Offline eCash 2.0

Robust in-person payments later onlineable

David Chaum
XX NETWORK

Abstract: When smartphones are relied on for payments, there are situations where payments are needed but cannot be consummated securely. One such use case is when the payer does not have their phone with them or it is not working; another is when both the payer and payee each have a working phone, but no suitable network connection is available. A third case, this time potentially affecting almost everyone, is when no online payment system is available for an extended period, such as due to an attack on infrastructure or the failure of many phones. A new kind of solution introduced here, based on a novel but very inexpensive physical card variously combined with smartphones, covers all three use cases.

Known approaches are inapplicable or impractical for this range of use cases. Solutions relying on trusted chips for instance, such as what was called "Mondex," suffer from systemic security vulnerabilities and are inapplicable when no electronic devices are available at the point of payment. Solutions relying only on software, including previous proposals by the present author, do not provide strong assurance of finality and are also inapplicable without physical devices to run that software. The approach introduced, however, is secured by a novel solution to what the author has called the "double spending" problem. In fact, double-spending is prevented here both at the point of payment and when payments are brought online. Moreover, some variations provide privacy and even what has been called "inalienable" privacy, when combined with (online) eCash 2.0.

Regarding inclusivity, the technology has a lot to offer the one third of the global population without bank accounts. Additionally, it can help the slightly larger percentage that skews rural and is without Internet access. Moreover where electronic payments have driven paper money out of widespread use, large-scale failure of electronic systems can leave people in any country vulnerable. In such emergency use cases, crucially, the technology introduced here allows value to be injected quickly, with all outstanding value readily "onlineable" afterwards.

Introduction

A physical card the size of a standard credit card made of transparent plastic and containing micro-glitter can be infeasible to clone. (In fact, such glitter suspended randomly in clear plastic has proven effective for anti-cloning security even in the context of international arms verification against national-laboratory adversaries.) Smartphones, especially with their software-controlled cameras and light, can readily recognize such dispersed micro-glitter patterns. The card can be confirmed as the genuine original when the glitter pattern captured by the camera of the smartphone receiving payment matches the one digitally signed by the card issuer.

Scratch-off "tiles" are arrayed on such cards. Since one payment mode requires tiles to be individually detached or "broken out" from the card, perforations akin to those on sheets of postage stamps are provided. Denominations printed on the scratch-off, like those printed on banknotes, label each tile. Under each scratch-off is a secret, represented in the examples shown as a two-dimensional barcode (see Figure 2). Revealing the barcode lets the tile and its value be authenticated via a corresponding digital signature. Those barcodes already revealed by being scratched-off will no longer be accepted in payment, either in person or when brought online; this ensures that no tile's secret barcode is accepted more than once, preventing double-spending both when the barcode is proffered at the point of payment and when it is brought online.

Each secret barcode is first randomly generated, printed on its respective tile, and then rendered infeasible to read by application of the scratch-off coating. The process is similar to the production of so-called "probability-game" scratch-off lottery tickets; if there were a known technique that could read the codes on such tickets without damaging the coating, it would likely already be used by attackers to obtain substantial payouts.

Barcodes formed simply by choosing uniformly at random which squares of a checkerboard are filled white and which black can be used since they are more space-efficient than standard QR codes. Each such barcode represents an unpredictable cryptographic key of a length believed adequate—about 100 bits in the examples shown. Using multiple colors, instead of simply black and white, could let the code's checkerboard pattern have sides several times shorter. Current smartphone camera resolution already allows considerably smaller features, and thus many more tiles and their checkerboards, than the number illustrated on the card of Figure 2. As will become apparent, though, usability places ultimate constraints on how small the tiles can be and hence on the number of tiles per card.

There are fundamentally only two ways the card can be used in payment. Either tiles remain "integral" to the card, even though a counterparty is able to learn barcodes hidden under the scratch-off of those tiles; or tiles are physically "broken out" from the card and physically transferred by payer to payee (called "breakout-tile mode" below). There are two different modes where tiles remain integral to the card: one is used in case both phones are present but the network is unavailable (called "offline-phone mode"); the other mode is used in case the payee's phone is online but the payer's phone is unavailable (called "card-only mode").

