth of credit card use on the internet has made database security lapses particularly costly. Whenever it happens millions of accounts have been compromised at a time. Today’s fraud detection systems are designed to prevent a very small percent of all transactions processed which still translates into billions of dollars in losses (Business Applications of Neural Networks by Bill Edisbury).

Benefits to End Users:

* End user doesn’t need to carry or keep track of plastics or check books.
* Protect user’s personal information from proliferating across the globe.
* We strongly believe that the retailers don’t need (and store) customers personal information to complete the transaction. Retailers can't misuse user data (like sharing or selling it to others as there is nothing to misuse).
* Convenient way of fastest money transfer to their close friends or family members in urgent need. Imagine a friend is travelling in New York City and he/she is in dire need of immediate money because he/she has lost all the belongings. In this scenario a Sender creates a virtual-transaction with all the details including a secret code (similar to a debit card pin #) and gives this information (a string) to the receiver over the phone who in turn uses it at ATM machine (or special kiosks at 7Elevan or 24-hr stores) to cash in.

Benefit to the Retailers:

* Since merchants don't get user's personal information, they don’t need to build an infrastructure to save and monitor that information.
* Retailer’s benefit tremendously by getting personal information of their customer which they can use for targeted advertising. To mitigate this issue, we are suggesting another piece of information which can be as anonymous as possible like an email address could be used to advertise the products to individual customer. Email addresses can also be used to send out the receipts.
* They can be protected from the use of fraudulent credit cards. In year 2009 BestBuy Inc., lost $100 million worth of goods to a gang of hackers/thieves who used stolen credit card information to place the orders online.

Solution:

* Both retailer and Provider needs to sign-up with ‘Intel Service’. This is like a router service which receives a virtual-transaction from the participating retailer and forwards it to the correct participating provider along with retailer information in encrypted form. Rest of the transaction completes as usual.
* For end user, there will be application (mobile or web) with common interface to all "Providers". User inputs a name for a transaction (optional), assign expiration date (optional), amount, and a pin code (optional and can be different every time if needed). The input process can be automated with few rules to make it more convenient.
* Then user submits to a "Provider" of choice at the time, who in turn generates an encrypted string or a number with a bar code (can simply be scanned at the brick-and-mortar store).
* User can use this string/number at online merchant (for e.g. amazon), which internally could decrypt enough information to know about "Provider". This gets sent to a Provider who can authenticate, decrypt and complete the transaction marking it as "done" in the system.
* Every provider can have their own encrypt/decrypt technology. This gives user a freedom and improves mobile banking experience.  "Providers" will certainly need to use Intel's best and fast server technology with dedicated encryption/decryption circuitry to provide faster service.
* These transactions will have default expiration date/time so unused transaction becomes obsolete.
* User or Retailer doesn’t need invest into NFC enabled devices (thought the proposed system can take advantage of NFC to automate the creation of virtual-transaction and using it at the retailer and giving seamless experience to the user)