Offline-phone mode applies when phones are working but there is a temporary lack of communication, such as during a visit to a remote area without good coverage. This mode can be used to consummate a payment transaction offline while keeping tiles integral with the card. Later, when the payee is online, they can upload the value received, transferring it for instance to their own account. Digital signatures that ensure card un-clonability, validity of the barcodes, and value availability are provided by the payer's phone to the payee's phone, using local short-range communication like Bluetooth. The scratch-off in effect lets the payee protect themselves against double-spending, while the online system protects against double-spending by payees.

Card-only mode applies when the payer's phone is not available but the payee's phone is functioning and connected online. The payer allows the payee's phone to obtain barcodes from tiles on the payer's card corresponding to the agreed amount, while keeping tiles integral with the card. Information for checking the card's validity is provided to the payee's phone online, as are confirmation of barcodes, of no double-spending, and of value availability.

Breakout-tile mode would be resorted to when disruption of online access is anticipated to persist or when many phones are not operational. Once breakout-tile mode has been initiated, payments use tiles that have been broken out from cards. The recipient of such a broken-out tile can later pass it on to another person, and so forth, ensuring no double-spending much like with paper money. Only when someone who has received such a tile is ready to take the value online do they scratch-off the tile. This renders the tile untransferable and ensures that they are the only person who could have learned the barcode. When they take the value online, by scanning in the barcode, the online system additionally ensures at this point that there is no double-spending. Features on the reverse of the card allow all tiles, whether or not previously scratched-off in offline-card or card-only modes, to be used in breakout-tile mode.

Cards can be sold to users prepaid. In either offline-phone mode or card-only mode, each tile remains integral to the card, but can be scratched-off in place and spent at "face value." In either of these two modes, however, a tile can also be used to make a payment for less than its face value. The unspent portion of the face value, similar to the "change" returned when payments are made with a banknote, remains in the account automatically created for the card when the card is first provided to the cardholder.

Cards need not be purchased with the full face value of all tiles; the prepaid balance on a card can also be increased as needed by the cardholder adding value online. Whenever value is added, all outstanding change can be incorporated into the new balance on the card. Tiles are fungible:

any previously-unused tile can be used in a payment up to its full face value, limited only by the current actual balance on the card. When all but one of the tiles are scratched off, that tile is reserved for "closing out" any unspent balance remaining on the card.

Below, first the offline-phone mode, then the card-only mode, and finally the breakout-tile mode are further introduced and detailed each in their own sections. Finally, privacy considerations are presented.[1]

Offline-Phone Mode

This mode requires that both the cardholder and the party receiving payment use their own smartphones. The phones communicate with each other locally, over Bluetooth or the like, but without needing any communication over a wider network at the time of payment. When the party receiving payment is later connected to the internet, that party can move the received value online. Use-case examples include:

- When users are outside reliable and affordable network coverage;
- When coverage and/or payment-system infrastructure is temporarily unavailable to users; or
- When, even though online systems are available to users, special lottery-like pop-ups appear randomly to incentivize exercise of system readiness (described further in the Discussion section).

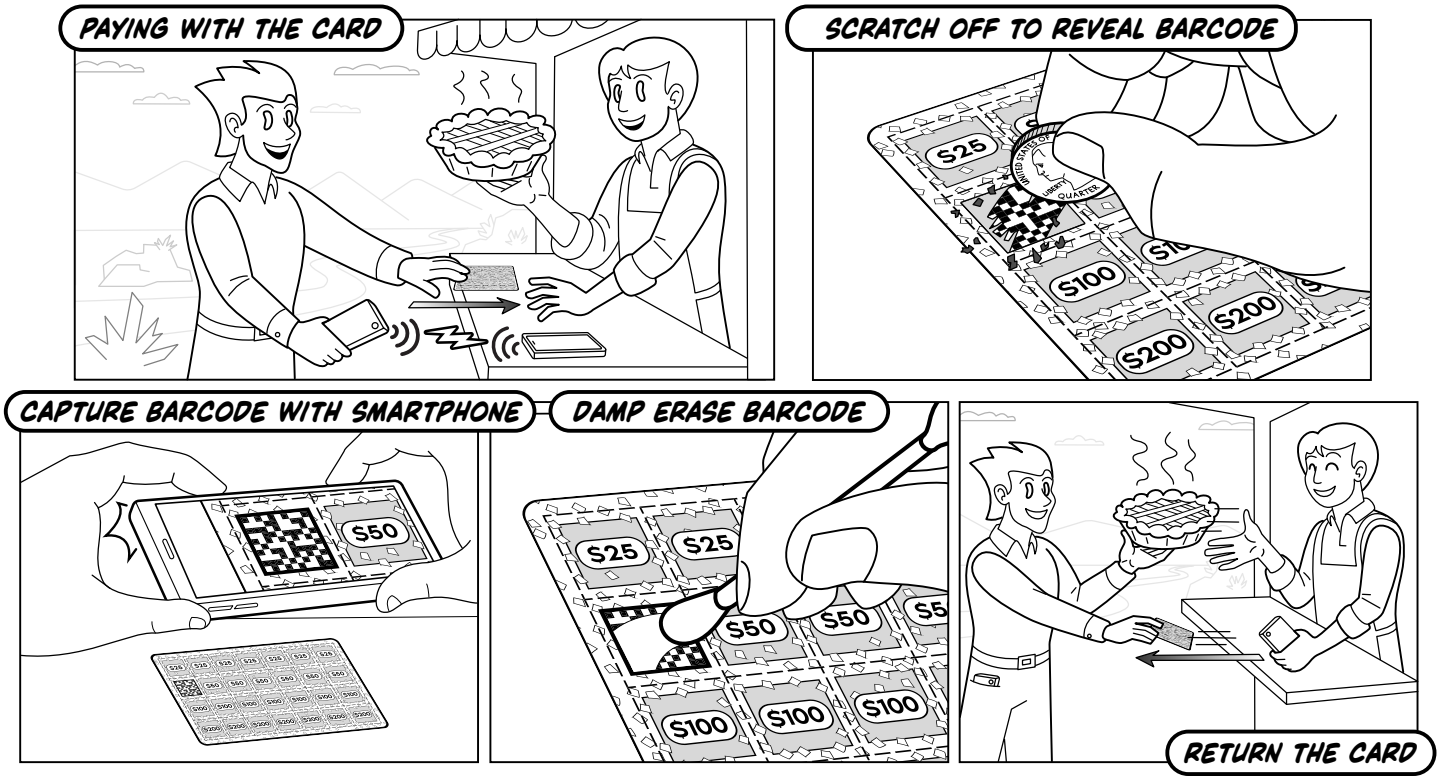

Figure 1: Paying in offline-phone mode

Figure 1: Paying in "offline-phone mode." (1) The buyer hands their card to the party to be paid, shown in the example as a seller. (2) The seller scratches-off a tile with the agreed denomination. (3) The seller uses their smartphone to capture the barcode along with the glitter pattern over the whole card including scratch-offs, which it checks cryptographically using information supplied to it electronically but locally by the buyer's smartphone. (4) The seller uses a damp wipe to erase the water-soluble barcode printing; this prevents anyone else from learning the barcode and onlining the money before the seller does. (5) The seller returns the card to the buyer along with the goods purchased. (6) Not shown is that later, once the seller is able to connect to the Internet, the barcode can be onlined and the value added to the seller's online account, whether a bank account or an automatically created card account for the seller's card.

[1]It is unclear what if any advantage chip cards bring. They cannot by definition work in "breakout tile mode." They are more easily cloned in "offline-phone mode" because keys have to be contained in each card instead of only at a secure location. To keep a card from being emptied by a payee in "card-only mode," a chip card still needs on-card scratch-off. And if a balance is to be shared securely between an offline-phone transaction and a "card-only" one, scratch-off would need to be integrated with the offline-phone one as well.

In the example shown in Figure 1, a payment is made by a cardholder to a seller. This could be in a remote area without online access and also where the seller, although possessing a smartphone, might be unbanked. The value provided is cryptographically protected at the time of payment, so that at any later point the value is onlineable only by the seller's smartphone. This later onlining of value could for instance be when the seller is routinely online or when making an occasional visit to a retail location that provides various forms of access. For instance, standard Internet access could be provided at the location so that the seller could themselves transfer the value received in payments. This transfer could be to the seller's own bank account; or it could be to the online account automatically created for the seller's card and be paid out later by the seller using that card. Alternatively, the location could be given access to the value received by the seller; the location could then, in real time, transfer the value in favor of the location's bank account while simultaneously providing the seller with physical goods in kind.

The entire digital part of the offline transaction can take place essentially automatically between the two smartphones. The two parties merely have to scratch-off the correct denomination, point the seller's phone camera at the card and barcodes, and then preferably wipe away the barcode.

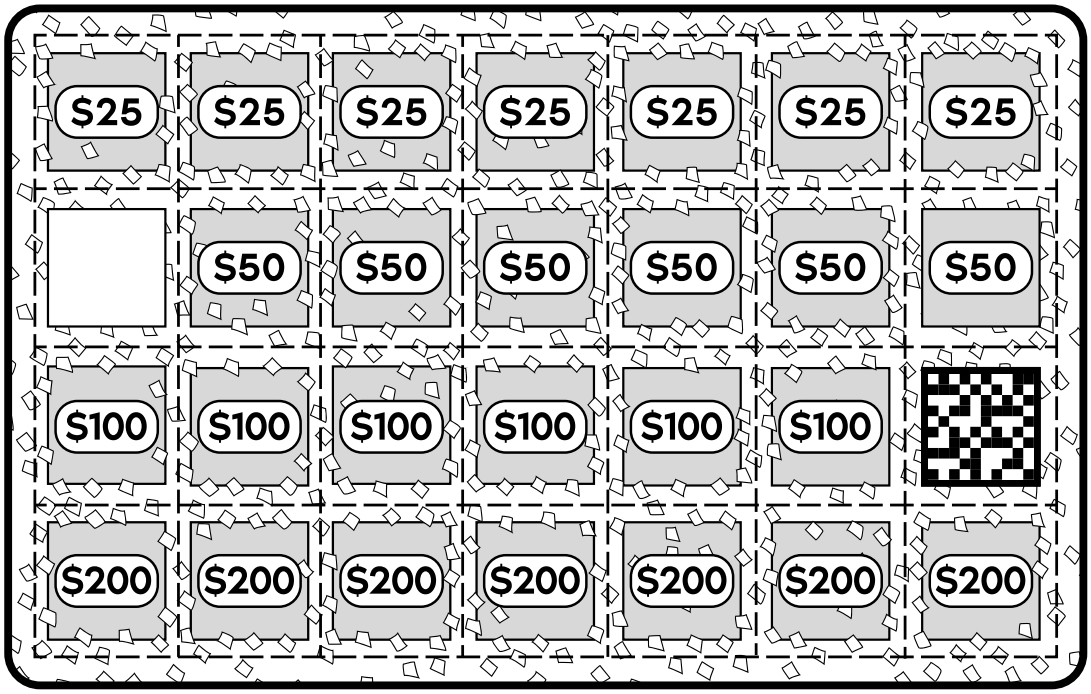

Figure 2: Example of partly-used card with integral tiles.

The tile on the left was spent as in Figure 1 and the one on the right is in the process of being spent, either in offline-phone mode or in card-only mode. The spent tile has been wiped of its barcode; the tile on the right shows the barcode before it is wiped.

Cryptographic setup: Tiles with denominations equal to or somewhat exceeding the total amount of payment are scratched off by either the payer or the payee, ideally while only the payee's smartphone camera can view the revealed barcodes. The payer's smartphone simultaneously provides the payee's smartphone with a copy of the digital signature from the card issuer, which the payer's phone obtained originally along with the card. This signature authenticates three things:

- The "root" of the "Merkle tree" of hashed images of the barcodes, which lets the validity of any tile's barcode be efficiently and definitively checked as being part of the signed cryptographic structure. (Merkle trees, common in cryptographic security systems, are for present purposes essentially an inverted branching structure such that the "root" is a hash of several nodes at the next level below the root, with similar additional levels down the tree, till the level comprising the separate hash of each barcode "leaf.") Knowing this digital information does not, however, allow barcodes themselves to be derived, because that would mean inverting the tree's one-way hash function to discover the code. Thus, the codes can only be obtained from the physical card.

- The pattern of glitter reflection angles, which the payee phone can use to validate the card. In much the same way as astronomy websites use a database of stars to easily search for and identify any view of the sky, the algorithms can recognize the pattern of glitter so that it can be checked as digitally signed and thus authenticate the card. Including the card issuer-signed portion of this data allows the payee smartphone to ensure that the physical card is the genuine card and not a clone. Glitter present on the scratch-off coating itself allows secure verification of which tiles have not already been scratched off, and thus the total face value already used.
- A public key of the payer's smartphone, which allows that phone to form a digital signature that verifiably has been signed on behalf of the payer. However, if the card is loaded by an (online) eCash 2.0 payment, and the Merkle tree is provided encrypted with the public key of the loading payment, the "inalienable" privacy-tracing property of the eCash 2.0 used would be conferred on all payments made with the card: the maker of the eCash 2.0 payment would have the inalienable ability to recognize or reveal any payment made with the card.

Transaction process detail: During a payment from a cardholder to a merchant, the merchant's smartphone: (1) receives data from the cardholder's phone; (2) can agree on the amount and optionally on any particulars of the purchase with the cardholder's phone; (3) checks that the cardholder's proffered card and scratch-off coverings are genuine; (4) checks that the card has sufficient unscratched tiles corresponding to the amount of payment and the balance signature; and (5) verifies that the barcode(s) revealed are valid.

Five digitally-signed data items are received by the cardholder's phone, either at the time of card issue or when the prepaid card balance is increased in a reload: public key (a) of the card holder, overall glitter pattern (b), Merkle tree (c) of the barcodes, net balance (d) on the card at time of latest reload, and total amount of tile face-value scratched-off (e) at the time of latest reload.

The phones agree on the amount of payment (f); and the merchant's phone optically determines the total amount of the face-value previously scratched-off (g).

More specifically:

1. The card-issuer-signed data, (a)–(e) above, is provided by the cardholder's phone to the merchant's phone.

2. The two phones agree on the transaction details. This includes at least the amount of payment (f), which they can display or audibly communicate to the respective parties, so that agreement is reached. The merchant's phone can optionally provide its own digitally-signed receipt, should suitable authentication for this be available. The receipt from a merchant could be issued early but include the proviso that a valid barcode will be provided. The cardholder's phone could also provide its own digital signature on agreed transaction details. This would be signed with the private key, presumably originally formed by the cardholder's phone, corresponding to the public key (a) in the signed data received by the cardholder's phone. Best practices would include using so-called "session-keys" to protect all communication.

3. The merchant's phone illuminates the card by blinking its LED and captures the pattern of glitter detected by its camera. This is verified against the card-issuer-signed glitter pattern (b) to prevent cloning. The merchant's phone will also, at the same time, securely learn the pattern of tiles remaining un-scratched-off, from which it can compute the total face value already scratched-off and spent from the card (g).

4. The merchant's phone checks that there is sufficient value on the card for the amount of payment. To do this, it checks that the amount of payment (f) is less than the card balance at latest reload (d) minus the amount scratched off at time of payment (g) minus the amount scratched off at time of latest reload (e): $d–g–e \geq f$. Put simply, the amount of value loaded on tiles that remain unscratched-off should exceed the amount of payment. Those tiles already scratched-off prior to reload can be subtracted from the total seen to have already been scratched off at time of payment, leaving the amount of tiles spent since reload. Once this amount of the reload that can have already been spent is deducted from the reload amount itself, what remains is the value available to spend, which should be at least the agreed payment amount.

5. A finalizing manual step locks in the payment: the merchant or the cardholder removes the scratch-off from the corresponding tiles, exposing barcodes with the total value equal to or somewhat exceeding the amount of payment (f). The merchant's phone is immediately able to hash and thereby verify the barcodes as having been signed by the card issuer as part of the Merkle tree (c), and thus assures the merchant that the amount (f) will later be honored online. The merchant can use a suitable wipe to remove the water-soluble barcodes from the card, to prevent the cardholder or any other party in future from gaining visual access to the barcode.

6. A finalizing digital step can include in effect a so-called "non-interactive zero-knowledge proof" of the barcode as well as the amount of payment and the merchant's private key. This provides proof of the portion of the tile value that was used, so if not yet onlined by the merchant, the change can still be included in the card balance at the next reload. Payment fraud by either party is prevented by this protocol. On the one hand, the merchant cannot online a false larger portion of the denomination as spent, since the signature on (f) with the private key corresponding to the public key (a) must be submitted. On the other hand, the cardholder cannot online while adding value to the card a false smaller amount of the denominations as spent, since the zero-knowledge proof from the merchant cryptographically authenticates the amount (f) as agreed by a party knowing the barcode.

Card-Only Mode

When the payer's phone is not working or is unavailable, but the payee's phone is functioning and connected online, the payer allows the payee's phone to obtain barcodes with an agreed amount of value. The payee's phone can then learn online the image under the Merkle tree hash function of the barcodes corresponding to the glitter pattern and the available balance. The example shown in Figure 1 would be largely the same, except that the buyer's phone would be absent and the seller's phone would communicate online, instead of locally with the payer's phone.

More specifically, steps (1), (2), and (6) above would essentially be combined into an online deposit of the barcodes at the time of payment. Portions of the card-issuer signed data, (b) and (c), supplied by the cardholder's phone in offline-phone mode, are in this mode instead supplied to the merchant phone by the online system so that the merchant phone can check the barcodes and glitter. The agreed-on amount of payment (f) is also confirmed online.

A PIN code or the like for online use could be assigned to the card, affording the cardholder additional protection of value on the card and in the automatically created account. (The card could not in any case be used without the relevant data stored in the cardholder's phone and the cardholder's account.)

Breakout-Tile Mode

No smartphones are used during payments made in this mode; a phone is, however, needed to online the value(s) once the tiles stop circulating. Use cases include:

- When a prolonged network outage is anticipated; or
- When prolonged unavailability of most phones is anticipated, such as when phones are disabled by so-called "electromagnetic pulse" or a prolonged power outage; or
- When both parties' phones are absent or not working, as might happen occasionally in an otherwise functioning setting (only with the privacy-protected version described below).

In the event of a general infrastructure failure caused by events like sabotage, conflict, or even environmental catastrophe, offline payment may become critical for distribution of necessities and to preserve civil society. In such emergency use cases, a central bank or government agency, for instance, could in effect "activate" all tiles or only some denominations as spendable in breakout mode. This could simply be by decree or be triggered by conditions announced in advance. The tiles might, for instance, be considered emergency loans, ration tickets, or even a grant of special backup currency. Each broken-out tile has its denomination unalterably marked much like with banknote security printing; however, interpretation of denominations in breakout mode could depend on the emergency.

Ultimately, once connectivity is restored, every holder of emergency tiles can "redeem" them individually by removing the scratch-off and onlining the barcode. These are readily checked online as genuine by the card issuer, which can then provide the value available in favor of the person who first onlined each one. In this way, all users themselves can more or less simultaneously transfer the emergency value online, without having to physically visit or otherwise use central locations. Quick, secure, and distributed onlining of value at such a time can be a critical part of providing continuity of payment functionality and minimizing disruption of civil society. The ability to rapidly issue and then redeem at scale are thus key unique features of the system introduced here.

A variety of visible and hidden document security techniques, such as holograms and special inks and inclusions, like those used for securing banknotes, are believed able to provide an acceptably high level of counterfeit-resistance for tiles and their denominations. These could be located on the reverse side of the card, with the scratch-off on the obverse. Hence, even when tiles are removed from a card, users can be adequately confident that the tiles do in fact represent specific amounts of value, each like a banknote with its corresponding denomination.

Breakout use of every tile: One way to allow tiles that have already been spent in offline-phone or card-only modes to be later

used in breakout mode is to have an additional barcode for this. This code could remain visible, possibly in its own indelible but more subdued color, after the barcode for integral-tile modes is wiped from the card as it should be in payment. A way is needed to prevent a race to redeem these exposed barcodes by anyone other than the party holding the tile "when the music stops." Requiring ten additional bits for onlining these already previously scratched-off tiles solves this problem if these extra bits are hidden under document-security features. For instance, heat or a solvent could be used to remove the document-security feature enough to reveal the position of a few pieces of glitter or printing. Trying to cheat by falsely claiming to be the party in possession of a tile with a particular barcode is a hard attack to scale without detection. And so, by simply requiring an escrowed penalty combined with a fixed dispute period, the extra bits would likely need only be resorted to in the rare case of a nuisance dispute. Already-scratched-off tiles could, provided that their document security features were still intact, thus safely be accepted in breakout mode.

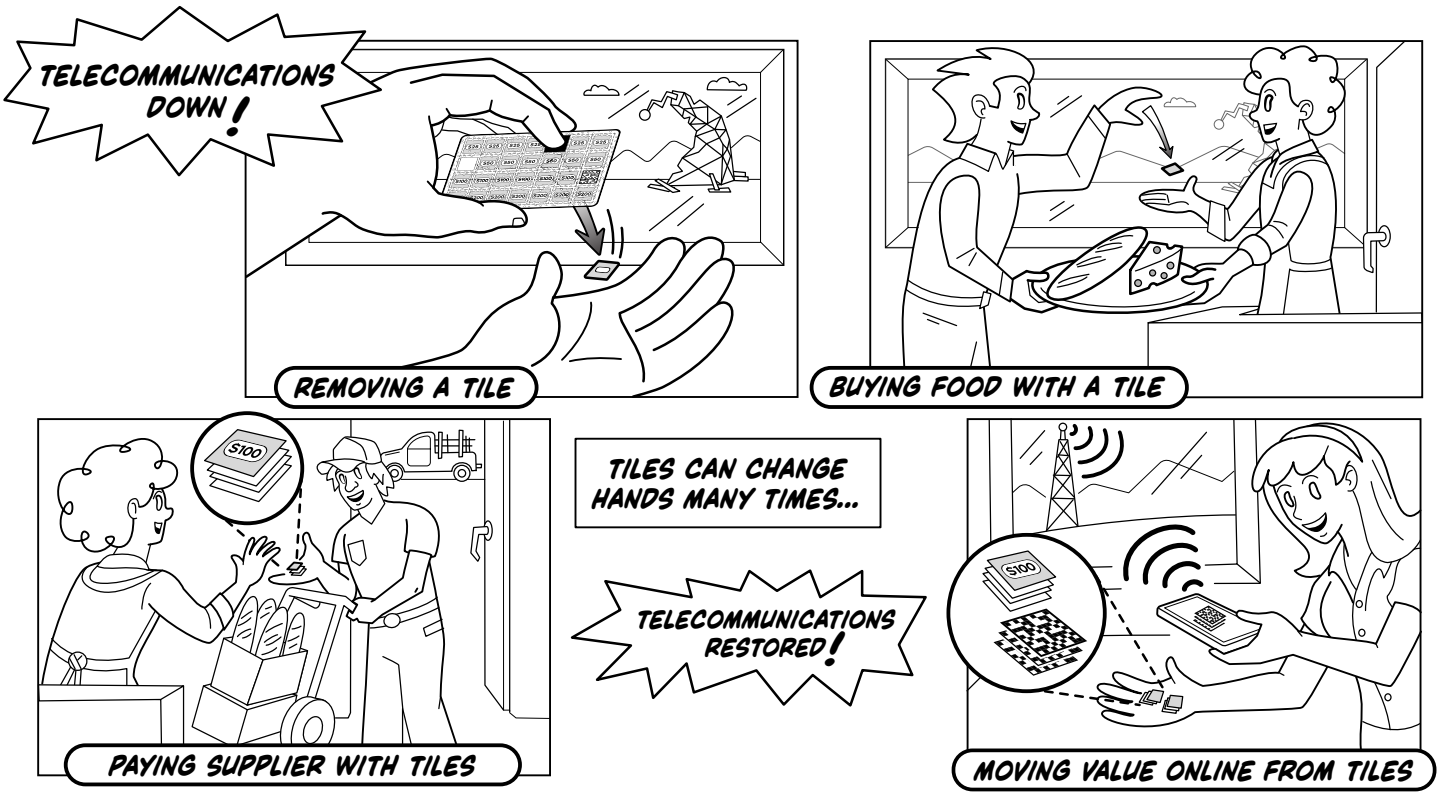

Figure 3: Paying with tiles broken out from the card.

(1) The original cardholder breaks a tile with the appropriate denomination out from their card. (2) They then provide the tile for a purchase. (3) The retailer receiving the tile, who may accumulate tiles, later provides tiles to pay a supplier. (4) The supplier can transfer the tiles in making whatever business or personal payments. Further parties receiving tiles from the supplier can accumulate and/or in turn transfer them on, and so forth. (5) Once communication is restored, a party holding tiles at that time can scratch them off to reveal the barcodes for capture by a functioning phone and subsequent onlining of the value.

Privacy of Payments

When cards are initially issued, they may to a degree be linked to a particular person or they may in effect be anonymous. All payments where the tiles remain integral to the card and where glitter dispersed through the whole card prevents cloning, though, are at least in principle linkable to that card. If the card is linked to a person, so are all payments made with it. Cards could be purchased anonymously, as with many prepaid cards today, thereby unlinking a card from a person, at least until the card is used extensively enough to link everything. Breakout-tile payments, however, can in fact be more private than cards or even paper money today. Serial numbers of paper banknotes are fully tracked through banking systems in some countries. Even in countries where this is not required, automatic counting machines used at every stage of cash handling routinely capture all serial numbers. Moreover, there are public websites on which volunteers link serial numbers to postal codes where the notes were seen.

The breakout tiles of a privacy-protected system are authenticated by the document security features, which are on the reverse side and essentially all identical. Only the information hidden under scratch-off would in practice uniquely identify such a tile. One way to produce cards where each tile is independently and unlinkably chosen starts by making randomly barcoded tiles in sheets or rolls before dicing them into separate tiles. Once diced, tiles are then tumbled in hoppers, like lottery tickets, ideally in public view. After that the tiles can be placed on cards by so-called "pick and place" machines, fast and precise machines used to assemble electronic circuit boards. The tiles, like with the plastic rings of the German five-euro coin, can finally all be pressed securely into the card at once.

The structure under scratch-off in such tiles would include at least some glitter. This could be augmented by barcode or other printing to conveniently bring the total amount of random bits up to about 100, as mentioned earlier. The scratch-off coatings on tiles, though of course unique at a microscopic level, can each be kept largely indistinguishable by ordinary cameras. The "star-pattern-finding" algorithm run on the glitter pattern lets the relevant Merkle tree portion be supplied (along with any printed barcode information) as part of the online transaction in card-only mode; for offline-phone mode, payer phones can store and then supply payee phones with the card-batch-specific portion of the Merkle tree.

There are two different systems for using independently-random barcodes with integral tiles. The systems differ depending on whether or not the glitter that is exposed by scratched-off tiles remains on the card. This is because it both identifies the card and also allows the total amount spent to be securely ascertained. Glitter can be wiped away, just like with the water-soluble ink barcodes of the non-privacy tiles, if glitter is suspended in a water-soluble clear plastic film, such as so-called "PVAc." In the system in which glitter is not to be wiped away, the integral-tile modes are essentially the same as without the privacy tiles. In the system where glitter is to be wiped away, if cards are required to be prepaid to full face value for integral-tile mode use, payee phones need not be allowed to see the whole card—and the linking of payments to cards can be hidden.

Discussion

To help make the cards attractive to carry, so that they are at the ready if needed in an emergency, the form factor can conform to current standards, such as ISO, and include conventional features as well. For instance, smart-card chips, with or without contacts, can be included to give compatibility with other systems. Also, both integral-tile and breakout-tile modes' ability to allow payments in situations where network communications or phones themselves are temporarily unavailable can be a compelling reason to carry the cards.

Carrying value in the form proposed here is further encouraged because it would be well protected against theft or misuse by others. For offline-card mode, the full range of techniques protecting smartphones from use by other than the owner would automatically apply. For card-only mode, a PIN code or the like, as mentioned, could be required to use the card, although the payee might learn the code. Only if breakout-tile mode were ever initiated would loose tiles be just like cash.

Financial incentives can additionally be provided to users and merchants to keep cards widely held and also to keep the integral-tile use-cases exercised. Such incentives could be randomly spread over time and be for small amounts. For instance, mini pop-up lotteries or discounts could unpredictably in effect "activate" certain tiles or certain retailers.

Altogether, these various aspects combine to help keep everything at the ready in case infrastructure failure requires the valuation of tiles for break-out.

Conclusion

The approach introduced here is innovative, practical, and secure in several major use cases. The advantages of this fundamentally new approach to payment technology hold tremendous potential to touch the lives of many.